Adaptive Risk Manager Online
Installation Guide
10*g* (10.1.4.3.0)

December 2007

Adaptive Risk Manager Online Installation Guide, 10g (10.1.4.3.0)

Contents

Preface

Adaptive Risk Manager Online is the administration user interface of Oracle Adaptive Access Manager, a set of web-based administration tools that provides sophisticated fraud monitoring, analysis, and tracking by user location, device, time of day, type of transaction, as well as a host of other factors, and evaluates these factors against a set of customizable rules.

The Adaptive Risk Manager Online Installation Guide takes you through the installation of the Adaptive Risk Manager Online.

After you have completed the installation procedures, refer to the *Adaptive Risk Manager Online Administrator's Guide* for information on how to use the Adaptive Risk Manager Online to create and manage the rules that evaluate a Web site's incoming traffic and initiate a response to meet the user's requirements.

The document is intended for integrators who deploy and integrate Adaptive Risk Manager Online to add multi-factor authentication to web applications.

Documentation

The Oracle Adaptive Access Manager 10g documentation includes the following:

- The Oracle® Adaptive Access Manager API Integration Guide, which provides information on natively integrating the client portion of the Adaptive Risk Manager Online solutions. In an API integration, the client application invokes the Adaptive Risk Manager Online APIs directly and manages the authentication and challenge flows.
- The Oracle® Adaptive Access Manager Database Installation Guide (Oracle), which provides information about installing the Adaptive Access Manager schema into an Oracle database. Access to the Adaptive Access Manager schema is a requirement of the Adaptive Access Manager Application Server, which hosts the Adaptive Strong Authenticator and the Adaptive Risk Manager. Note that the Adaptive Manager Access Manager schema needs to be installed into the Oracle database before proceeding to the installation of the proxy.
- The Oracle® Adaptive Access Manager Database Installation Guide for SQL Server 2005, which provides information about installing the Adaptive Access Manager schema into SQL Server 2005. Access to the Adaptive Access Manager schema is a requirement of the Adaptive Access Manager Application Server, which hosts the Adaptive Strong Authenticator and the Adaptive Risk Manager. Note that the Adaptive Manager Access Manager schema needs to be installed into SQL Server 2005 before proceeding to the installation of the proxy.
- The Oracle® Adaptive Access Manager Proxy Integration Guide, which provides programming information and instructions on the installation of the Adaptive Access Manager proxy, one of the components in the Adaptive Access Manager UIO deployment. The Oracle Adaptive Access Manager's Universal Installation Option (UIO) offers multi-factor authentication to Web applications without requiring any change to the application code. The Oracle® Adaptive Access Manager Proxy and The Oracle® Adaptive Access Manager Proxy Web Publishing Configuration are guides specific to the UIO deployment.

- The Oracle® Adaptive Access Manager Proxy Web Publishing Configuration, which provides information on creating web publishing rules and listeners so that Web applications and the WebUIO can be accessible from the Internet. The Oracle Adaptive Access Manager's Universal Installation Option (UIO) offers multi-factor authentication to Web applications without requiring any change to the application code. The Oracle® Adaptive Access Manager Proxy and The Oracle® Adaptive Access Manager Proxy Web Publishing Configuration are guides specific to the UIO deployment.
- The Oracle® Adaptive Risk Manager Online Installation Guide, which provides information on the installation of the administration user interface of Oracle Adaptive Access Manager. Adaptive Risk Manager Online is the administration user interface of Oracle Adaptive Access Manager, a set of web-based administration tools that provides sophisticated fraud monitoring, analysis, and tracking by user location, device, time of day, type of transaction, as well as a host of other factors, and evaluates these factors against a set of customizable rules.
- The Oracle® Adaptive Access Manager LDAP Configuration Guide, which provides information on how to configure the Oracle Adaptive Access Manager Application Server to allow a user to be authenticated via a user identifier and password. The intended audience of this manual are users of WebLogic and Tomcat who want to use LDAP to set up users instead of the functionality in WebLogic and Tomcat.
- The Oracle® Adaptive Access Manager Import/Export Manual, which provides information importing groups, rule templates, and models from the Adaptive Access Manager schema.
- The Oracle® Adaptive Risk Manager Online Customer Care API Guide, which provides information about the Adaptive Risk Manager Online Customer Care API and provides the XML definition for each of the APIs.
- The Oracle® Adaptive Access Manager Database Tables Archiving and Purging Procedure, which provides information on the purge and archive scripts in the Oracle Adaptive Access Manager Database Tables of Microsoft SQL Server 2005. The procedure to trigger the scripts and information on verification and validation of script results are also provided.
- The Oracle® Adaptive Access Manager SQL Server Maintenance Guide, which provides instructions to set up The Oracle Adaptive Access Manager Maintenance Plan to purge and archive scripts in the Oracle Adaptive Access Manager database tables of Microsoft SQL Server 2005. The manual also discusses in detail how to trigger the scripts and provides information on the verification and validation of script results.
- The Oracle® Adaptive Risk Manager™ Administrator's Guide, which provides step-by-step instructions for creating and managing groups, creating models that contain rules, and customizing and managing rules.
- The Oracle® Adaptive Risk Manager™ Dashboard and Reporting Guide, which provides detailed instructions on how to use the dashboard and reporting functionality within the Oracle® Adaptive Risk Manager Online. The Oracle® Adaptive Risk Manager Online includes a dashboard that provides a high-level overview of users and devices that have generated alerts and the alerts themselves, and it contains a comprehensive collection of reports on users, locations, devices, and security alerts.
- The Oracle® Adaptive Risk Manager™ Customer Care Administration Guide, which provides information on creating new customer cases and administering them.

Introduction

Adaptive Risk Manager Online is the administration user interface used to configure rules.

Adaptive Risk Manager Online provides sophisticated fraud monitoring, analysis, and tracking by user location, device, time of day, type of transaction, as well as a host of other factors, and evaluating these factors against a set of customizable rules.

The purpose of this manual is to guide you through the installation and configuration of Adaptive Risk Manager Online. The document is intended for integrators who deploy and integrate Adaptive Risk Manager Online to add multi-factor authentication to web applications.

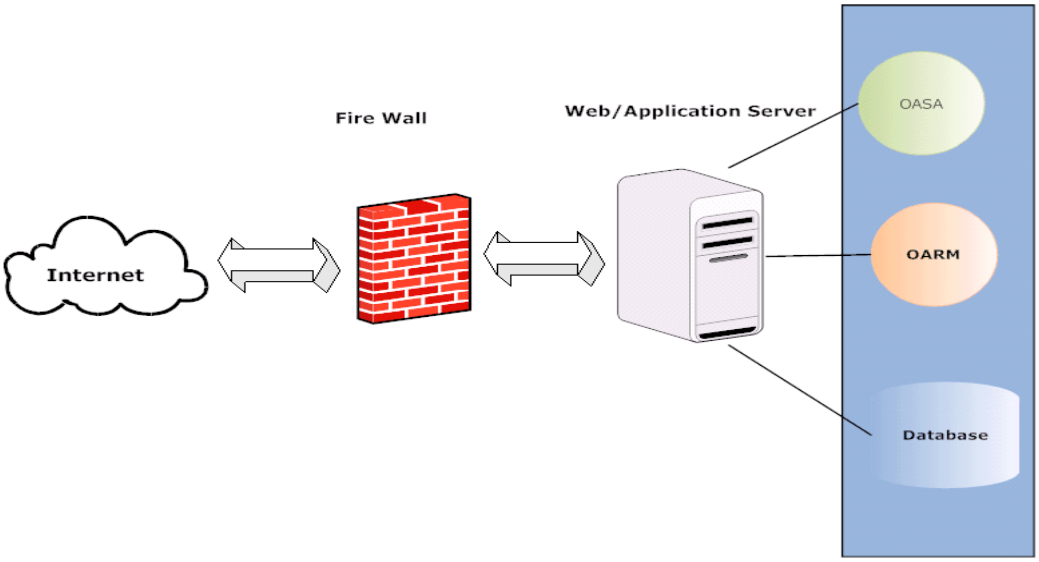
Architecture

The Adaptive Risk Manager Online solution can be deployed in various configurations.

Standard Deployments

Minimal Standard Deployment

The following illustrates a single-box solution in which the Adaptive Strong Authenticator and Adaptive Risk Manager Online are on the same server.

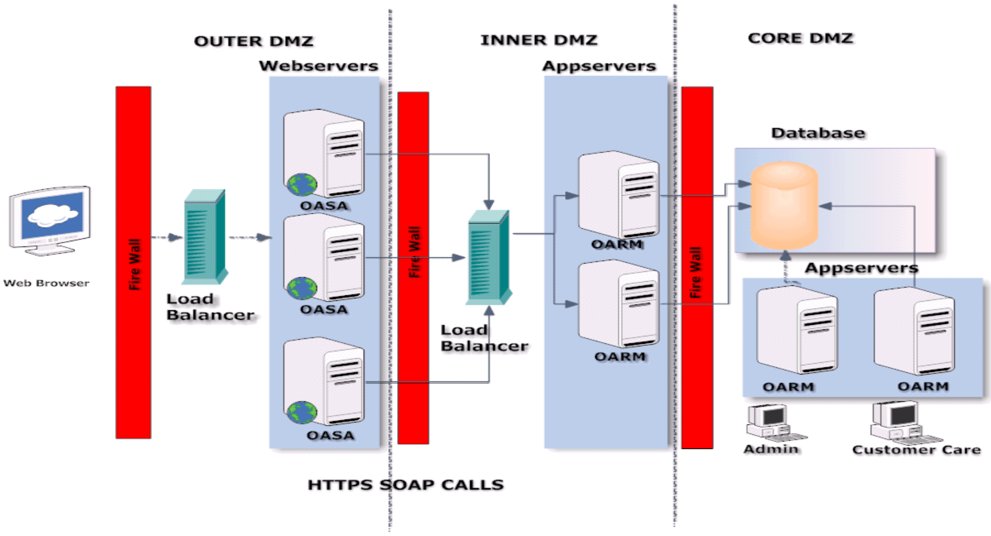


Optimal Standard Deployment

In the optimal standard deployment, the Adaptive Risk Manager Online solution is scaled independently and horizontally, with the Adaptive Risk Manager Online and database separated for performance, scalability and increased security.

High-End Standard Deployment

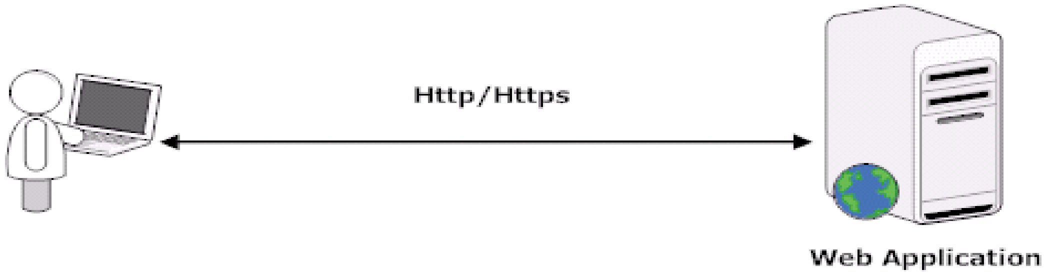
In the high-end standard deployment, the Adaptive Risk Manager Online is separated for performance and scalability, and horizontal scalability for the Adaptive Risk Manager Online and database. The Adaptive Risk Manager Online database is separated for stand-alone reporting and fraud analysis objectives.



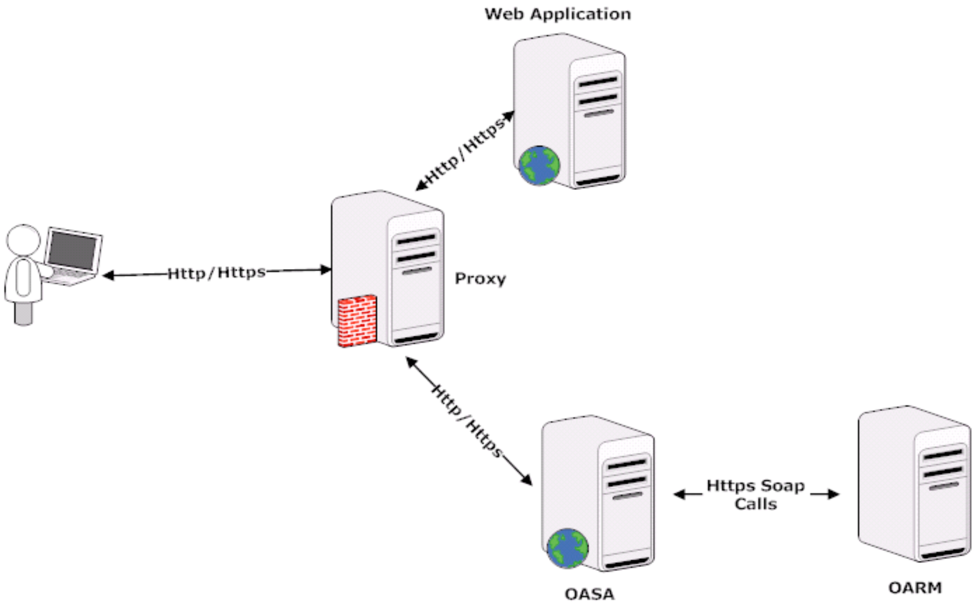
UIO Deployments

Oracle Adaptive Access Manager’s Universal Installation Option (UIO) is a proxy-based deployment of the Adaptive Risk Manager and Adaptive Strong Authenticator that requires little or no integration with enterprise applications.

The first diagram shows a Web application before deploying Adaptive Access Manager.



The second diagram shows an Adaptive Access Manager deployment.



A proxy intercepts site traffic and routes it through Adaptive Risk Manager Online for Strong Authentication.

For more information on the Adaptive Access Manager’s Universal Installation Option (UIO), refer to the *Oracle Adaptive Access Manager Proxy Integration Guide* and *Oracle Adaptive Access Manager Proxy Web Publishing Configuration*.

Minimal UIO Deployment

The minimal UIO deployment is a single-box solution where the UIO, Adaptive Strong Authenticator and Adaptive Risk Manager are on the same server.

Optimal UIO Deployment

In the optimal UIO deployment, the Adaptive Access Manager solution is scaled independently and horizontally, with the Adaptive Risk Manager and database separated for performance, scalability and increased security.

High-End UIO Deployment

In the high-end UIO deployment, the Adaptive Risk Manager is separated for performance and scalability, and horizontal scalability for the Adaptive Risk Manager and database. The Adaptive Risk Manager Online database is separated for stand-alone reporting and fraud analysis objectives.

Native and Web Services Integration Architecture

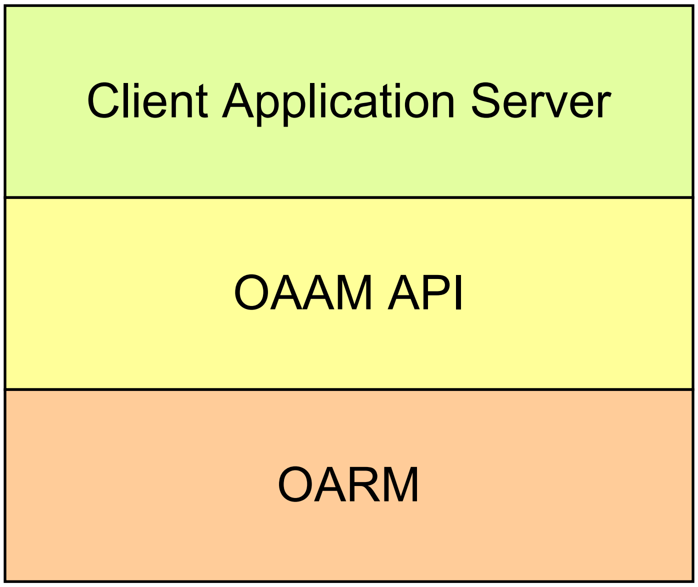
The web application communicates with Adaptive Risk Manager Online using the Adaptive Risk Manager Online Native Client API or via Web Services.

For more information on natively integrating the client portion of the Adaptive Risk Manager Online, refer to the *Oracle® Adaptive Access Manager API Integration Guide*.

Static Linked Integration

The native API is a wrapper over the SOAP API that is published by the Adaptive Risk Manager Online Server and written in the client's native application language. An optional interface, it provides the integrator with procedures to use to link into the application server code.

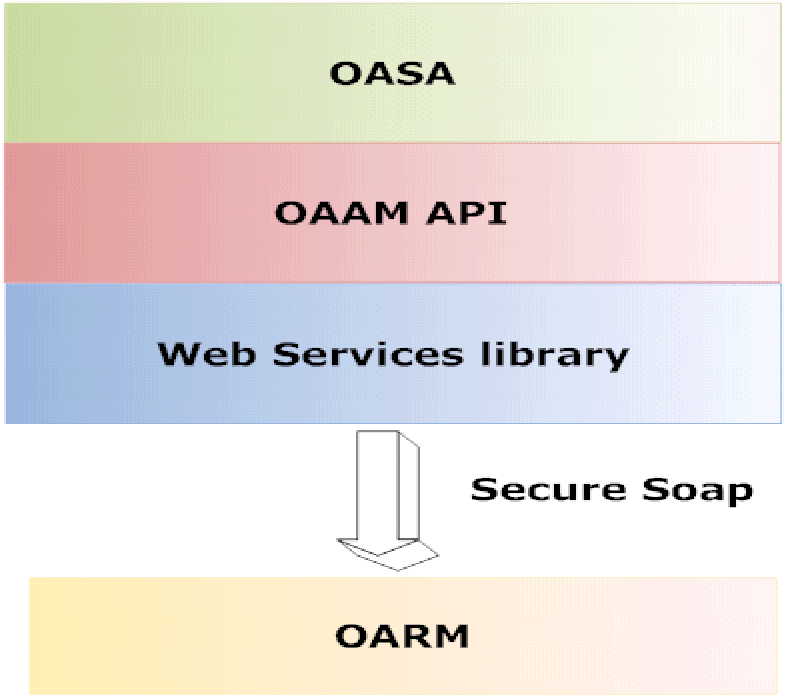
In the Native Integration Option, which is shown below, the Adaptive Risk Manager Online Native Client API (which is statically integrated with the Adaptive Risk Manager Online library) is used to call the Application Server Code.



Web Services Integration

The Web Services Wrapper are libraries that have utility methods which make direct SOAP calls to call the Application Server Code.

In the Web Service Wrapper option, which is shown below, the user decides to use his own secure SOAP library and Web services library, which are integrated with Adaptive Risk Manager Online, to call the Adaptive Risk Manager Online Server.



Getting Started

RAM

1.5 GB Minimum

Database

- Oracle 9i or later
- MySQL 2005

Application Server

- Oracle Application Server
- WebLogic
- WebSphere
- Tomcat
- Pramati
- MSSQL server

Software

- JDK 1.5 or later
- JDBC driver

Operating System

- Redhat Linux
- Windows XP or later
- Solaris
- HP-UX
- AIX

Performance

Note: You must restart the machine in order for some of the settings to take effect.

JVM Settings

The Minimum Memory setting is 1024 MB.

For high volume deployments, please perform load testing to come up with ideal settings.

IP Intelligence License

Adaptive Access Manager integrates with numerous IP Intelligence products due to our open API's. Common IP Intelligence products include:

- Quova
- IP2Location
- Digital Envoy

TCP/IP Parameters

For windows based deployments, the following TCP/IP parameters are highly recommended:

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\
```

TcpTimedWaitDelay= 1e

MaxUserPort = ffff

Prerequisites and Dependencies

The prerequisites and dependencies for the installation and configuration of Adaptive Risk Manager Online are summarized in the table below.

Prerequisites and Dependencies	Descriptions
Java	Java Runtime Environment, version 1.5 or higher, needs to be installed. Environment variables JAVA_HOME and PATH must be set appropriately.
Database	The Adaptive Risk Manager Online Server needs access to the database server that contains the Adaptive Risk Manager Online schema and it needs to be populated with some initial data. Follow the instructions in the *Oracle Adaptive Access Manager Database Installation Guide for Oracle* or the *Oracle Adaptive Access Manager Database Installation Guide for SQL Server* for creating the Adaptive Risk Manager Online schema and populating it with the default values. Note: Any failover, clustering, and replication technology for the database is supported in Adaptive Risk Manager Online. To load data to Microsoft SQL Server database, sqljdbc.jar should be copied to a third-party directory. This file can be freely downloaded from Microsoft at http://www.microsoft.com/downloads/details.aspx?FamilyID=6d483869-816a-44cb-9787-a866235efc7c&DisplayLang=en.
File Write Permission	The Adaptive Risk Manager Online Server writes activity logs to rolling log files. The verbosity of the logs can optionally be configured using standard log4j.xml configuration. For more information on setting up logging, refer to the “Setting Up Logging” section of this manual.
Shared Images Directory	If personalized authentication devices are used, it is recommended that all Adaptive Risk Manager Online Application servers have access to the directories containing the images and that they be on a shared drive. If this is not feasible, please duplicate the image files on each server. Note that the base paths must be identical on all machines that will render the images, including the client applications. For more information on setting up background images, refer to the “Setting Up Background Images” section of this manual.
Port Configuration	Ensure that the port used by the Adaptive Risk Manager Online Application Server is accessible to the client machine. You are allowed to configure the port number.

Deploying Oracle Adaptive Risk Manager Online

Adaptive Risk Manager Online provides sophisticated fraud monitoring, analysis, and tracking.

Adaptive Risk Manager Online includes the Adaptive Strong Authenticator, which provides authentication and authorization services to any web application and can be deployed in most industry-standard J2EE containers.

This section provides instructions for the deployment and installation of Adaptive Risk Manager Online (and its components) into the following application servers.

- Oracle Application Server 10g
- WebLogic
- Tomcat 5.5.xx
- Websphere 6.1

WebLogic and Tomcat users who want to use LDAP to set up users instead of the functionality in WebLogic and Tomcat, refer to the *Oracle Adaptive Access Manager LDAP Configuration Guide*, which provides information on how to configure the Adaptive Risk Manager Online Application Server to allow a user to be authenticated via a user identifier and password.

Note: Because of licensing, the sqljdbc.jar (for Microsoft SQL Server Database) and other jars to support various functionalities of Adaptive Risk Manager Online need to be downloaded separately.

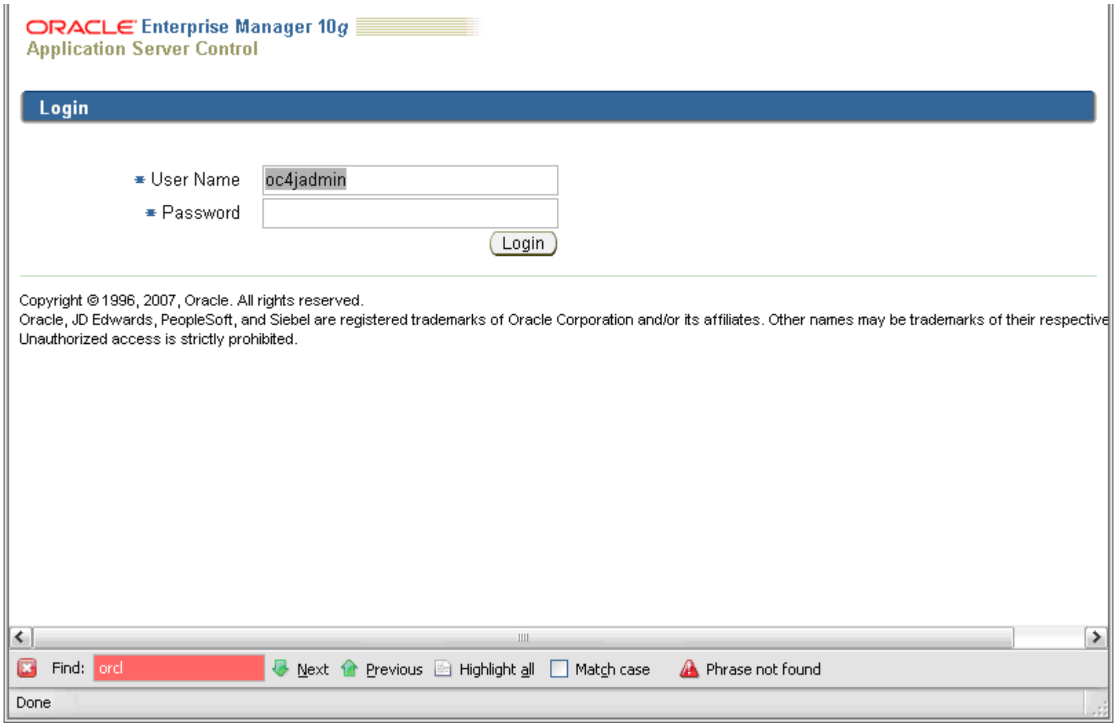
Oracle 10g Application Server

The Oracle Containers for J2EE (OC4J) installation provides an HTTP/S server, all of the required J2EE 1.4 APIs and services, a complete EJB 3.0 and JPA implementation, Oracle TopLink, extensive Web Services capabilities and the browser-based Application Server Control Console management interface to configure the server and deploy the Adaptive Risk Manager Online.

Installing Adaptive Risk Manager Online into Oracle Application Server

1. Install the Oracle Application Server. For detailed information about how to install the Oracle Application server, refer to the *Oracle Application Server Installation Guide*.
2. Log in to the **Oracle Application Server Console** using an Admin user.

   For example, oc4jadmin/<password>.
3. Log in to the **Enterprise Application Server Control**.



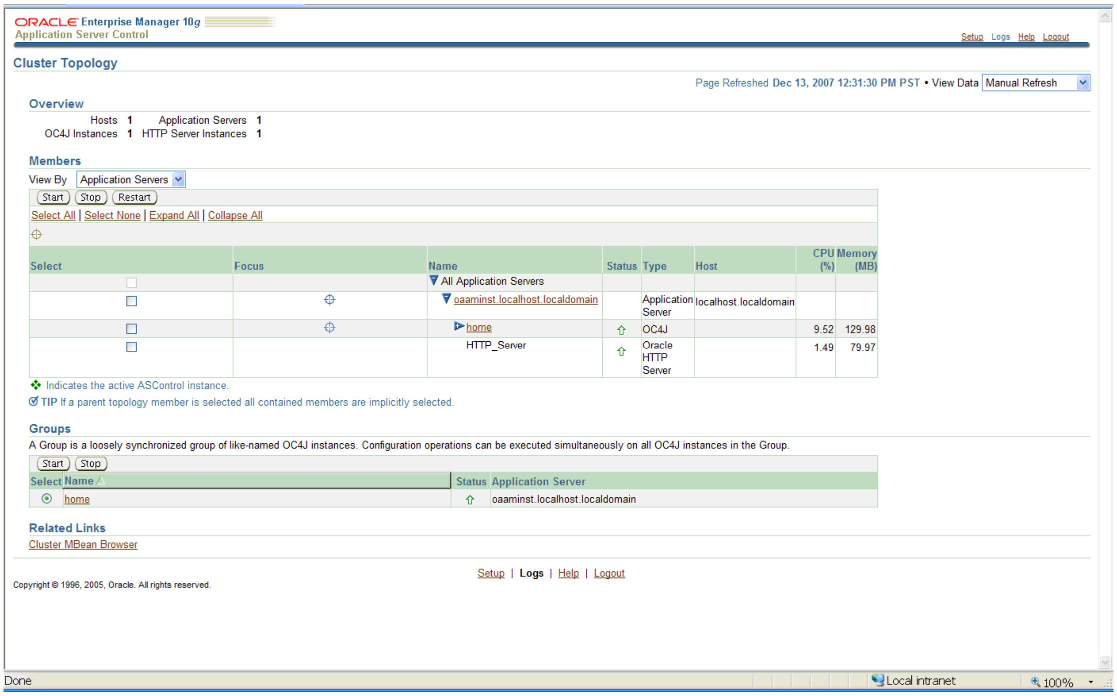
* User Name: oc4jadmin

* Password:

Find: orcl

Copyright © 1996, 2007, Oracle. All rights reserved.
Oracle, JD Edwards, PeopleSoft, and Siebel are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective
Unauthorized access is strictly prohibited.

4. When the **Cluster Topology** page appears, click the **home** link to navigate to the OC4J page.



ORACLE Enterprise Manager 10g
Application Server Control
Setup Logs Help Logout

Cluster Topology

Page Refreshed Dec 13, 2007 12:31:30 PM PST • View Data Manual Refresh

Overview

Hosts	1	Application Servers	1
OC4J Instances	1	HTTP Server Instances	1

Members

View By Application Servers

Start Stop Restart
Select All | Select None | Expand All | Collapse All

Select	Focus	Name	Status	Type	Host	CPU (%)	Memory (MB)
□		All Application Servers					
□	⌖	oaaminst.localhost.localdomain		Application Server	localhost.localdomain		
□	⌖	home	⇧	OC4J		9.52	129.98
□		HTTP_Server	⇧	Oracle HTTP Server		1.49	79.97

Indicates the active ASControl instance.

TIP If a parent topology member is selected all contained members are implicitly selected.

Groups

A Group is a loosely synchronized group of like-named OC4J instances. Configuration operations can be executed simultaneously on all OC4J instances in the Group.

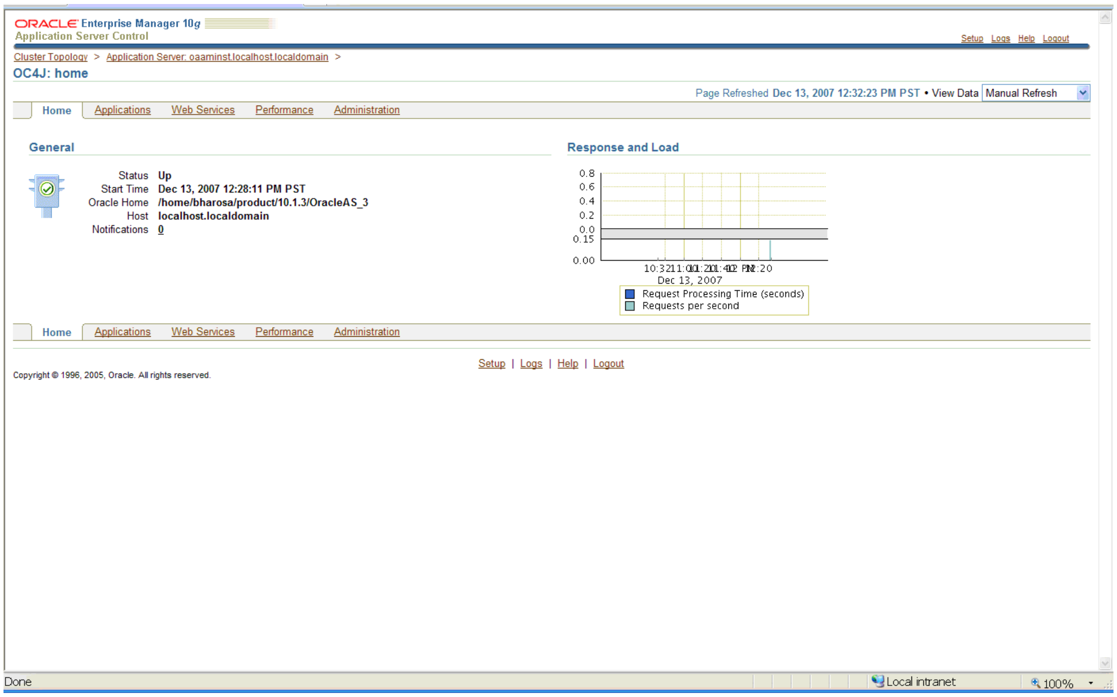
Select	Name	Status	Application Server
●	home	⇧	oaaminst.localhost.localdomain

Related Links

Cluster MBean Browser

Copyright © 1996, 2005, Oracle. All rights reserved.

5. On the **OC4J home** page, click the **Application** tab to display the **Application** page.


ORACLE Enterprise Manager 10g
Application Server Control
Setup Logs Help Logout
Cluster Topology > Application Server: oaaminst.localhost.localdomain >
Home
Applications
Web Services
Performance
Administration
Response and Load
0.8
0.6
0.4
0.2
0.0
0.15
0.00
10:3211:0011:2011:40 PM 12:20
Dec 13, 2007
Request Processing Time (seconds)
Requests per second
Setup | Logs | Help | Logout
Done
Local intranet
100%

OC4J: home

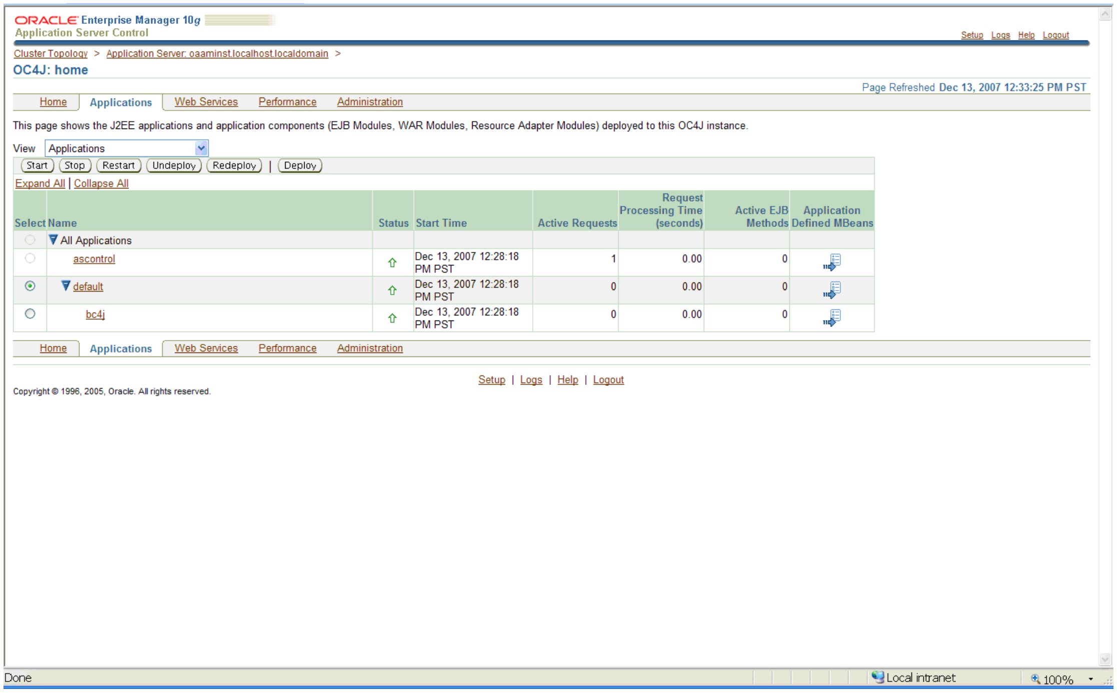
Page Refreshed Dec 13, 2007 12:32:23 PM PST • View Data Manual Refresh

General

Status Up
Start Time Dec 13, 2007 12:28:11 PM PST
Oracle Home /home/bharosa/product/10.1.3/OracleAS_3
Host localhost.localdomain
Notifications 0

Copyright © 1996, 2005, Oracle. All rights reserved.

6. Then, click the **Deploy** button.


ORACLE Enterprise Manager 10g
Application Server Control
Setup Logs Help Logout
Cluster Topology > Application Server: oaaminst.localhost.localdomain >
Home
Applications
Web Services
Performance
Administration
Start
Stop
Restart
Undeploy
Redeploy
Deploy
Expand All | Collapse All
Setup | Logs | Help | Logout
Done
Local intranet
100%

OC4J: home

Page Refreshed Dec 13, 2007 12:33:25 PM PST

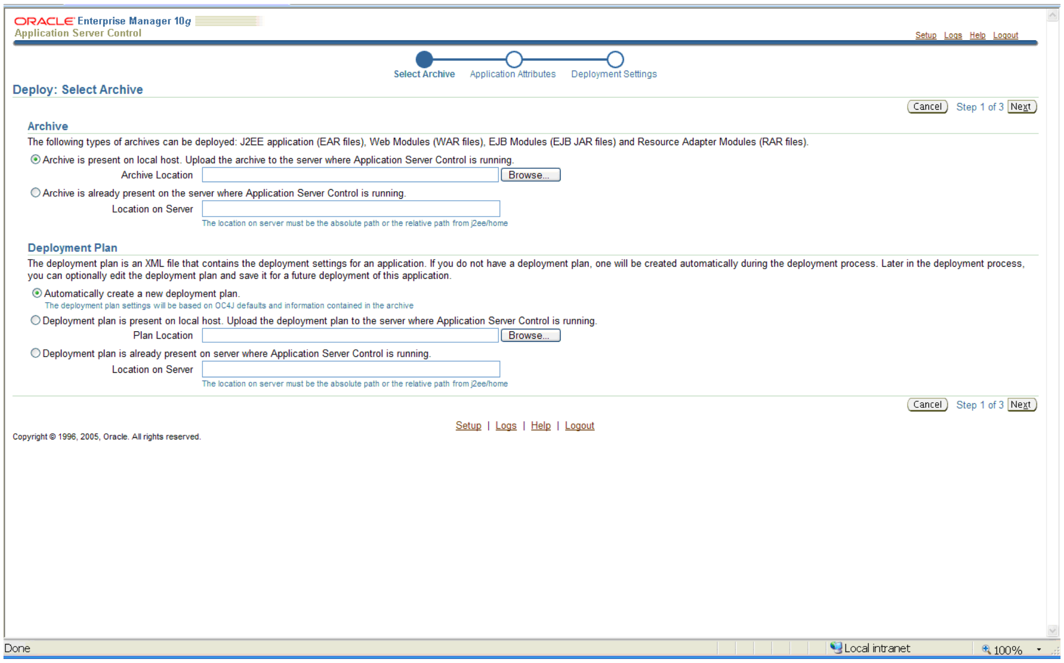
This page shows the J2EE applications and application components (EJB Modules, WAR Modules, Resource Adapter Modules) deployed to this OC4J instance.

View Applications

Select	Name	Status	Start Time	Active Requests	Request Processing Time (seconds)	Active EJB Methods	Application Defined MBeans
○	All Applications						
○	ascontrol	⇧	Dec 13, 2007 12:28:18 PM PST	1	0.00	0	
●	default	⇧	Dec 13, 2007 12:28:18 PM PST	0	0.00	0	
○	bc4j	⇧	Dec 13, 2007 12:28:18 PM PST	0	0.00	0	

Copyright © 1996, 2005, Oracle. All rights reserved.

7. On the **Select Archive** page, enter the war file and its location. Then, click **Next**.



Deploy: Select Archive

Cancel Step 1 of 3 Next

Archive

The following types of archives can be deployed: J2EE application (EAR files), Web Modules (WAR files), EJB Modules (EJB JAR files) and Resource Adapter Modules (RAR files).

● Archive is present on local host. Upload the archive to the server where Application Server Control is running.

Archive Location [ ] Browse...

○ Archive is already present on the server where Application Server Control is running.

Location on Server [ ]

The location on server must be the absolute path or the relative path from j2ee/home

Deployment Plan

The deployment plan is an XML file that contains the deployment settings for an application. If you do not have a deployment plan, one will be created automatically during the deployment process. Later in the deployment process, you can optionally edit the deployment plan and save it for a future deployment of this application.

● Automatically create a new deployment plan.

The deployment plan settings will be based on OC4J defaults and information contained in the archive

○ Deployment plan is present on local host. Upload the deployment plan to the server where Application Server Control is running.

Plan Location [ ] Browse...

○ Deployment plan is already present on server where Application Server Control is running.

Location on Server [ ]

The location on server must be the absolute path or the relative path from j2ee/home

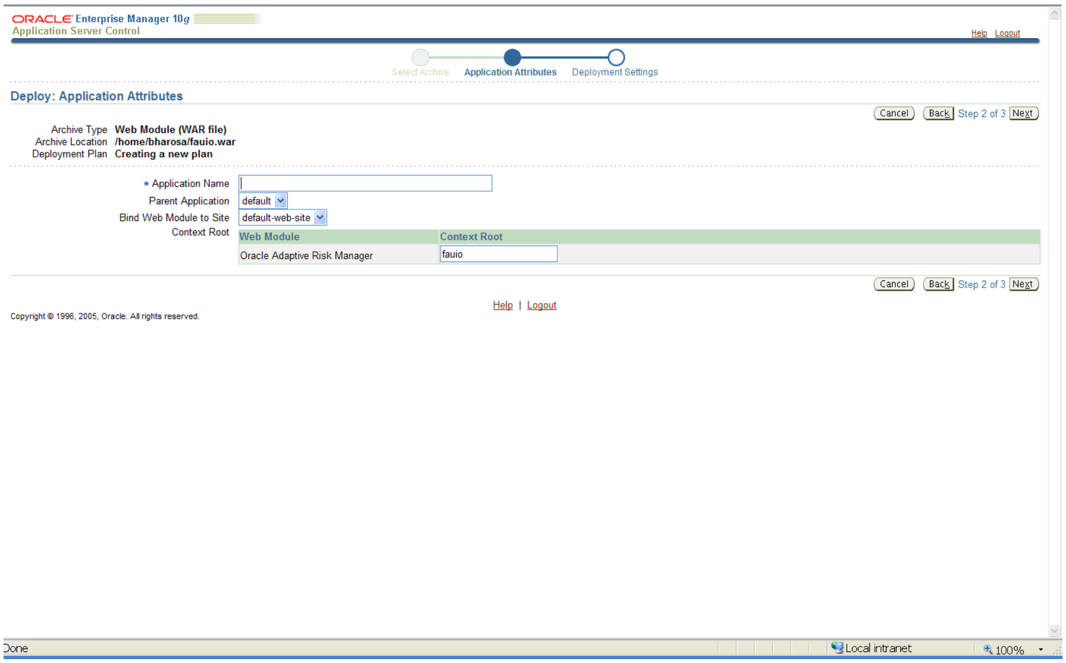
Cancel Step 1 of 3 Next

Setup | Logs | Help | Logout

Copyright © 1996, 2005, Oracle. All rights reserved.

8. On the **Application Attributes** page, enter the application name and context root. Then click **Next**.

   For example, the value for **Application Name** and **Context Root** could be oaam.



Deploy: Application Attributes

Cancel Back Step 2 of 3 Next

Archive Type	**Web Module (WAR file)**
Archive Location	**/home/bharosa/fauio.war**
Deployment Plan	**Creating a new plan**

* Application Name [ ]

Parent Application: default

Bind Web Module to Site: default-web-site

Context Root

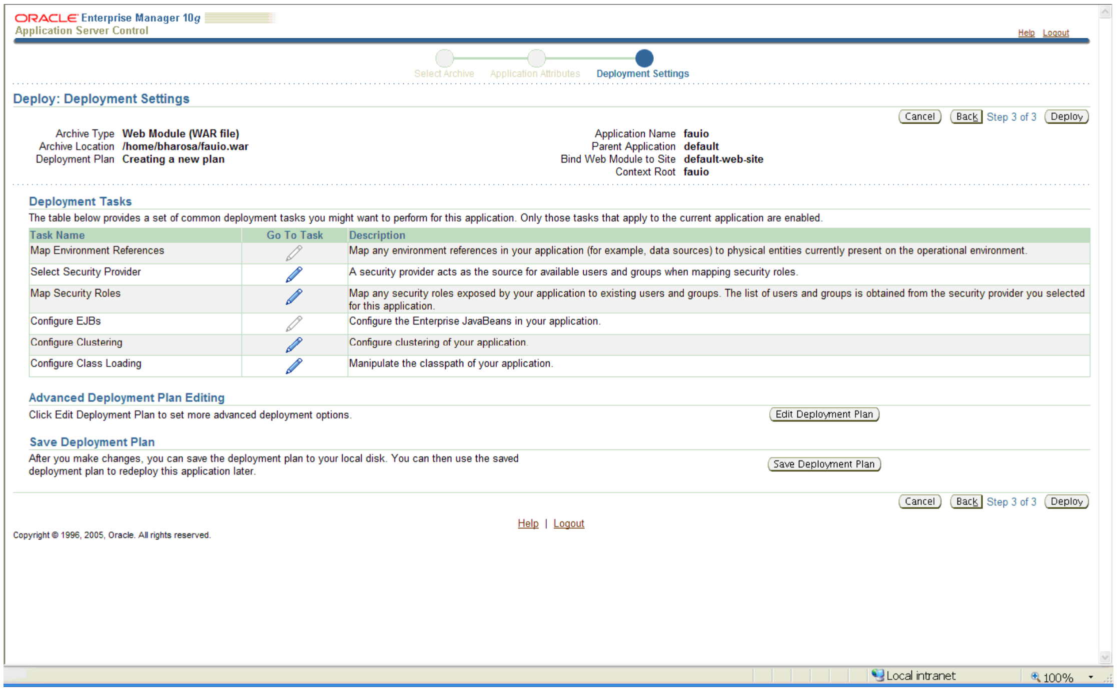
Web Module	Context Root
Oracle Adaptive Risk Manager	fauio

Cancel Back Step 2 of 3 Next

Help | Logout

Copyright © 1996, 2005, Oracle. All rights reserved.

9. On **Deployment Settings** page, click the **Go to Task** link next to **Configure Class Loading** to modify application class loading configuration.



Deploy: Deployment Settings

Archive Type **Web Module (WAR file)**
Archive Location **/home/bharosa/fauio.war**
Deployment Plan **Creating a new plan**

Application Name **fauio**
Parent Application **default**
Bind Web Module to Site **default-web-site**
Context Root **fauio**

Deployment Tasks

The table below provides a set of common deployment tasks you might want to perform for this application. Only those tasks that apply to the current application are enabled.

Task Name	Go To Task	Description
Map Environment References	✎	Map any environment references in your application (for example, data sources) to physical entities currently present on the operational environment.
Select Security Provider	✎	A security provider acts as the source for available users and groups when mapping security roles.
Map Security Roles	✎	Map any security roles exposed by your application to existing users and groups. The list of users and groups is obtained from the security provider you selected for this application.
Configure EJBs	✎	Configure the Enterprise JavaBeans in your application.
Configure Clustering	✎	Configure clustering of your application.
Configure Class Loading	✎	Manipulate the classpath of your application.

Advanced Deployment Plan Editing

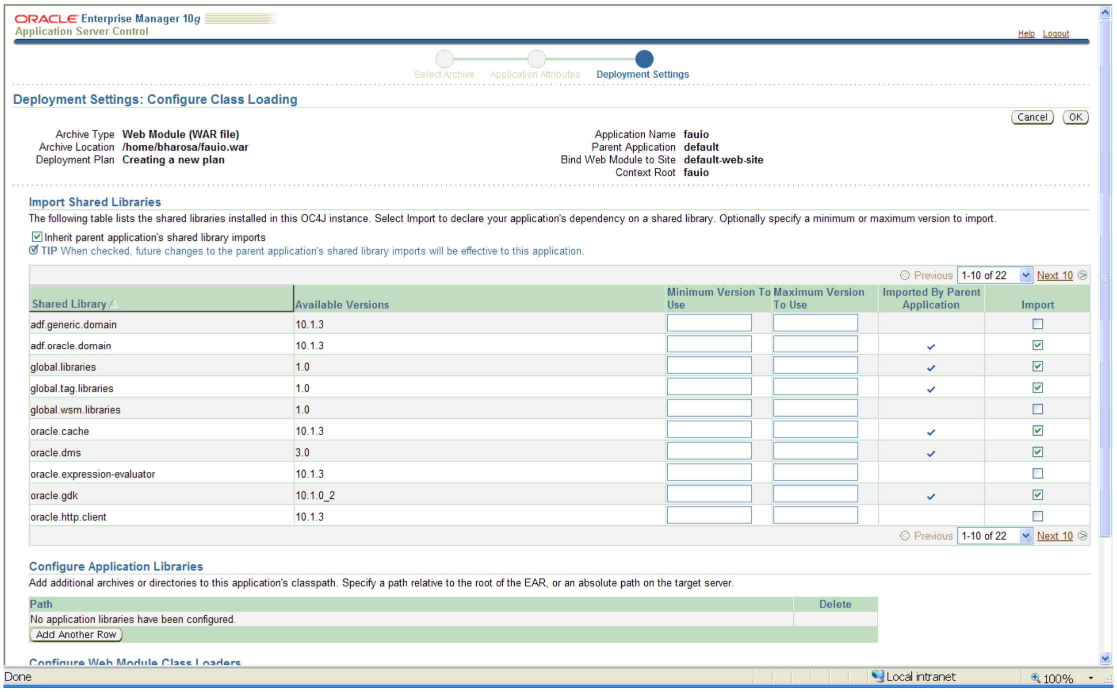
Click Edit Deployment Plan to set more advanced deployment options.

Save Deployment Plan

After you make changes, you can save the deployment plan to your local disk. You can then use the saved deployment plan to redeploy this application later.

Copyright © 1996, 2005, Oracle. All rights reserved.

10. When the **Configure Class Loading** page is displayed, check **Search Local Classes First** under **Configure Web Module Class Loaders**; then, click **OK**..



Deployment Settings: Configure Class Loading

Archive Type	**Web Module (WAR file)**	Application Name	**fauio**
Archive Location	**/home/bharosa/fauio.war**	Parent Application	**default**
Deployment Plan	**Creating a new plan**	Bind Web Module to Site	**default-web-site**
		Context Root	**fauio**

Import Shared Libraries

The following table lists the shared libraries installed in this OC4J instance. Select Import to declare your application's dependency on a shared library. Optionally specify a minimum or maximum version to import.

☑ Inherit parent application's shared library imports

TIP When checked, future changes to the parent application's shared library imports will be effective to this application.

Shared Library	Available Versions	Minimum Version To Use	Maximum Version To Use	Imported By Parent Application	Import
adf.generic.domain	10.1.3				☐
adf.oracle.domain	10.1.3			✓	☑
global.libraries	1.0			✓	☑
global.tag.libraries	1.0			✓	☑
global.wsm.libraries	1.0				☐
oracle.cache	10.1.3			✓	☑
oracle.dms	3.0			✓	☑
oracle.expression-evaluator	10.1.3				☐
oracle.gdk	10.1.0_2			✓	☑
oracle.http.client	10.1.3				☐

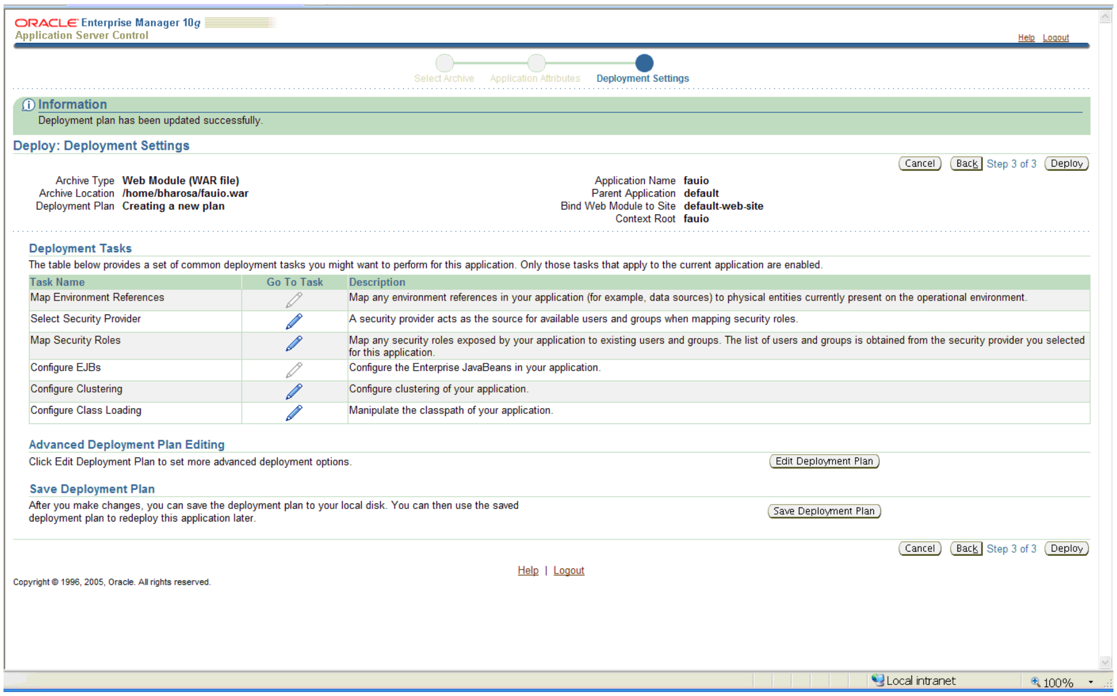
Configure Application Libraries

Add additional archives or directories to this application's classpath. Specify a path relative to the root of the EAR, or an absolute path on the target server.

Path	Delete
No application libraries have been configured.	

Configure Web Module Class Loaders

11. Now, click the **Deploy** button.



Information

Deployment plan has been updated successfully.

Deploy: Deployment Settings

Archive Type	**Web Module (WAR file)**	Application Name	**fauio**
Archive Location	**/home/bharosa/fauio.war**	Parent Application	**default**
Deployment Plan	**Creating a new plan**	Bind Web Module to Site	**default-web-site**
		Context Root	**fauio**

Deployment Tasks

The table below provides a set of common deployment tasks you might want to perform for this application. Only those tasks that apply to the current application are enabled.

Task Name	Go To Task	Description
Map Environment References	✎	Map any environment references in your application (for example, data sources) to physical entities currently present on the operational environment.
Select Security Provider	✎	A security provider acts as the source for available users and groups when mapping security roles.
Map Security Roles	✎	Map any security roles exposed by your application to existing users and groups. The list of users and groups is obtained from the security provider you selected for this application.
Configure EJBs	✎	Configure the Enterprise JavaBeans in your application.
Configure Clustering	✎	Configure clustering of your application.
Configure Class Loading	✎	Manipulate the classpath of your application.

Advanced Deployment Plan Editing

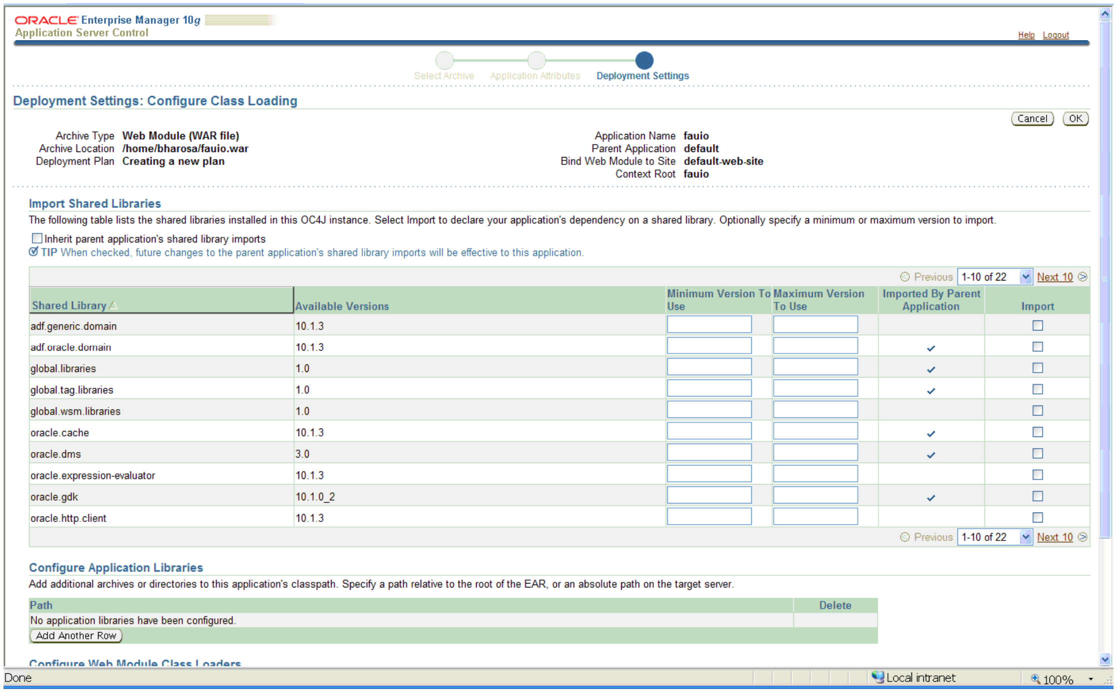
Click Edit Deployment Plan to set more advanced deployment options.

Save Deployment Plan

After you make changes, you can save the deployment plan to your local disk. You can then use the saved deployment plan to redeploy this application later.

Copyright © 1996, 2005, Oracle. All rights reserved.

12. Click **OK**.



Deployment Settings: Configure Class Loading

Archive Type	**Web Module (WAR file)**	Application Name	**fauio**
Archive Location	**/home/bharosa/fauio.war**	Parent Application	**default**
Deployment Plan	**Creating a new plan**	Bind Web Module to Site	**default-web-site**
		Context Root	**fauio**

Import Shared Libraries

The following table lists the shared libraries installed in this OC4J instance. Select Import to declare your application's dependency on a shared library. Optionally specify a minimum or maximum version to import.

□ Inherit parent application's shared library imports

TIP When checked, future changes to the parent application's shared library imports will be effective to this application.

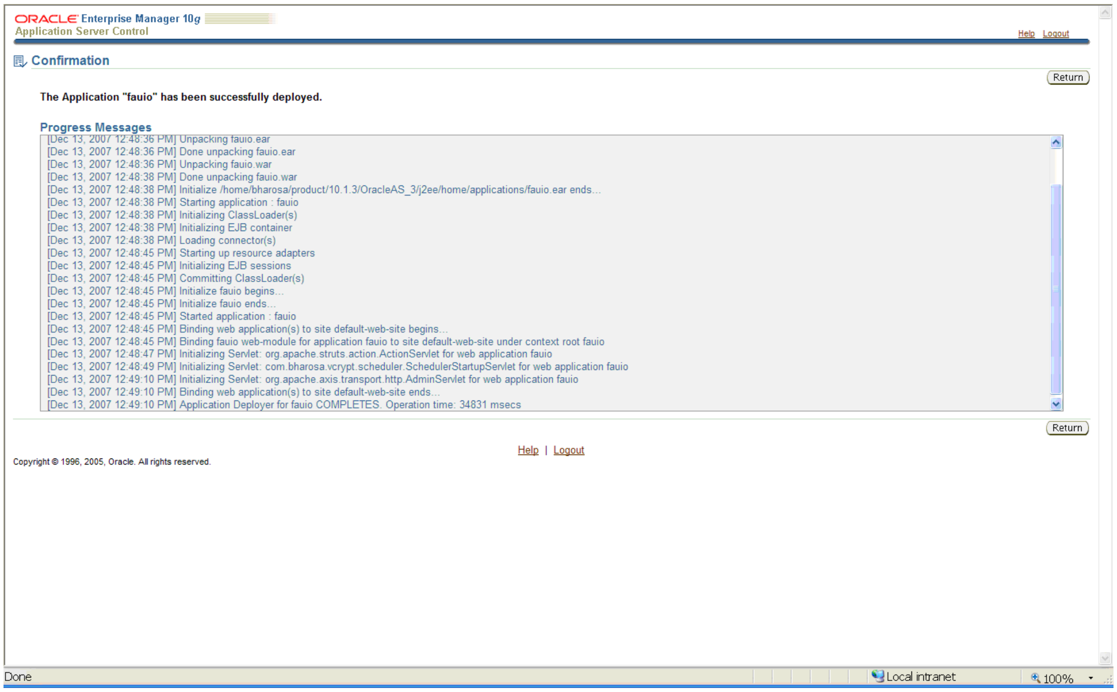
Shared Library	Available Versions	Minimum Version To Use	Maximum Version To Use	Imported By Parent Application	Import
adf.generic.domain	10.1.3				□
adf.oracle.domain	10.1.3			✓	□
global.libraries	1.0			✓	□
global.tag.libraries	1.0			✓	□
global.wsm.libraries	1.0				□
oracle.cache	10.1.3			✓	□
oracle.dms	3.0			✓	□
oracle.expression-evaluator	10.1.3				□
oracle.gdk	10.1.0_2			✓	□
oracle.http.client	10.1.3				□

Configure Application Libraries

Add additional archives or directories to this application's classpath. Specify a path relative to the root of the EAR, or an absolute path on the target server.

Path	Delete
No application libraries have been configured.	

The confirmation screen appears.



Confirmation

The Application "fauio" has been successfully deployed.

Progress Messages

```
[Dec 13, 2007 12:48:36 PM] Unpacking fauio.ear
[Dec 13, 2007 12:48:36 PM] Done unpacking fauio.ear
[Dec 13, 2007 12:48:36 PM] Unpacking fauio.war
[Dec 13, 2007 12:48:38 PM] Done unpacking fauio.war
[Dec 13, 2007 12:48:38 PM] Initialize /home/bharosa/product/10.1.3/OracleAS_3/j2ee/home/applications/fauio.ear ends...
[Dec 13, 2007 12:48:38 PM] Starting application : fauio
[Dec 13, 2007 12:48:38 PM] Initializing ClassLoader(s)
[Dec 13, 2007 12:48:38 PM] Initializing EJB container
[Dec 13, 2007 12:48:38 PM] Loading connector(s)
[Dec 13, 2007 12:48:45 PM] Starting up resource adapters
[Dec 13, 2007 12:48:45 PM] Initializing EJB sessions
[Dec 13, 2007 12:48:45 PM] Committing ClassLoader(s)
[Dec 13, 2007 12:48:45 PM] Initialize fauio begins...
[Dec 13, 2007 12:48:45 PM] Initialize fauio ends...
[Dec 13, 2007 12:48:45 PM] Started application : fauio
[Dec 13, 2007 12:48:45 PM] Binding web application(s) to site default-web-site begins...
[Dec 13, 2007 12:48:45 PM] Binding fauio web-module for application fauio to site default-web-site under context root fauio
[Dec 13, 2007 12:48:47 PM] Initializing Servlet: org.apache.struts.action.ActionServlet for web application fauio
[Dec 13, 2007 12:48:49 PM] Initializing Servlet: com.bharosa.vcrypt.scheduler.SchedulerStartupServlet for web application fauio
[Dec 13, 2007 12:49:10 PM] Initializing Servlet: org.apache.axis.transport.http.AdminServlet for web application fauio
[Dec 13, 2007 12:49:10 PM] Binding web application(s) to site default-web-site ends...
[Dec 13, 2007 12:49:10 PM] Application Deployer for fauio COMPLETES. Operation time: 34831 msecs
```

Copyright © 1996, 2005, Oracle. All rights reserved.

13. Now, navigate to OAAM deployment webapp directory to configure the JDBC url (sessions.xml) and logging (log4j.xml).

    For example : $OC4J_HOME/J2EE/home/applications/oaam/oaam/WEB-INF/classes.

Once configuration is completed please restart your Oracle Application Server using the “opmnctl“ command

Check your Web application using

http://<hostname>:<port>/<webappname>

For Example : http://<local host>:7777/oaam

Creating Groups and Adding Users

1. Enable security by commenting out the following lines from bharosa_server.properties:

   #vcrypt.web.security.access.flag=false

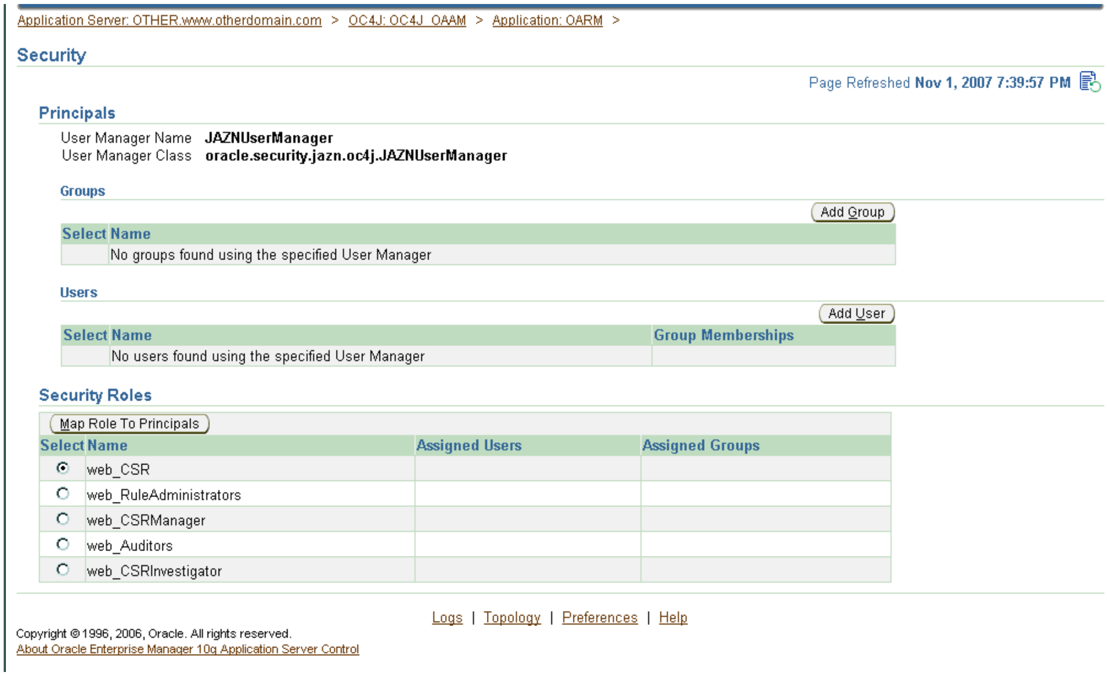
   #security.check.flag = false

2. Comment out the following section from **web.xml** to enable security contraints:

```
<!--
    <login-config>
        <auth-method>FORM</auth-method>
        <form-login-config>
            <form-login-page>/securedLogin.jsp</form-login-page>
            <form-error-page>/securedLoginError.jsp</form-error-page>
        </form-login-config>
    </login-config>


-->
```

3. Restart the OC4J_OAAM instance.
4. Go to **Application: OARM** page.



Application Server: OTHER.www.otherdomain.com > OC4J: OC4J_OAAM > Application: OARM >

Security

Page Refreshed **Nov 1, 2007 7:39:57 PM**

Principals

User Manager Name **JAZNUserManager**
User Manager Class **oracle.security.jazn.oc4j.JAZNUserManager**

Groups

Select	Name
	No groups found using the specified User Manager

Users

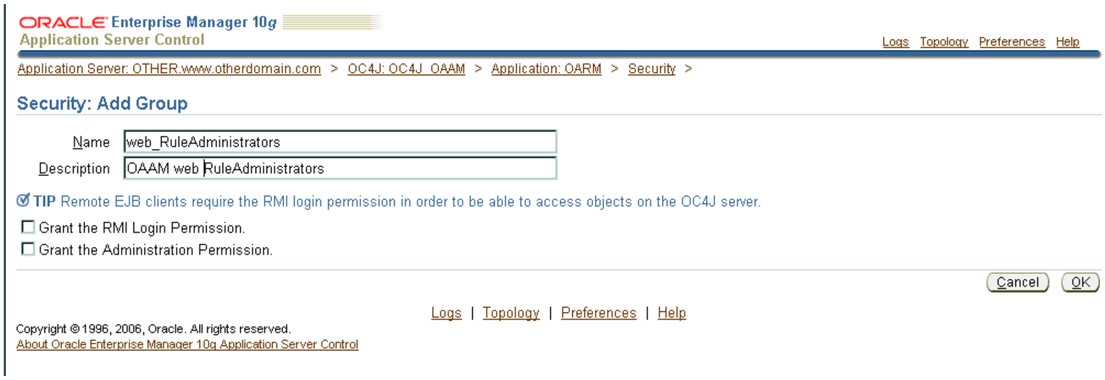
Select	Name	Group Memberships
	No users found using the specified User Manager	

Security Roles

Select	Name	Assigned Users	Assigned Groups
●	web_CSR		
○	web_RuleAdministrators		
○	web_CSRManager		
○	web_Auditors		
○	web_CSRInvestigator		

About Oracle Enterprise Manager 10g Application Server Control

5. Add the **Web_RuleAdministrators** group and click **OK**.
6. Similarly, create the **web_CSRManager**, **web_CSR**, and **web_Auditors** groups.


ORACLE Enterprise Manager 10g
Application Server Control
Logs Topology Preferences Help
Cancel
OK
Logs | Topology | Preferences | Help

Application Server: OTHER.www.otherdomain.com > OC4J: OC4J_OAAM > Application: OARM > Security >

Security: Add Group

Name: web_RuleAdministrators

Description: OAAM web RuleAdministrators

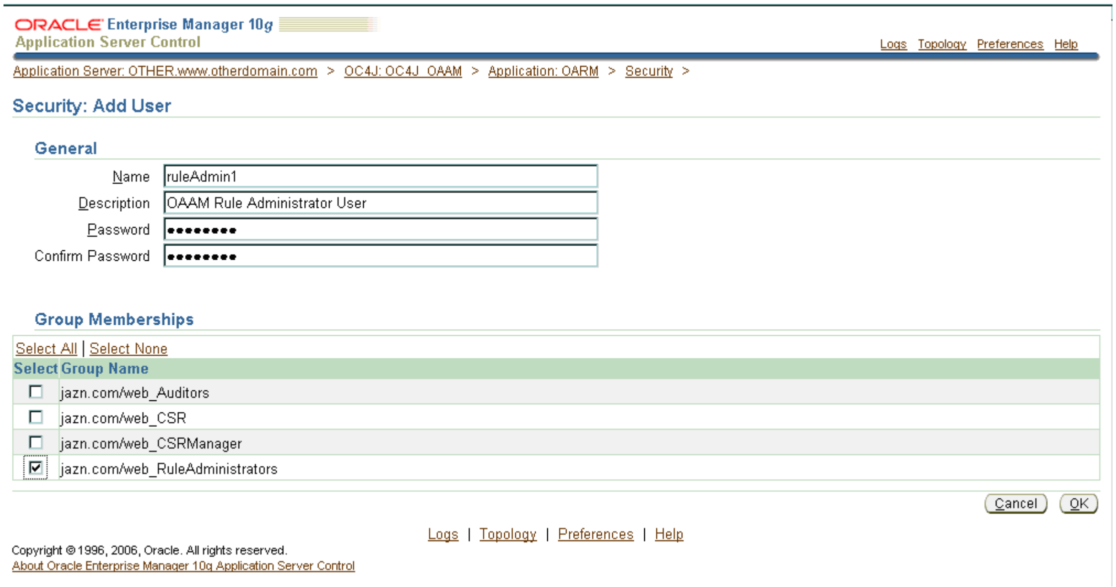
TIP Remote EJB clients require the RMI login permission in order to be able to access objects on the OC4J server.

□ Grant the RMI Login Permission.

□ Grant the Administration Permission.

Copyright © 1996, 2006, Oracle. All rights reserved.
About Oracle Enterprise Manager 10g Application Server Control

7. Add the user by entering the name (user name), description, and password .
8. Select the group that this user belongs to and click **OK**. In the example below, RuleAdmin1 belongs to the web-ruleadministrators group.
9. Similarly, create other users


ORACLE Enterprise Manager 10g
Application Server Control
Logs Topology Preferences Help
Select All | Select None
Cancel
OK
Logs | Topology | Preferences | Help

Application Server: OTHER.www.otherdomain.com > OC4J: OC4J_OAAM > Application: OARM > Security >

Security: Add User

General

Name: ruleAdmin1

Description: OAAM Rule Administrator User

Password: ••••••••

Confirm Password: ••••••••

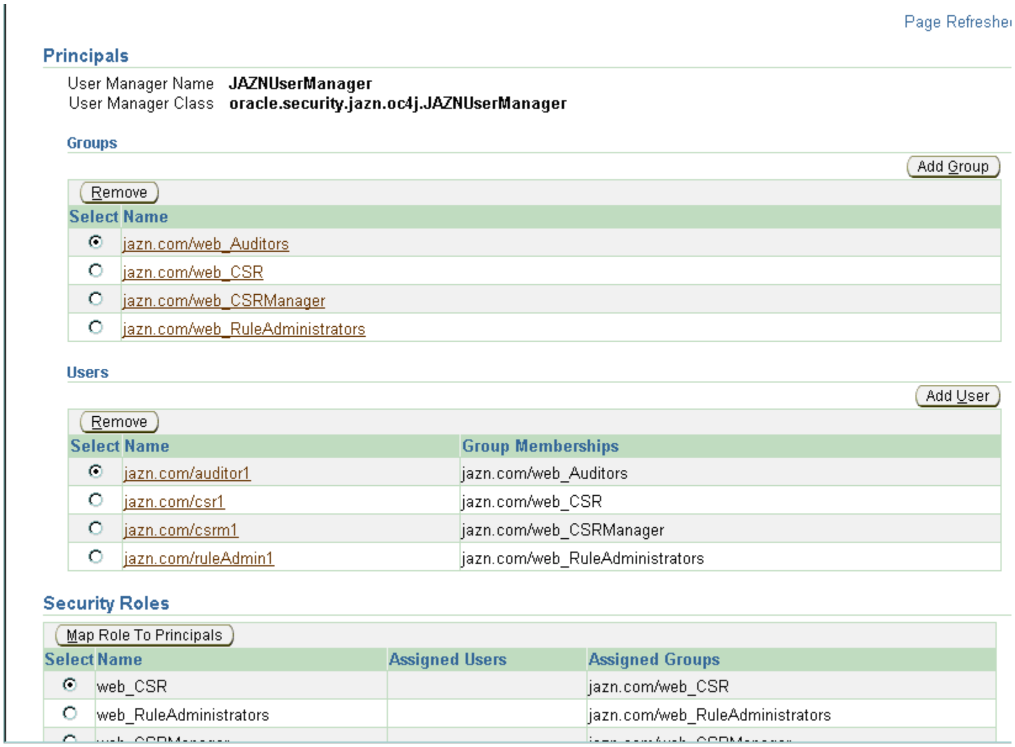
Group Memberships

Select	Group Name
□	jazn.com/web_Auditors
□	jazn.com/web_CSR
□	jazn.com/web_CSRManager
☑	jazn.com/web_RuleAdministrators

Copyright © 1996, 2006, Oracle. All rights reserved.
About Oracle Enterprise Manager 10g Application Server Control

10. Create a snapshot of the users and groups that were created.

11. Press the **Map Role To Principals** button, and from the application, map the groups to their respective roles.



Principals

User Manager Name **JAZNUserManager**
User Manager Class **oracle.security.jazn.oc4j.JAZNUserManager**

Groups

Select	Name
●	jazn.com/web_Auditors
○	jazn.com/web_CSR
○	jazn.com/web_CSRManager
○	jazn.com/web_RuleAdministrators

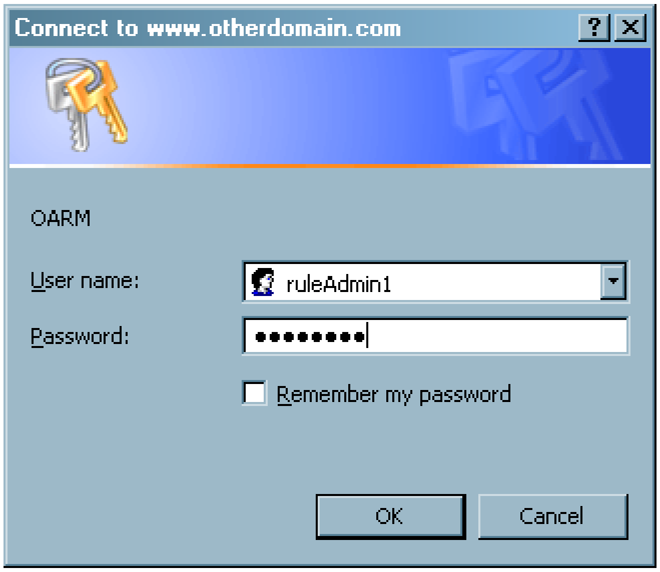
Users

Select	Name	Group Memberships
●	jazn.com/auditor1	jazn.com/web_Auditors
○	jazn.com/csr1	jazn.com/web_CSR
○	jazn.com/csrm1	jazn.com/web_CSRManager
○	jazn.com/ruleAdmin1	jazn.com/web_RuleAdministrators

Security Roles

Select	Name	Assigned Users	Assigned Groups
●	web_CSR		jazn.com/web_CSR
○	web_RuleAdministrators		jazn.com/web_RuleAdministrators
○	web_CSRManager		jazn.com/web_CSRManager

12. (Optional) Restart the application or Instance and access the application at http://otherdomain.com:8778/oarm, logging in as the ruleAdmin1 user.



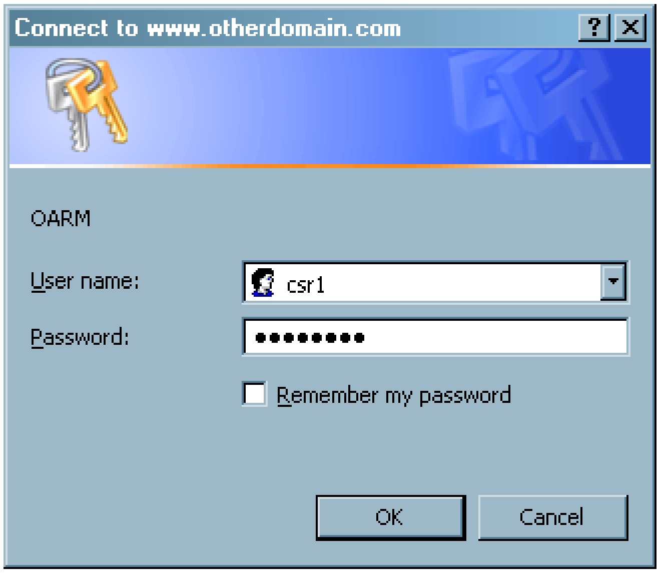
OARM

User name: ruleAdmin1

Password: ●●●●●●●●●

□ Remember my password

13. (Optional) Also try accessing the application and logging in as the csr user.



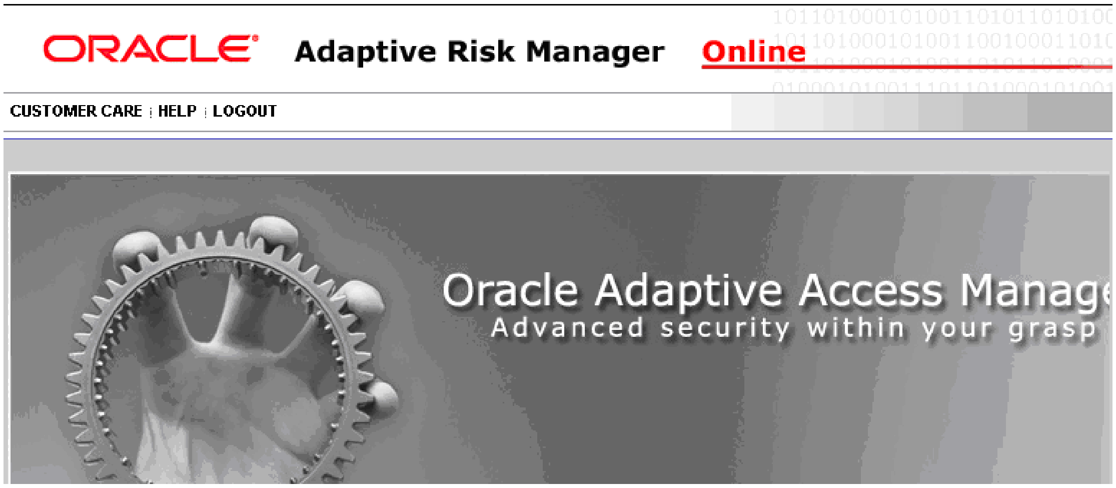
OARM

User name: csr1

Password: •••••••••

□ Remember my password

The following screen appears if you were successful in logging in.


ORACLE
Adaptive Risk Manager Online
CUSTOMER CARE | HELP | LOGOUT
Oracle Adaptive Access Manage
Advanced security within your grasp

WebLogic

For more detailed information on setting up WebLogic, refer to the BEA Web site.

Creating Groups and Adding Users to Groups from the WebLogic Administration Console

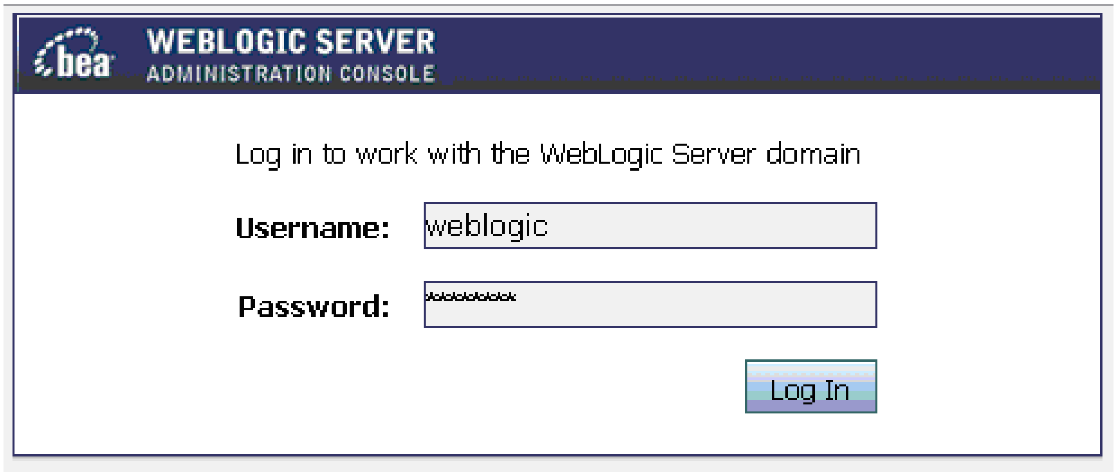
To create groups and add users

1. Log in to the WebLogic Server Administration Console by accessing http://*hostname:port*/console as a WebLogic Administrator.

   The hostname is the DNS name or IP address of the Administration Server.

   The port is the listen port on which the Administration Server is listening for requests (port 7001 by default).

   In the example below, **weblogic** was used to log in.

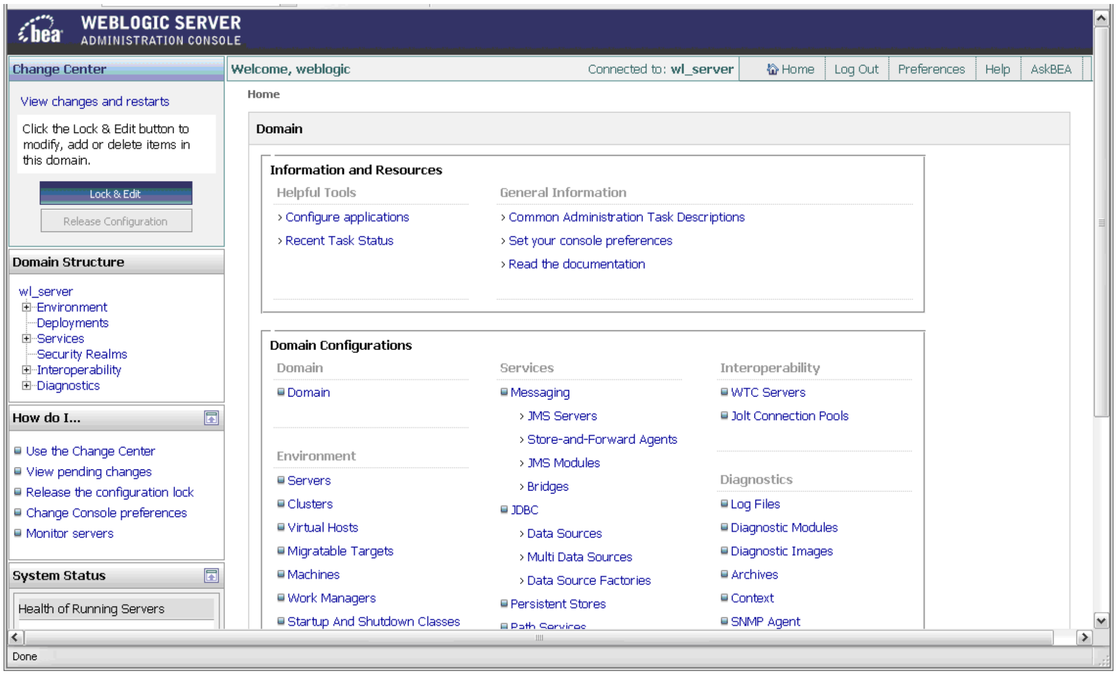


Log in to work with the WebLogic Server domain

Username: weblogic

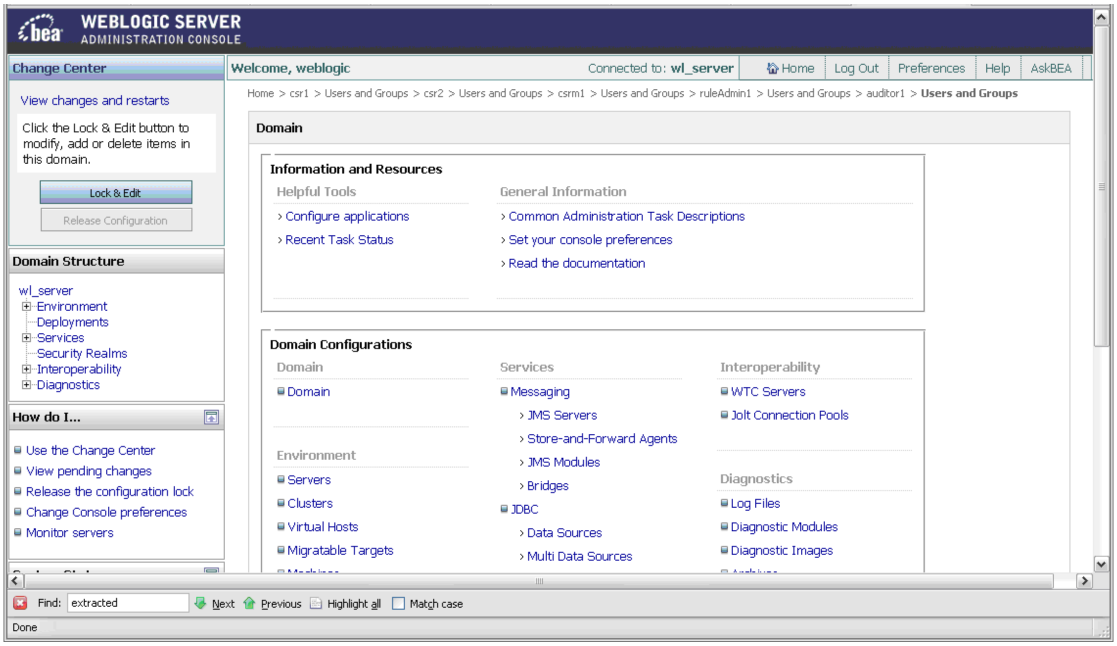
Password: *********

2. In the left pane, click the **Lock & Edit** button under the **Change Center** section.



Click the Lock & Edit button to modify, add or delete items in this domain.

3. From the **Domain Structure** section in left pane, select **Security Realms**.

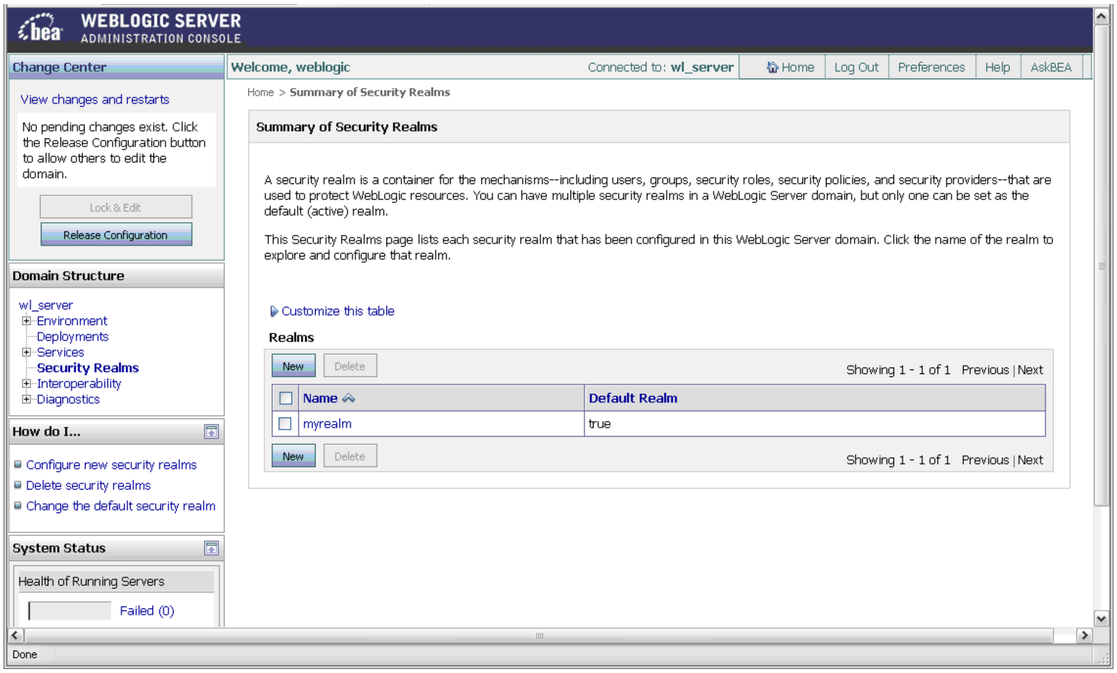


Click the Lock & Edit button to modify, add or delete items in this domain.

Home > csr1 > Users and Groups > csr2 > Users and Groups > csrm1 > Users and Groups > ruleAdmin1 > Users and Groups > auditor1 > **Users and Groups**

Find: extracted

4. In **Summary of Security Realms** page, select the check box next to the realm you are using.



No pending changes exist. Click the Release Configuration button to allow others to edit the domain.

Summary of Security Realms

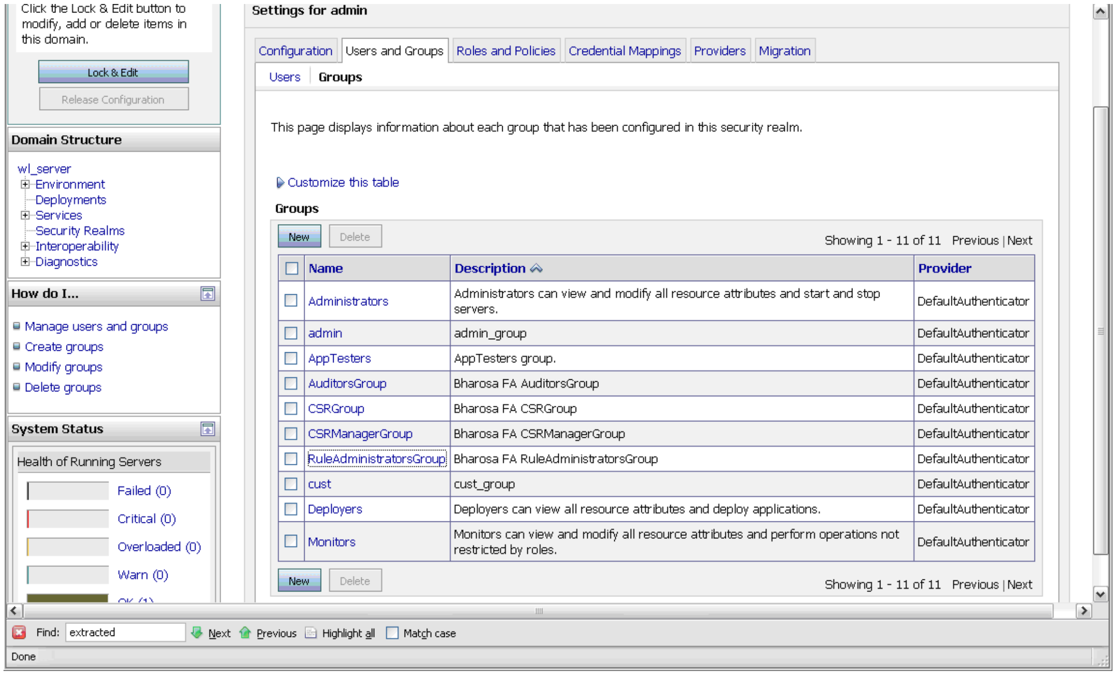
A security realm is a container for the mechanisms--including users, groups, security roles, security policies, and security providers--that are used to protect WebLogic resources. You can have multiple security realms in a WebLogic Server domain, but only one can be set as the default (active) realm.

This Security Realms page lists each security realm that has been configured in this WebLogic Server domain. Click the name of the realm to explore and configure that realm.

Realms

□	Name	Default Realm
□	myrealm	true

5. In the **Summary of Security Realms** page, click the realm you are using. For example, **myrealm**.
6. Click the **Users and Groups** tab.
7. To display the **Groups** page, click the **Groups** subtab. If you encounter an error, you may have to restart the WebLogic server.
8. Then, click the **New** button to create each of the four groups listed below.
    - CSRManagerGroup
    - CSRGroup
    - RuleAdministratorsGroup
    - AuditorsGroup



Click the Lock & Edit button to modify, add or delete items in this domain.

This page displays information about each group that has been configured in this security realm.

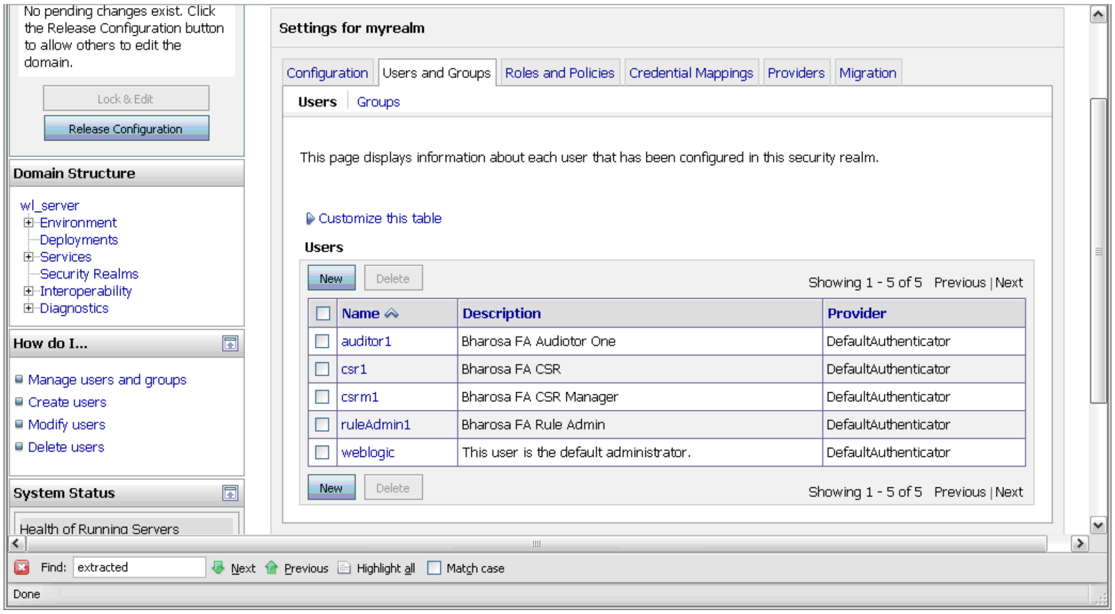
Groups

Showing 1 - 11 of 11

□	Name	Description	Provider
□	Administrators	Administrators can view and modify all resource attributes and start and stop servers.	DefaultAuthenticator
□	admin	admin_group	DefaultAuthenticator
□	AppTesters	AppTesters group.	DefaultAuthenticator
□	AuditorsGroup	Bharosa FA AuditorsGroup	DefaultAuthenticator
□	CSRGroup	Bharosa FA CSRGroup	DefaultAuthenticator
□	CSRManagerGroup	Bharosa FA CSRManagerGroup	DefaultAuthenticator
□	RuleAdministratorsGroup	Bharosa FA RuleAdministratorsGroup	DefaultAuthenticator
□	cust	cust_group	DefaultAuthenticator
□	Deployers	Deployers can view all resource attributes and deploy applications.	DefaultAuthenticator
□	Monitors	Monitors can view and modify all resource attributes and perform operations not restricted by roles.	DefaultAuthenticator

Showing 1 - 11 of 11

9. **Optional:** click the **Users** subtab. Then, click the **New** button for each of the following four users you want to create.
    - csrm1
    - csr
    - ruleAdmin1
    - auditor1



No pending changes exist. Click the Release Configuration button to allow others to edit the domain.

This page displays information about each user that has been configured in this security realm.

Users

Showing 1 - 5 of 5

□	Name	Description	Provider
□	auditor1	Bharosa FA Audiotor One	DefaultAuthenticator
□	csr1	Bharosa FA CSR	DefaultAuthenticator
□	csrm1	Bharosa FA CSR Manager	DefaultAuthenticator
□	ruleAdmin1	Bharosa FA Rule Admin	DefaultAuthenticator
□	weblogic	This user is the default administrator.	DefaultAuthenticator

Showing 1 - 5 of 5

10. **Optional**: to assign csrm1 to CSRManagerGroup, csr to CSRGroup, ruleAdmin1 to RuleAdministratorsGroup, and auditor1 to AuditorsGroup, follow the steps provided below.

    a. In the left pane select **Security Realms**.

    b. On **the Summary of Security Realms** page select the name of the realm (for example, **myrealm**).

    c. On the **Settings for Realm Name** page select **Users and Groups** > **Users**.

    d. In the **Users** table click the user you want to add to a group. For example, **csrm1**.

    e. On the **Settings for <User Name>** page select the **Groups** subtab.

    f. Select a group or groups from the **Available** list box and move the group or groups over to the **Chosen** list box. For example, **CSRManagerGroup.**

    e. Click **Save.**

11. Commit the users and groups created by clicking the **Release Configuration** button in the left pane.

For more information about groups, refer to the “Adaptive Risk Manager Online User Groups Reference” section of this manual.

Deploying the Adaptive Risk Manager Online Application WAR File

To deploy the Adaptive Risk Manager Online Application WAR file,

1. Create a directory named **oarm**.

   You must place the actual WAR file in a directory having the name of the application within that directory.

2. Extract the Adaptive Risk Manager Online WAR file, **oarm.war,** into the **oarm** directory created in the previous step.

   The WAR file can be extracted using the command, jar –xvf **oarm.war**, with **oarm** as the present working directory.

3. Edit the **log4j.xml**, **sessions.xml**, and **bharosa_server.properties** files for appropriate values.

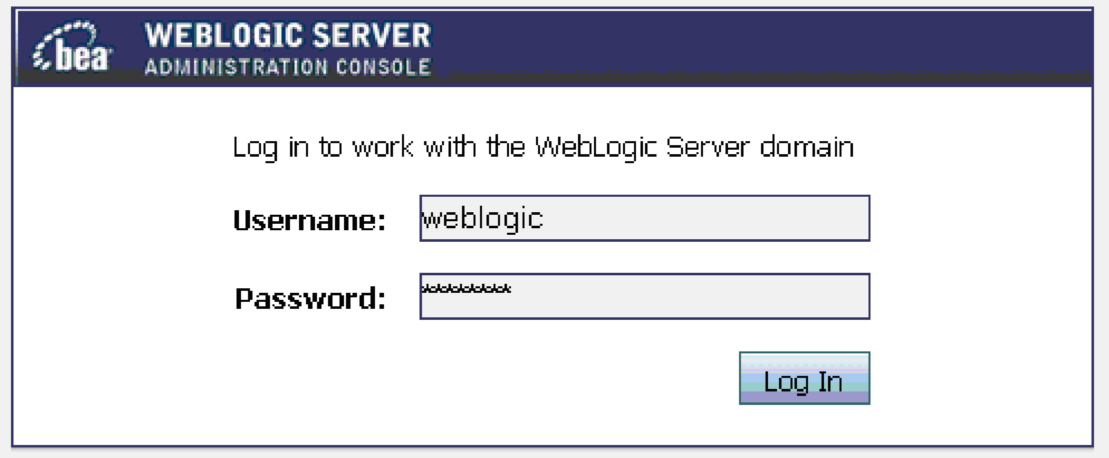
   They are located in the **oarm/WEB-INF/classes/** directory. Refer to the log4j configuration and Adaptive Risk Manager Server properties configuration sections.

4. Download the SQL Server 2005 JDBC driver (sqljdbc.jar) and any other third-party jars into the **oarm/WEB-INF/lib** directory.

5. Next, log in to the **WebLogic Server Administration Console** by accessing http://*hostname:port*/console as a WebLogic Administrator.

   The hostname is the DNS name or IP address of the Administration Server.

   The port is the listen port on which the Administration Server is listening for requests (port 7001 by default).

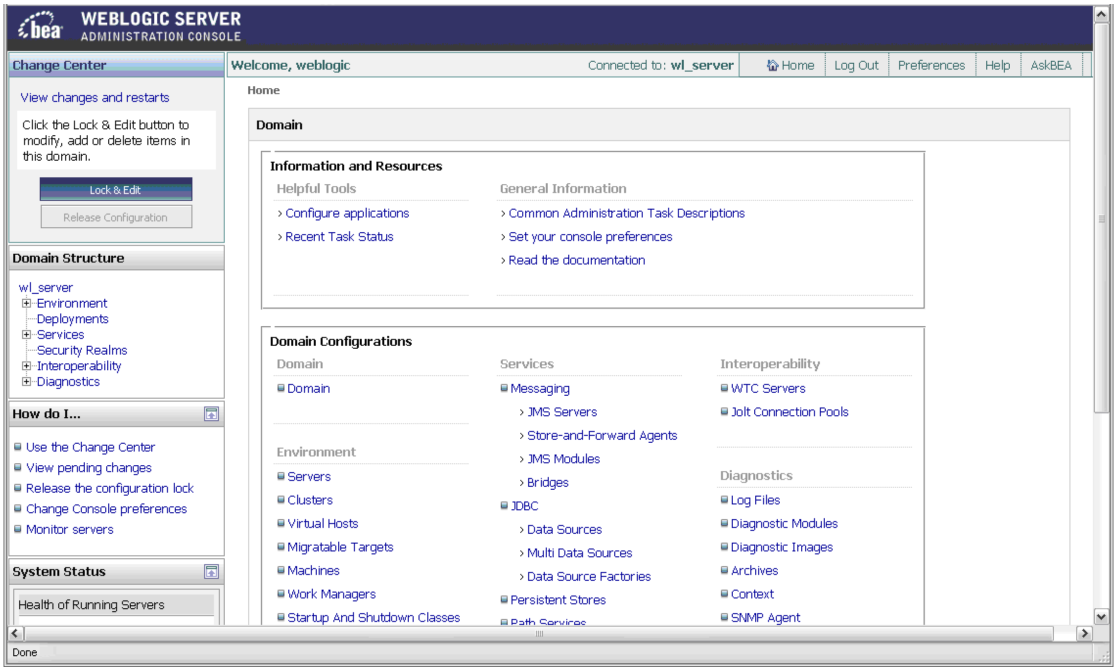


Log in to work with the WebLogic Server domain

Username: weblogic

Password: ********

6. In the left pane, click the **Lock & Edit** button under the **Change Center** section.



WEBLOGIC SERVER
ADMINISTRATION CONSOLE

Change Center

View changes and restarts

Click the Lock & Edit button to modify, add or delete items in this domain.

Domain Structure

wl_server
- Environment
- Deployments
- Services
- Security Realms
- Interoperability
- Diagnostics

How do I...

- Use the Change Center
- View pending changes
- Release the configuration lock
- Change Console preferences
- Monitor servers

System Status

Health of Running Servers

Home

Domain

Information and Resources

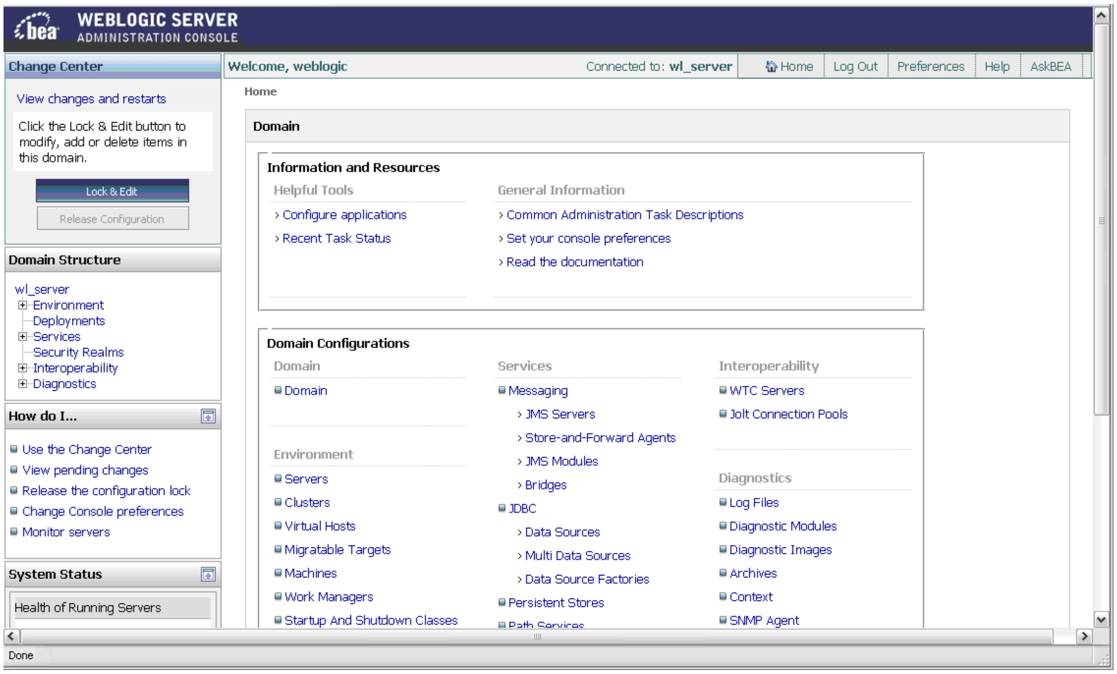
Helpful Tools	General Information
› Configure applications	› Common Administration Task Descriptions
› Recent Task Status	› Set your console preferences
	› Read the documentation

Domain Configurations

Domain	Services	Interoperability
Domain	Messaging	WTC Servers
	› JMS Servers	Jolt Connection Pools
	› Store-and-Forward Agents	
Environment	› JMS Modules	
Servers	› Bridges	**Diagnostics**
Clusters	JDBC	Log Files
Virtual Hosts	› Data Sources	Diagnostic Modules
Migratable Targets	› Multi Data Sources	Diagnostic Images
Machines	› Data Source Factories	Archives
Work Managers	Persistent Stores	Context
Startup And Shutdown Classes	Path Services	SNMP Agent

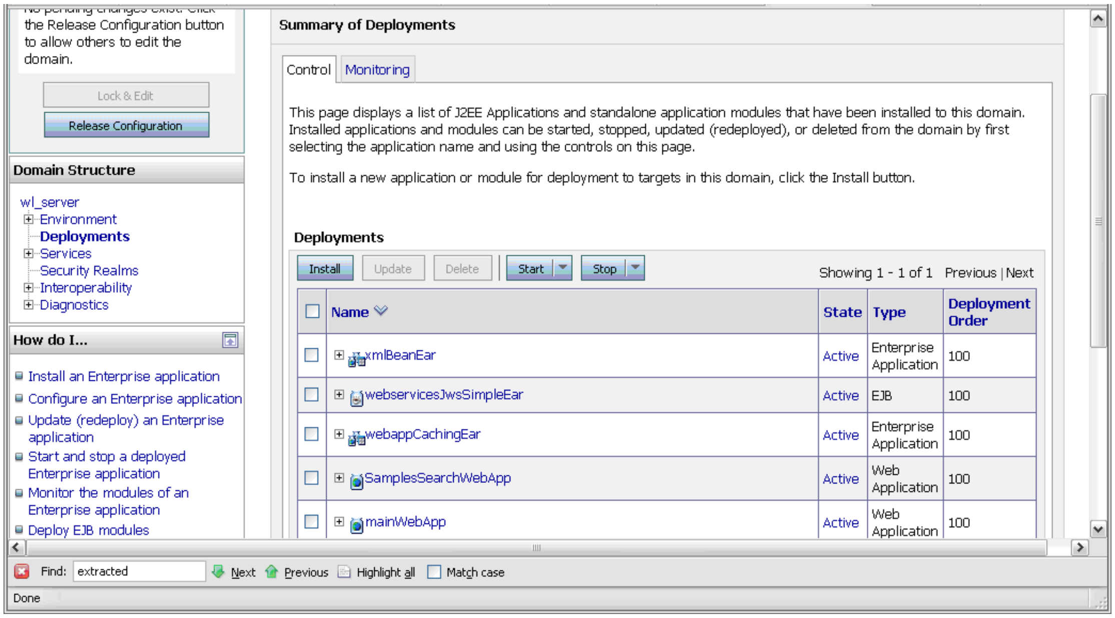
Done

7. From the **Domain Structure** section in the left pane, select **Deployments**.



Click the Lock & Edit button to modify, add or delete items in this domain.

8. From the **Summary of Deployments** page, select **Control**, and then click **Install**.



No pending changes exist. Click the Release Configuration button to allow others to edit the domain.

Summary of Deployments

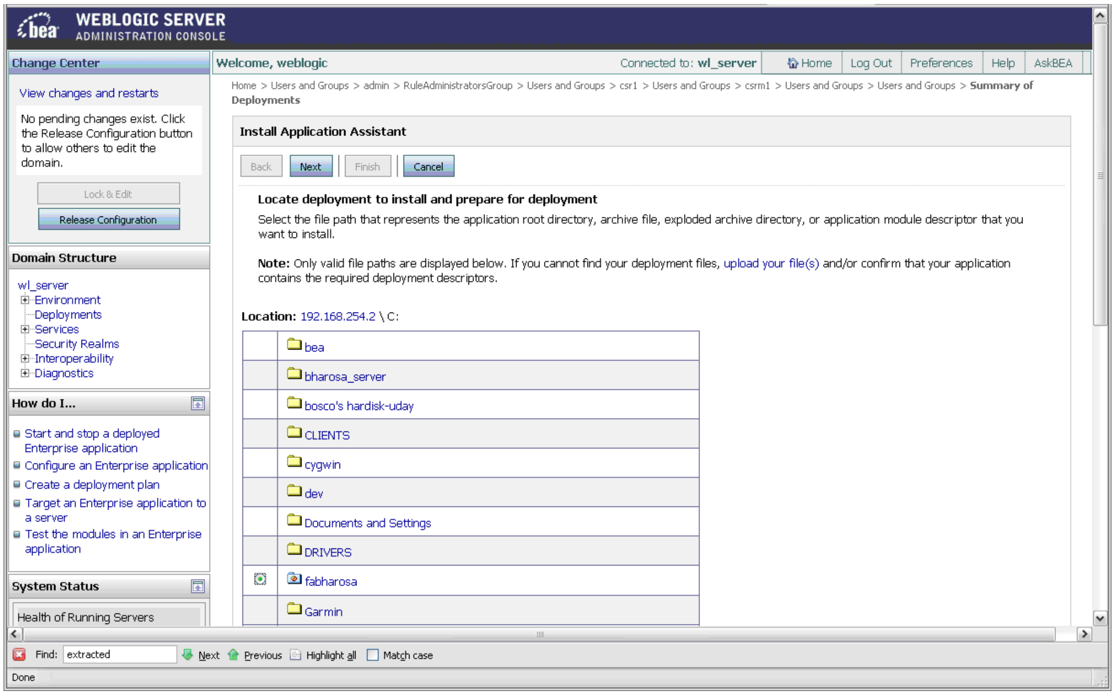
This page displays a list of J2EE Applications and standalone application modules that have been installed to this domain. Installed applications and modules can be started, stopped, updated (redeployed), or deleted from the domain by first selecting the application name and using the controls on this page.

To install a new application or module for deployment to targets in this domain, click the Install button.

Deployments

□	Name	State	Type	Deployment Order
□	xmlBeanEar	Active	Enterprise Application	100
□	webservicesJwsSimpleEar	Active	EJB	100
□	webappCachingEar	Active	Enterprise Application	100
□	SamplesSearchWebApp	Active	Web Application	100
□	mainWebApp	Active	Web Application	100

9. In the **Install Application Assistant** pane, locate the **oarm** directory. Since **oarm** is an exploded directory, WebLogic Server will install all components in and below the oarm directory. Then, click **Next**.



No pending changes exist. Click the Release Configuration button to allow others to edit the domain.

Home > Users and Groups > admin > RuleAdministratorsGroup > Users and Groups > csr1 > Users and Groups > csrm1 > Users and Groups > Users and Groups > **Summary of Deployments**

Install Application Assistant

Locate deployment to install and prepare for deployment

Select the file path that represents the application root directory, archive file, exploded archive directory, or application module descriptor that you want to install.

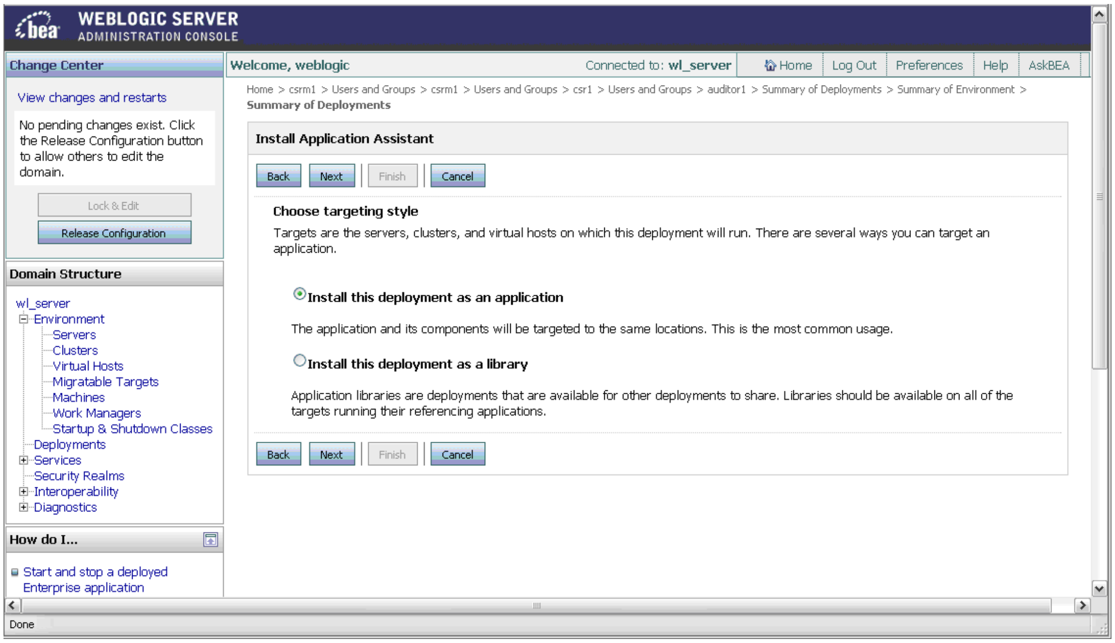
Note: Only valid file paths are displayed below. If you cannot find your deployment files, upload your file(s) and/or confirm that your application contains the required deployment descriptors.

Location: 192.168.254.2 \ C:

	bea
	bharosa_server
	bosco's hardisk-uday
	CLIENTS
	cygwin
	dev
	Documents and Settings
	DRIVERS
○	fabharosa
	Garmin

Find: extracted

10. Specify to target the installation as an application and click **Next**.



No pending changes exist. Click the Release Configuration button to allow others to edit the domain.

Install Application Assistant

Choose targeting style

Targets are the servers, clusters, and virtual hosts on which this deployment will run. There are several ways you can target an application.

● Install this deployment as an application

The application and its components will be targeted to the same locations. This is the most common usage.

○ Install this deployment as a library

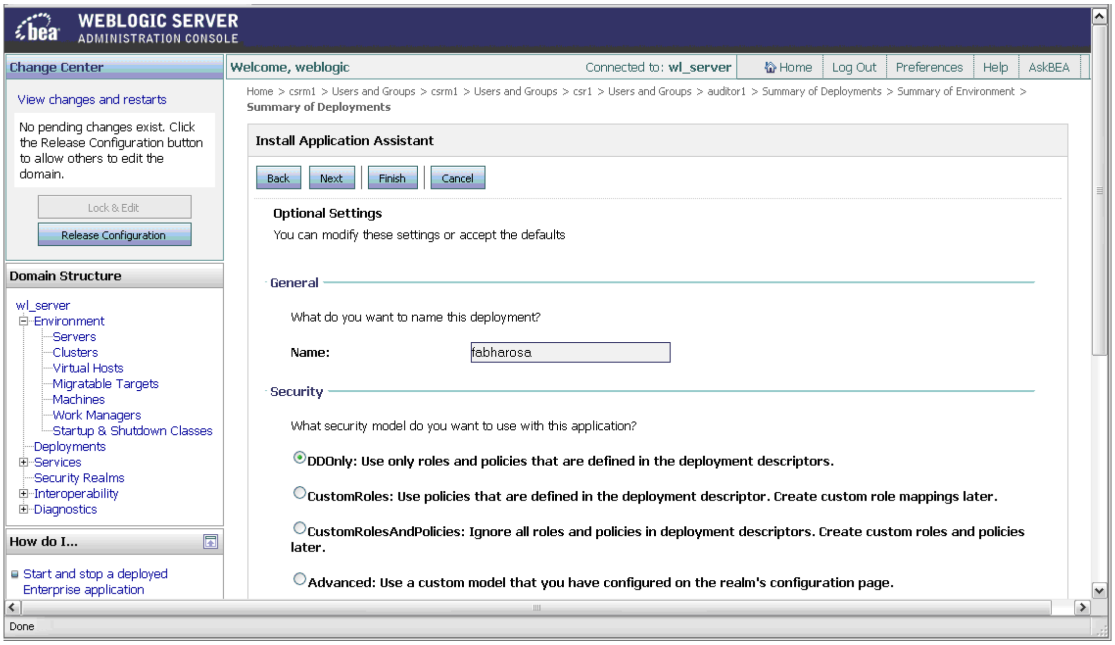
Application libraries are deployments that are available for other deployments to share. Libraries should be available on all of the targets running their referencing applications.

11. (Optional Step) Update additional deployment settings.

    Settings include:

    - The deployed name of the Adaptive Risk Manager Online Web application.
    - The security model that is applied to the Adaptive Risk Manager Online Web application.
    - How the directory contents are made available to targeted managed servers and clusters.

    Typically, the default values are adequate.



No pending changes exist. Click the Release Configuration button to allow others to edit the domain.

Install Application Assistant

Optional Settings

You can modify these settings or accept the defaults

General

What do you want to name this deployment?

Name: fabharosa

Security

What security model do you want to use with this application?

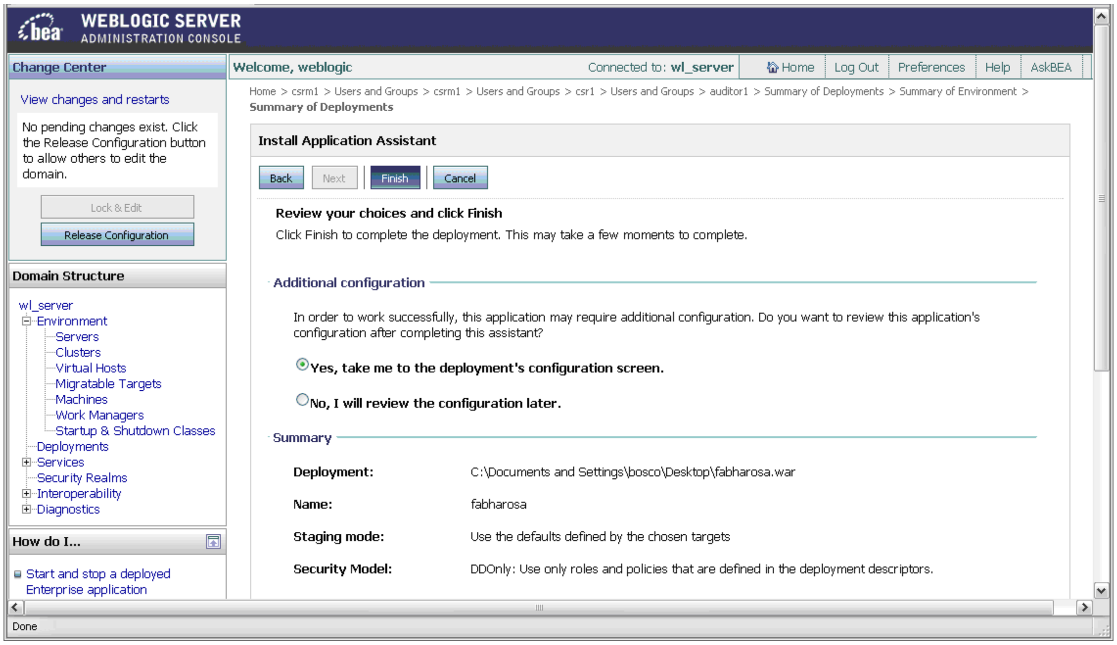
● **DDOnly: Use only roles and policies that are defined in the deployment descriptors.**

○ **CustomRoles: Use policies that are defined in the deployment descriptor. Create custom role mappings later.**

○ **CustomRolesAndPolicies: Ignore all roles and policies in deployment descriptors. Create custom roles and policies later.**

○ **Advanced: Use a custom model that you have configured on the realm's configuration page.**

12. Review the configuration settings you specified, and click **Finish** to complete the installation.



No pending changes exist. Click the Release Configuration button to allow others to edit the domain.

Review your choices and click Finish

Click Finish to complete the deployment. This may take a few moments to complete.

Additional configuration

In order to work successfully, this application may require additional configuration. Do you want to review this application's configuration after completing this assistant?

● **Yes, take me to the deployment's configuration screen.**

○ **No, I will review the configuration later.**

Summary

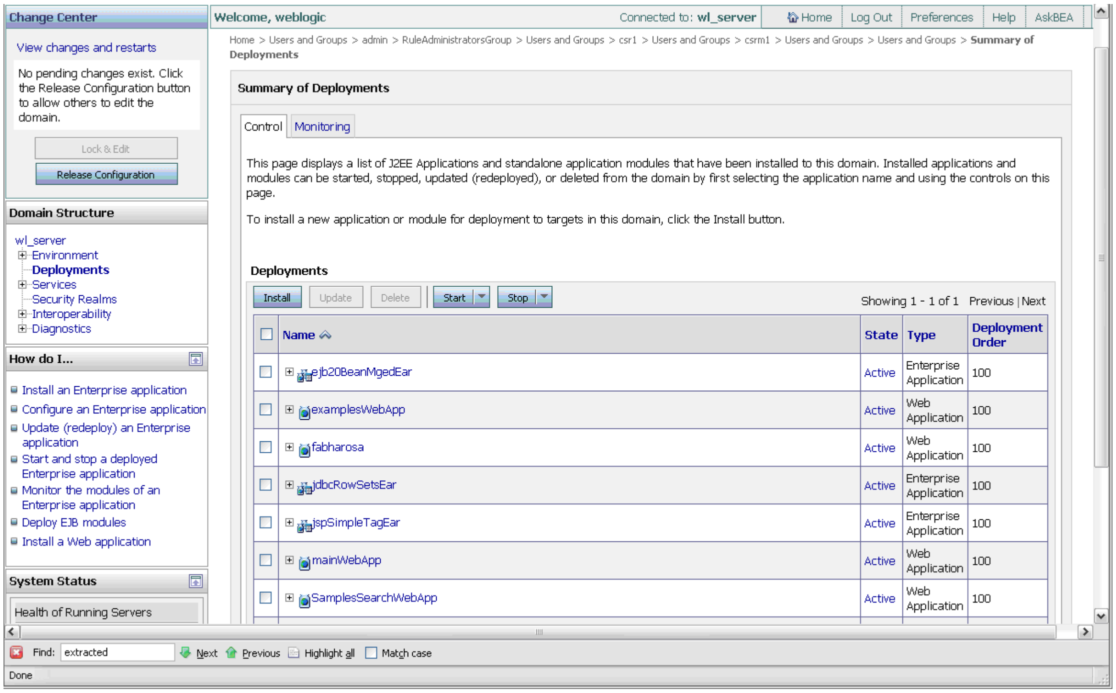
Deployment:	C:\Documents and Settings\bosco\Desktop\fabharosa.war
Name:	fabharosa
Staging mode:	Use the defaults defined by the chosen targets
Security Model:	DDOnly: Use only roles and policies that are defined in the deployment descriptors.

13. In order to work successfully, the application may require additional configuration. In the **Additional Configuration** section of the **Install Application Assistant** page, choose from the two options available.

- Yes, take me to the deployment's configuration screen
- No, I will review the configuration later

If you chose the **Yes, take me to the deployment’s configuration screen** option, you will go immediately to the deployment's configuration screen where you will be able to click the tabs to set additional configuration settings for the Adaptive Risk Manager Online Web application.

If you chose the **No, I will review the configuration later** option, the Administration Console returns you to the Deployments table, which should now include your newly-installed Adaptive Risk Manager Online Web application.


Change Center
View changes and restarts
Lock & Edit
Release Configuration
Domain Structure
wl_server
Environment
Deployments
Services
Security Realms
Interoperability
Diagnostics
How do I...
Install an Enterprise application
Configure an Enterprise application
Update (redeploy) an Enterprise application
Start and stop a deployed Enterprise application
Monitor the modules of an Enterprise application
Deploy EJB modules
Install a Web application
System Status
Health of Running Servers
Welcome, weblogic
Connected to: wl_server
Home
Log Out
Preferences
Help
AskBEA
Home > Users and Groups > admin > RuleAdministratorsGroup > Users and Groups > csr1 > Users and Groups > csrm1 > Users and Groups > Users and Groups > Summary of Deployments
Summary of Deployments
Control
Monitoring
Deployments
Install
Update
Delete
Start
Stop
Showing 1 - 1 of 1
Previous | Next
Find: extracted
Next
Previous
Highlight all
Match case
Done

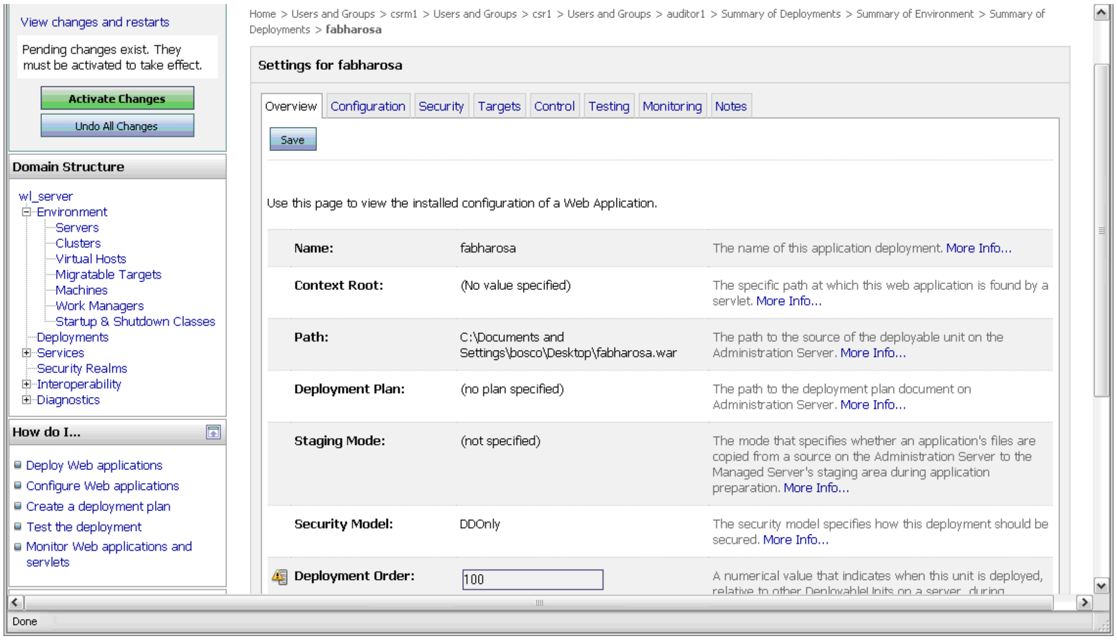
No pending changes exist. Click the Release Configuration button to allow others to edit the domain.

This page displays a list of J2EE Applications and standalone application modules that have been installed to this domain. Installed applications and modules can be started, stopped, updated (redeployed), or deleted from the domain by first selecting the application name and using the controls on this page.

To install a new application or module for deployment to targets in this domain, click the Install button.

□	Name	State	Type	Deployment Order
□	ejb20BeanMgedEar	Active	Enterprise Application	100
□	examplesWebApp	Active	Web Application	100
□	fabharosa	Active	Web Application	100
□	jdbcRowSetsEar	Active	Enterprise Application	100
□	jspSimpleTagEar	Active	Enterprise Application	100
□	mainWebApp	Active	Web Application	100
□	SamplesSearchWebApp	Active	Web Application	100

14. In the left pane, click the **Activate Changes** button under the **Change Center** section.



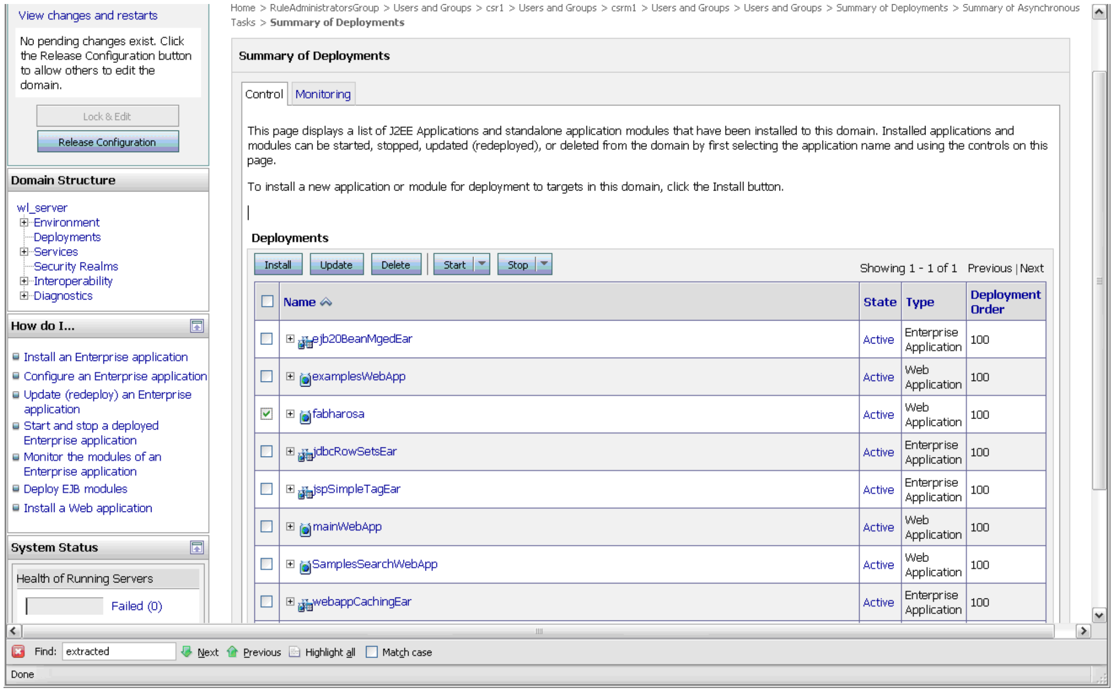
Pending changes exist. They must be activated to take effect.

Settings for fabharosa

Use this page to view the installed configuration of a Web Application.

Name:	fabharosa	The name of this application deployment. More Info...
Context Root:	(No value specified)	The specific path at which this web application is found by a servlet. More Info...
Path:	C:\Documents and Settings\bosco\Desktop\fabharosa.war	The path to the source of the deployable unit on the Administration Server. More Info...
Deployment Plan:	(no plan specified)	The path to the deployment plan document on Administration Server. More Info...
Staging Mode:	(not specified)	The mode that specifies whether an application's files are copied from a source on the Administration Server to the Managed Server's staging area during application preparation. More Info...
Security Model:	DDOnly	The security model specifies how this deployment should be secured. More Info...
Deployment Order:	100	A numerical value that indicates when this unit is deployed, relative to other DeployableUnits on a server, during

15. From the **Domain Structure** section in the left pane, select **Deployments**.
16. Select the Adaptive Risk Manager Online Web Application Module, **oarm**, and click **Stop**.
17. Select the **oarm** module again, click **Start**, and wait for its state to become active.



View changes and restarts

No pending changes exist. Click the Release Configuration button to allow others to edit the domain.

Domain Structure

wl_server
- ⊞ Environment
- Deployments
- ⊞ Services
- Security Realms
- ⊞ Interoperability
- ⊞ Diagnostics

How do I...

- Install an Enterprise application
- Configure an Enterprise application
- Update (redeploy) an Enterprise application
- Start and stop a deployed Enterprise application
- Monitor the modules of an Enterprise application
- Deploy EJB modules
- Install a Web application

System Status

Health of Running Servers

Failed (0)

Home > RuleAdministratorsGroup > Users and Groups > csr1 > Users and Groups > csrm1 > Users and Groups > Users and Groups > Summary of Deployments > Summary of Asynchronous Tasks > **Summary of Deployments**

Summary of Deployments

This page displays a list of J2EE Applications and standalone application modules that have been installed to this domain. Installed applications and modules can be started, stopped, updated (redeployed), or deleted from the domain by first selecting the application name and using the controls on this page.

To install a new application or module for deployment to targets in this domain, click the Install button.

Deployments

Showing 1 - 1 of 1 Previous | Next

□	Name	State	Type	Deployment Order
□	⊞ ejb20BeanMgedEar	Active	Enterprise Application	100
□	⊞ examplesWebApp	Active	Web Application	100
☑	⊞ fabharosa	Active	Web Application	100
□	⊞ jdbcRowSetsEar	Active	Enterprise Application	100
□	⊞ jspSimpleTagEar	Active	Enterprise Application	100
□	⊞ mainWebApp	Active	Web Application	100
□	⊞ SamplesSearchWebApp	Active	Web Application	100
□	⊞ webappCachingEar	Active	Enterprise Application	100

Tomcat

Notes on Tomcat

1. Download the Tomcat 5.5.xx admin package from the archives of Tomcat's 5.x downloads.

   For example, Tomcat 5.5.20 can be downloaded from the following link:

   `http://archive.apache.org/dist/tomcat/tomcat-5/v5.5.20/bin/apache-tomcat-5.5.20-admin.tar.gz`

2. Unzip the package and copy the files to the Tomcat home directory.

   For example, `/opt/apache/apache-tomcat-5.5.20/`

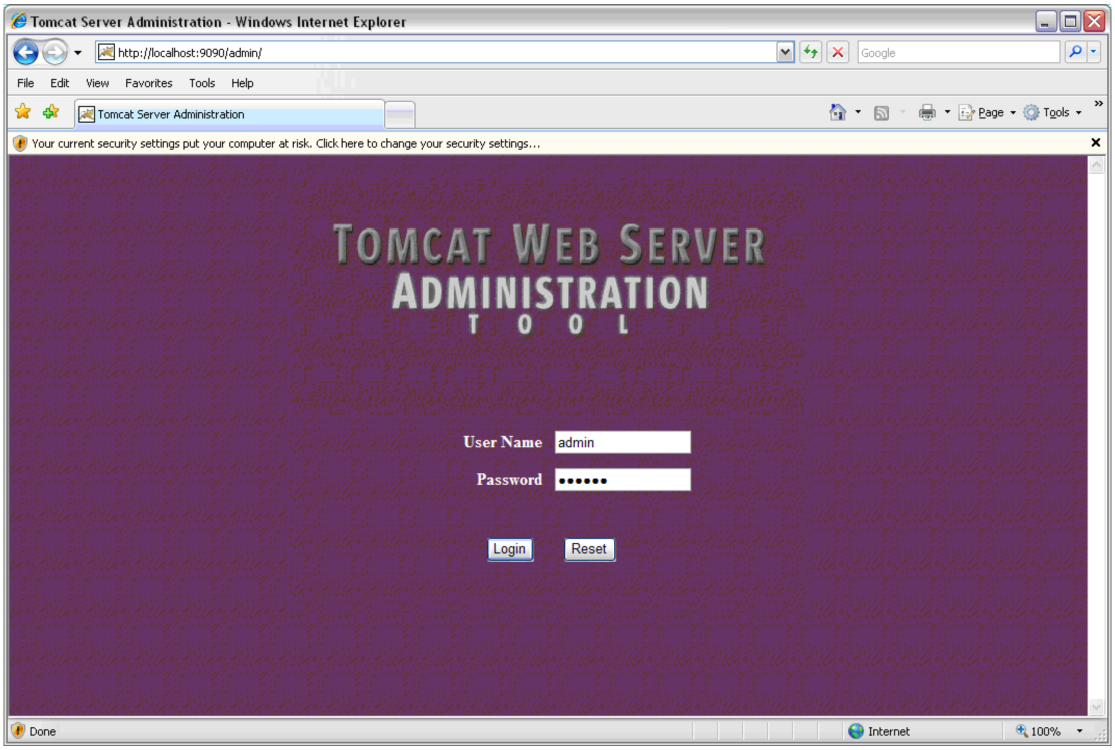
3. Delete the admin directory in the `webapps/ROOT` directory in the Tomcat directory, if any exists.

For more detailed information on setting up the Tomcat Web Server Administration Tool, refer to the "Tomcat FAQ" available at `http://tomcat.apache.org/`.

Creating Roles and Adding Users from the Tomcat Web Server Administration Tool

To create roles and add users from the Tomcat Web Server's Administration Tool Application:

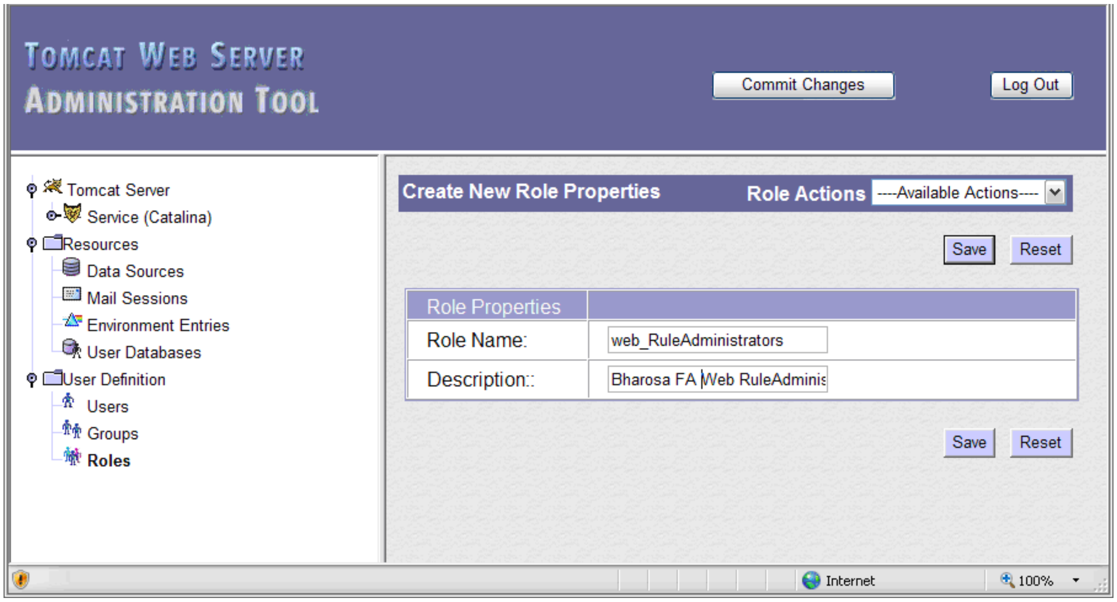
1. Log in to the **Tomcat Web Server Administration Tool** by entering the username and password for the administrator account you created for Tomcat; then click **Login**.


Tomcat Server Administration - Windows Internet Explorer
http://localhost:9090/admin/
Google
File Edit View Favorites Tools Help
Tomcat Server Administration
Page Tools
Your current security settings put your computer at risk. Click here to change your security settings...
TOMCAT WEB SERVER
ADMINISTRATION
TOOL
Login
Reset
Done
Internet
100%

User Name admin

Password ••••••

2. From the **Administration Tool**'s left pane, select **User Definition** and click **Roles**.
3. From the **Role Actions** list in the right pane, select **Create New Role**.
4. In the **Role Properties** section, enter `web_RuleAdministrators` in the **Role Name** field and `Bharosa FA Web RuleAdministrators` in the **Description** field and click **Save**.

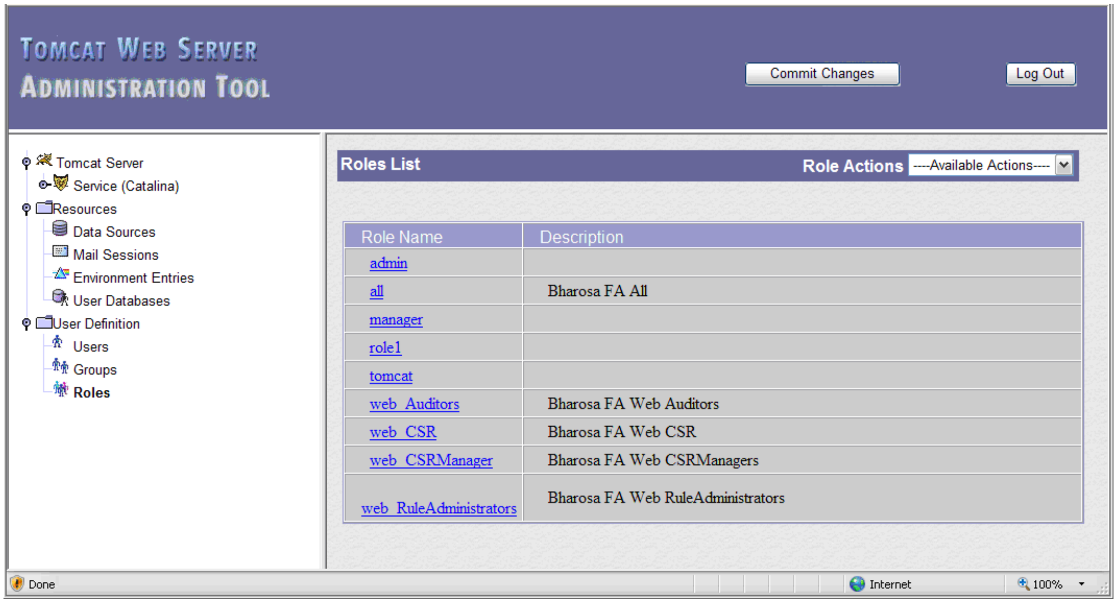


Role Name: web_RuleAdministrators

Description:: Bharosa FA Web RuleAdminis

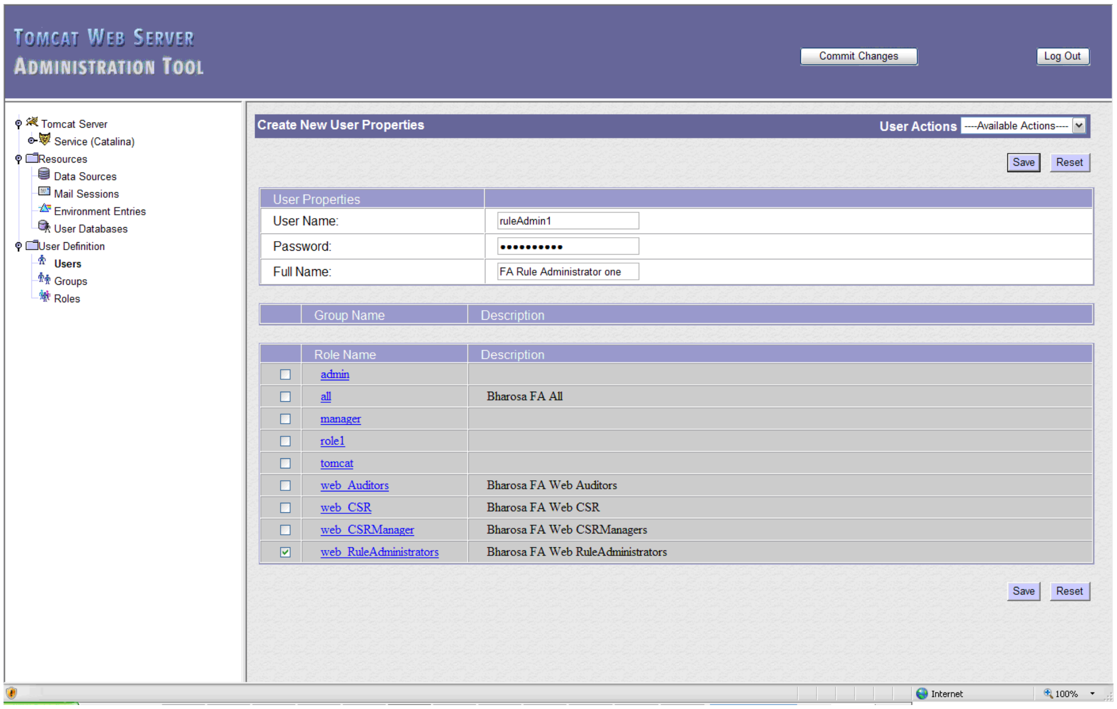
5. Then, repeat the process to create the **web_CSRManager**, **web_CSR**, **web_Auditors**, and **all** roles.

The screen below shows the five user roles created.



Role Name	Description
admin	
all	Bharosa FA All
manager	
role1	
tomcat	
web_Auditors	Bharosa FA Web Auditors
web_CSR	Bharosa FA Web CSR
web_CSRManager	Bharosa FA Web CSRManagers
web_RuleAdministrators	Bharosa FA Web RuleAdministrators

6. From the **Administration Tool**’s left pane, select **User Definition** and click **Users**.
7. From the **User Actions** list in the right pane, select **Create New User**.
8. Enter **ruleAdmin1** in the **User Name** field, values for the **Password** and **Full Name** fields, and select the **web_RuleAdministrators** check box. Then, click **Save**.



Create New User Properties — **User Actions** ----Available Actions----

Save Reset

User Properties	
User Name:	ruleAdmin1
Password:	••••••••••
Full Name:	FA Rule Administrator one

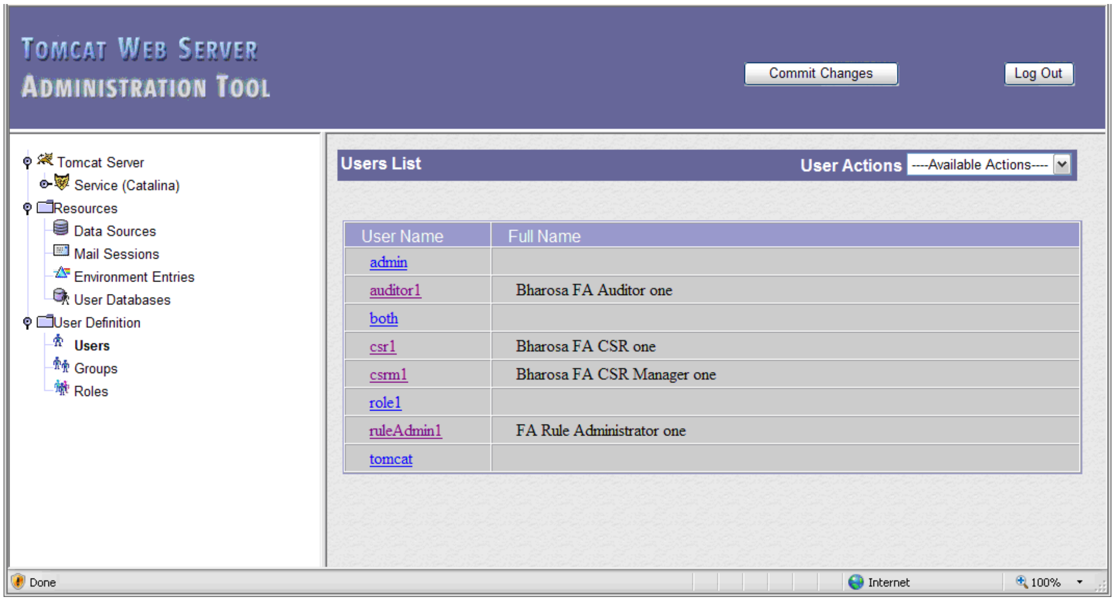
	Group Name	Description

	Role Name	Description
□	admin	
□	all	Bharosa FA All
□	manager	
□	role1	
□	tomcat	
□	web_Auditors	Bharosa FA Web Auditors
□	web_CSR	Bharosa FA Web CSR
□	web_CSRManager	Bharosa FA Web CSRManagers
☑	web_RuleAdministrators	Bharosa FA Web RuleAdministrators

Save Reset

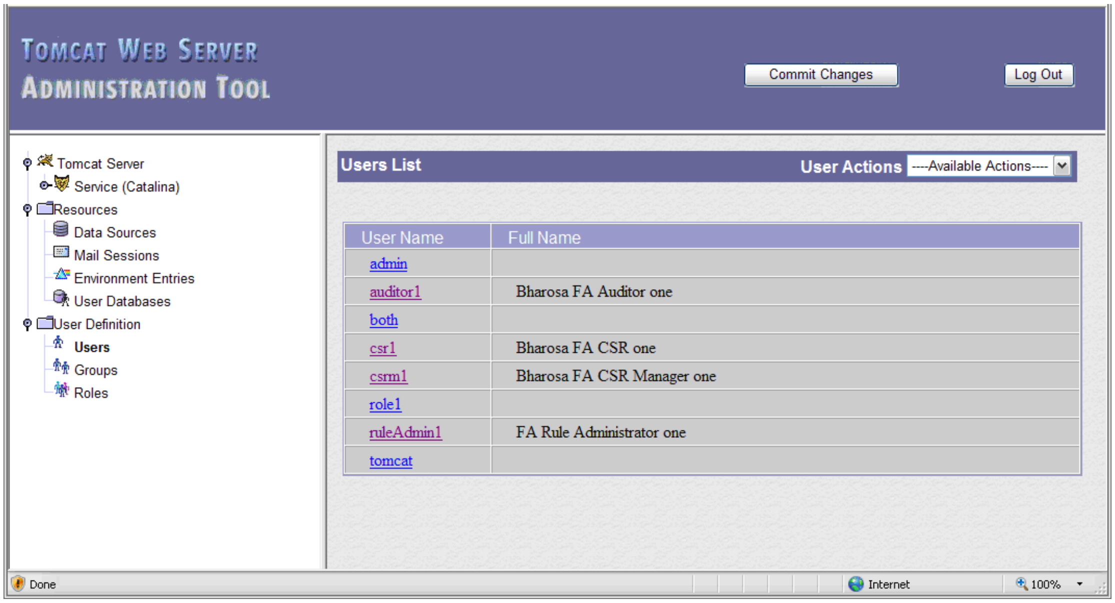
9. Repeat the process for creating users for
   - user **csrm1** with Role **web_CSRManager**
   - user **csr1** with Role **web_CSR**
   - user **auditor1** with Role **web_Auditors**
10. Optionally, you can attach all users created (**ruleAdmin1**, **csrm1**, **csr1**, and **auditor1)** so far to role **all**.

The four users are shown in the following screen.



User Name	Full Name
admin	
auditor1	Bharosa FA Auditor one
both	
csr1	Bharosa FA CSR one
csrm1	Bharosa FA CSR Manager one
role1	
ruleAdmin1	FA Rule Administrator one
tomcat	

11. Click the **Commit Changes** button to commit the changes for the roles and users created.



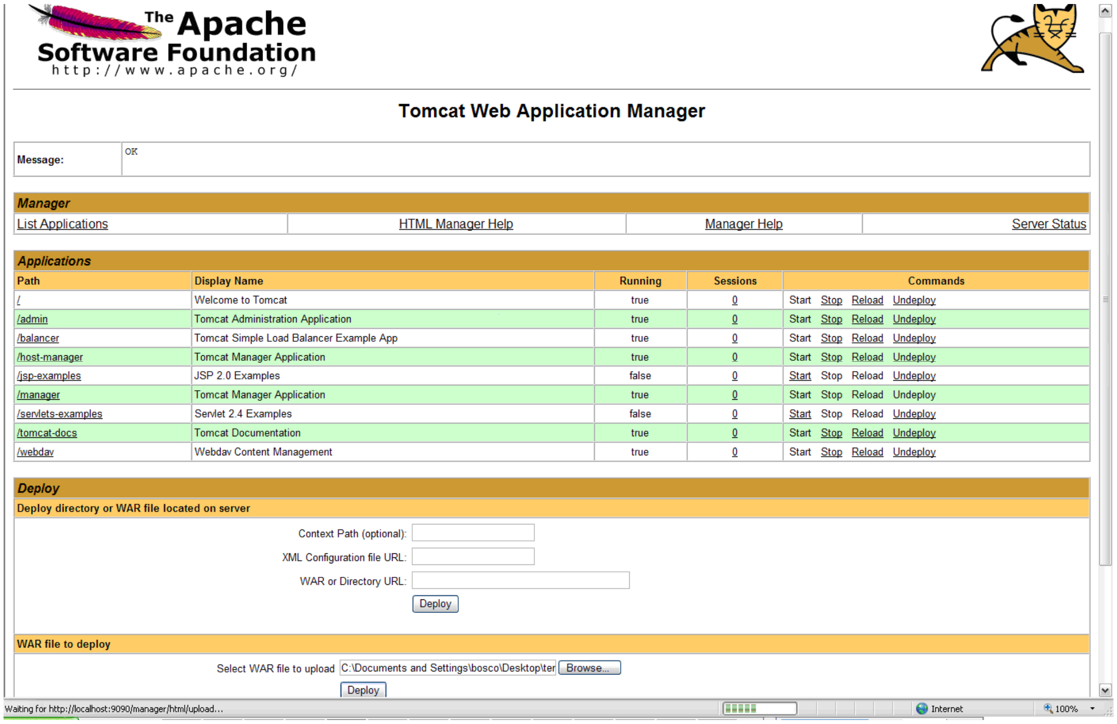
User Name	Full Name
admin	
auditor1	Bharosa FA Auditor one
both	
csr1	Bharosa FA CSR one
csrm1	Bharosa FA CSR Manager one
role1	
ruleAdmin1	FA Rule Administrator one
tomcat	

For more information about groups, refer to the “Adaptive Risk Manager Online User Groups Reference” section of this manual.

Deploying the Adaptive Risk Manager Online Application WAR

To deploy the Adaptive Risk Manager Online Application WAR,

1. Log in to the Tomcat Web Application Manager.
2. In the Deploy section, click the **Browse** button to select the WAR file to upload and deploy.



Tomcat Web Application Manager

Message:	OK

Manager

List Applications	HTML Manager Help	Manager Help	Server Status

Applications

Path	Display Name	Running	Sessions	Commands
/	Welcome to Tomcat	true	0	Start Stop Reload Undeploy
/admin	Tomcat Administration Application	true	0	Start Stop Reload Undeploy
/balancer	Tomcat Simple Load Balancer Example App	true	0	Start Stop Reload Undeploy
/host-manager	Tomcat Manager Application	true	0	Start Stop Reload Undeploy
/jsp-examples	JSP 2.0 Examples	false	0	Start Stop Reload Undeploy
/manager	Tomcat Manager Application	true	0	Start Stop Reload Undeploy
/servlets-examples	Servlet 2.4 Examples	false	0	Start Stop Reload Undeploy
/tomcat-docs	Tomcat Documentation	true	0	Start Stop Reload Undeploy
/webdav	Webdav Content Management	true	0	Start Stop Reload Undeploy

Deploy

Deploy directory or WAR file located on server

Context Path (optional):

XML Configuration file URL:

WAR or Directory URL:

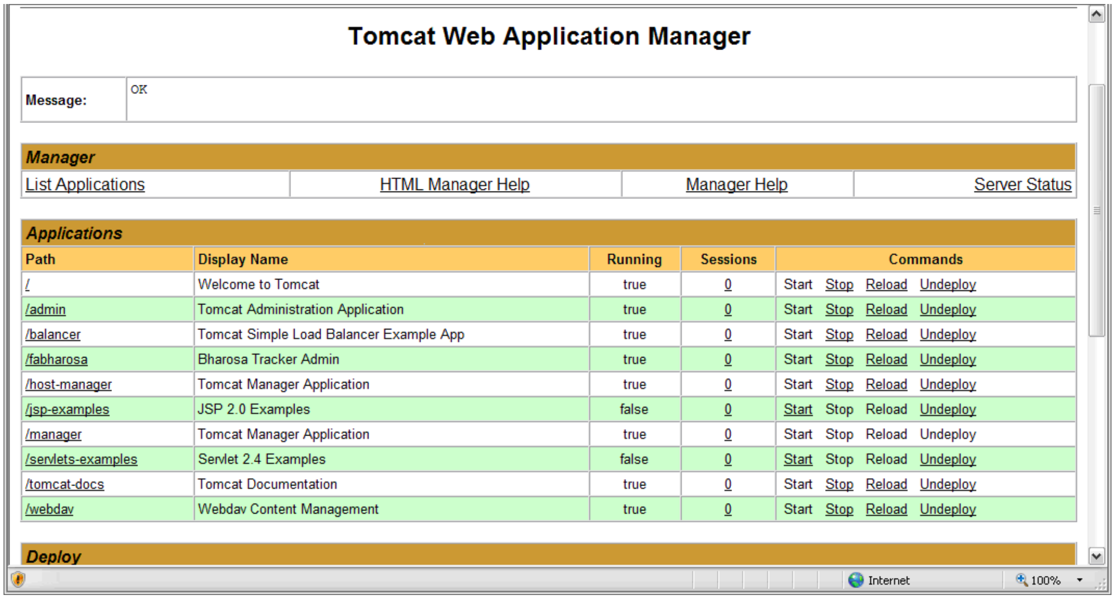
WAR file to deploy

Select WAR file to upload C:\Documents and Settings\bosco\Desktop\ter

Waiting for http://localhost:9090/manager/html/upload...

3. Select the **oarm.war** of the Adaptive Risk Manager Online Application and click **Open**; then, in the Tomcat Web Application Manager page, click **Deploy**.

4. Find the deployed application under the **Applications** section of the **Tomcat Web Application Manager** Web page.



Tomcat Web Application Manager

Message: OK

Manager

List Applications | HTML Manager Help | Manager Help | Server Status

Applications

Path	Display Name	Running	Sessions	Commands
/	Welcome to Tomcat	true	0	Start Stop Reload Undeploy
/admin	Tomcat Administration Application	true	0	Start Stop Reload Undeploy
/balancer	Tomcat Simple Load Balancer Example App	true	0	Start Stop Reload Undeploy
/fabharosa	Bharosa Tracker Admin	true	0	Start Stop Reload Undeploy
/host-manager	Tomcat Manager Application	true	0	Start Stop Reload Undeploy
/jsp-examples	JSP 2.0 Examples	false	0	Start Stop Reload Undeploy
/manager	Tomcat Manager Application	true	0	Start Stop Reload Undeploy
/servlets-examples	Servlet 2.4 Examples	false	0	Start Stop Reload Undeploy
/tomcat-docs	Tomcat Documentation	true	0	Start Stop Reload Undeploy
/webdav	Webdav Content Management	true	0	Start Stop Reload Undeploy

Deploy

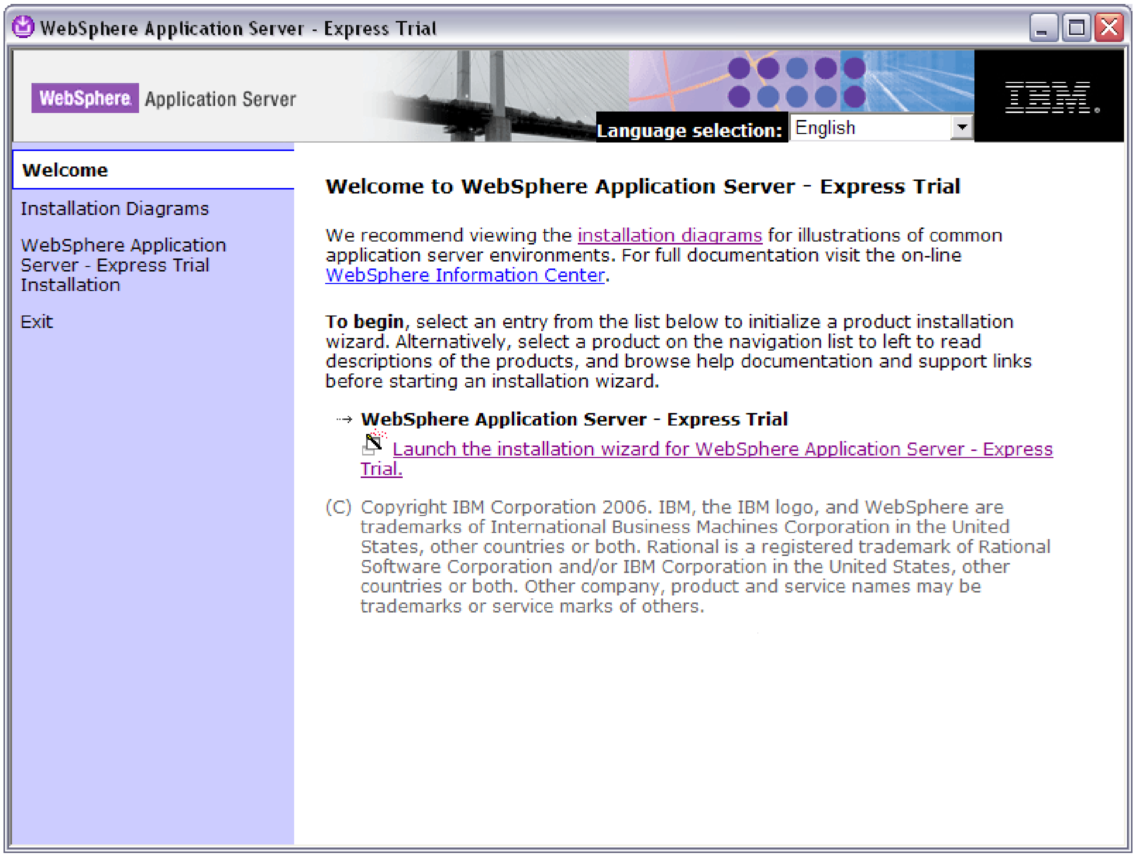
5. Edit the files **log4j.xml**, **sessions.xml**, and **bharosa_server.properties** from **TOMCAT_HOME/webapps/oarm/WEB-INF/classes/** for appropriate values as mentioned in log4j configuration, TopLink Configuration Reference, and Server Properties Configuration sections of this document.
6. Download any third-party jars like sqljdbc.jar into **TOMCAT_HOME/webapps/oarm/WEB-INF/lib** directory.
7. Restart the **Tomcat Application Server** from **Services** or from the command prompt.

IBM WebSphere Application Server 6.1

Using the Launchpad to Start the Installation

1. Go to http://www.ibm.com/developerworks/downloads/ws/was/.
2. Click the **System requirements** link to check that the minimum operating system and hardware requirements are met on the server to support the basic installation and use of the **WebSphere Application Server**.
3. Register for a universal IBM user ID if you have not already done so. You will need an IBM ID to proceed with the **WebSphere Application Server** download.
4. Navigate to the download page and select the WebSphere Application Server Base option. Then, click **Download now**.
5. Use a file extracting utility to unpack the **WebSphere Application Server** files into a single, temporary directory on your system.
6. Double-click launchpad.exe, which is located in the temporary directory, to start the install process.

   The launchpad panel for the **WebSphere Application Server - Express** appears.


WebSphere Application Server - Express Trial
WebSphere Application Server
IBM
Language selection: English
Welcome
Installation Diagrams
WebSphere Application Server - Express Trial Installation
Exit

Welcome to WebSphere Application Server - Express Trial

We recommend viewing the installation diagrams for illustrations of common application server environments. For full documentation visit the on-line WebSphere Information Center.

To begin, select an entry from the list below to initialize a product installation wizard. Alternatively, select a product on the navigation list to left to read descriptions of the products, and browse help documentation and support links before starting an installation wizard.

→ **WebSphere Application Server - Express Trial**

Launch the installation wizard for WebSphere Application Server - Express Trial.

(C) Copyright IBM Corporation 2006. IBM, the IBM logo, and WebSphere are trademarks of International Business Machines Corporation in the United States, other countries or both. Rational is a registered trademark of Rational Software Corporation and/or IBM Corporation in the United States, other countries or both. Other company, product and service names may be trademarks or service marks of others.

7. Click **Install Diagrams** to view the diagrams for common installation configurations.
8. Launch the installation wizard by clicking the **Launch the installation wizard for Websphere Application Server – Express** link in the launchpad panel.

9. In the **Welcome to the IBM WebSphere Application Server Trial install wizard** screen, click **Next** to continue.
10. When the **Software License Agreement** screen appears, accept the IBM and non-IBM terms and press **Next** to continue.
11. In the **System prerequisite check** screen, click **Next** to continue.
12. In the **Install Sample Applications** screen, deselect the **Install the sample applications** option, and press **Next** to continue.
13. When the **Product install location** screen appears, click **Next** to install to the default location or click **Browse** to install in another location.
14. When the **Enable Administrative Security** screen appears, select the **Enable administrative security** option and type in a username and password. Then, click **Next** to continue.

    By enabling security, you protect your server from unauthorized users and are then able to provide application isolation and requirements for authenticating application users.
15. In the **Installation Summary** screen, click **Next** to continue.
16. Press the **Finish** button after the installation completes.

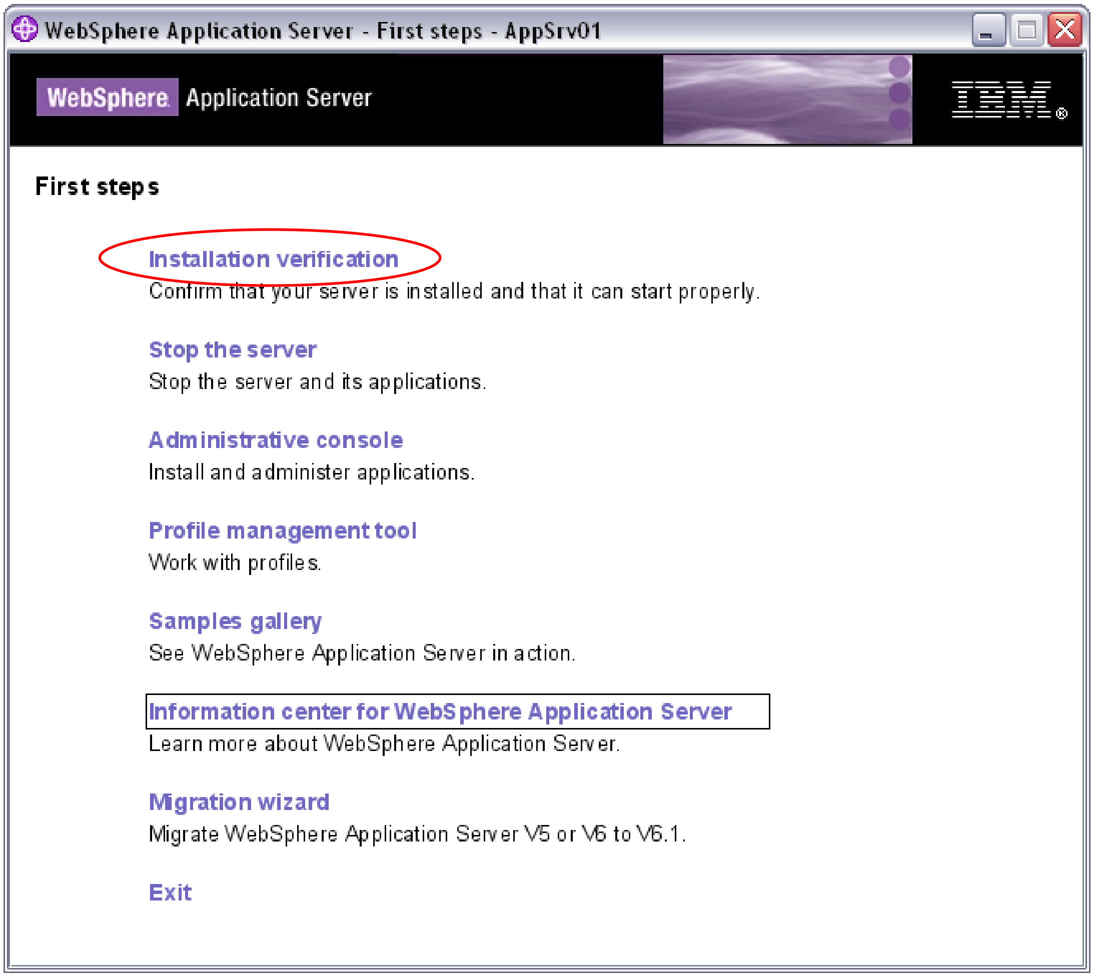
Verifying the WebSphere Installation

1. Launch the **First steps console** from the **Start** menu if it did not launch automatically after the installation.

   Select **IBM WebSphere** > **Application Server** > **Profiles** > **AppSrv01** > **First steps**.

   The **First steps console** will enable you to verify the installation, start or stop the Application Server, access the administrative console, access the information center, and so on from a central location.

2. Click **Installation Verification** from the **First steps console** to ensure that your installation has been successful.


WebSphere Application Server - First steps - AppSrv01
WebSphere Application Server
IBM

First steps

Installation verification

Confirm that your server is installed and that it can start properly.

Stop the server

Stop the server and its applications.

Administrative console

Install and administer applications.

Profile management tool

Work with profiles.

Samples gallery

See WebSphere Application Server in action.

Information center for WebSphere Application Server

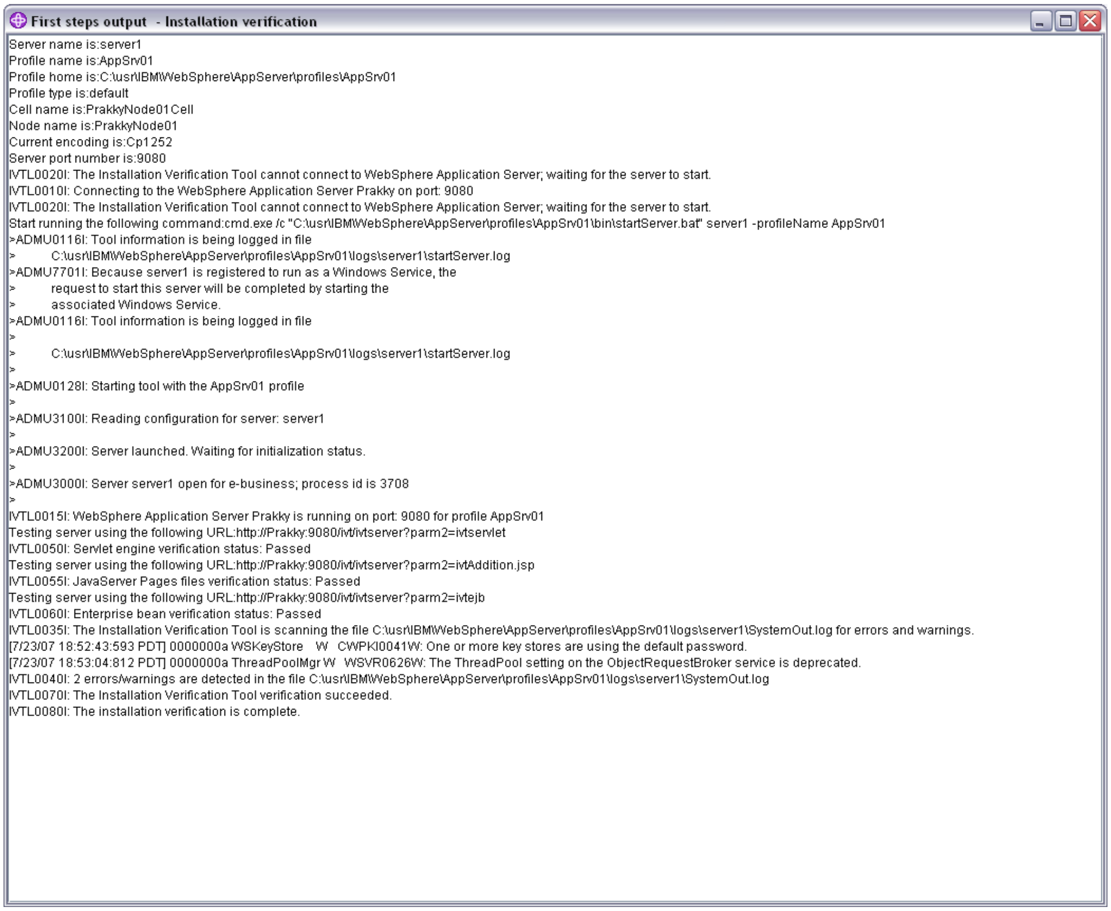
Learn more about WebSphere Application Server.

Migration wizard

Migrate WebSphere Application Server V5 or V6 to V6.1.

Exit

An example of an **Installation verification** screen is shown below.



```
Server name is:server1
Profile name is:AppSrv01
Profile home is:C:\usr\IBM\WebSphere\AppServer\profiles\AppSrv01
Profile type is:default
Cell name is:PrakkyNode01Cell
Node name is:PrakkyNode01
Current encoding is:Cp1252
Server port number is:9080
IVTL0020I: The Installation Verification Tool cannot connect to WebSphere Application Server; waiting for the server to start.
IVTL0010I: Connecting to the WebSphere Application Server Prakky on port: 9080
IVTL0020I: The Installation Verification Tool cannot connect to WebSphere Application Server; waiting for the server to start.
Start running the following command:cmd.exe /c "C:\usr\IBM\WebSphere\AppServer\profiles\AppSrv01\bin\startServer.bat" server1 -profileName AppSrv01
>ADMU0116I: Tool information is being logged in file
>          C:\usr\IBM\WebSphere\AppServer\profiles\AppSrv01\logs\server1\startServer.log
>ADMU7701I: Because server1 is registered to run as a Windows Service, the
>          request to start this server will be completed by starting the
>          associated Windows Service.
>ADMU0116I: Tool information is being logged in file
>
>          C:\usr\IBM\WebSphere\AppServer\profiles\AppSrv01\logs\server1\startServer.log
>
>ADMU0128I: Starting tool with the AppSrv01 profile
>
>ADMU3100I: Reading configuration for server: server1
>
>ADMU3200I: Server launched. Waiting for initialization status.
>
>ADMU3000I: Server server1 open for e-business; process id is 3708
>
IVTL0015I: WebSphere Application Server Prakky is running on port: 9080 for profile AppSrv01
Testing server using the following URL:http://Prakky:9080/ivt/ivtserver?parm2=ivtservlet
IVTL0050I: Servlet engine verification status: Passed
Testing server using the following URL:http://Prakky:9080/ivt/ivtserver?parm2=ivtAddition.jsp
IVTL0055I: JavaServer Pages files verification status: Passed
Testing server using the following URL:http://Prakky:9080/ivt/ivtserver?parm2=ivtejb
IVTL0060I: Enterprise bean verification status: Passed
IVTL0035I: The Installation Verification Tool is scanning the file C:\usr\IBM\WebSphere\AppServer\profiles\AppSrv01\logs\server1\SystemOut.log for errors and warnings.
[7/23/07 18:52:43:593 PDT] 0000000a WSKeyStore    W   CWPKI0041W: One or more key stores are using the default password.
[7/23/07 18:53:04:812 PDT] 0000000a ThreadPoolMgr W   WSVR0626W: The ThreadPool setting on the ObjectRequestBroker service is deprecated.
IVTL0040I: 2 errors/warnings are detected in the file C:\usr\IBM\WebSphere\AppServer\profiles\AppSrv01\logs\server1\SystemOut.log
IVTL0070I: The Installation Verification Tool verification succeeded.
IVTL0080I: The installation verification is complete.
```

If there are errors during the verification that indicate that the Application Server did not start, you will have to manually start the server before continuing to the next step.

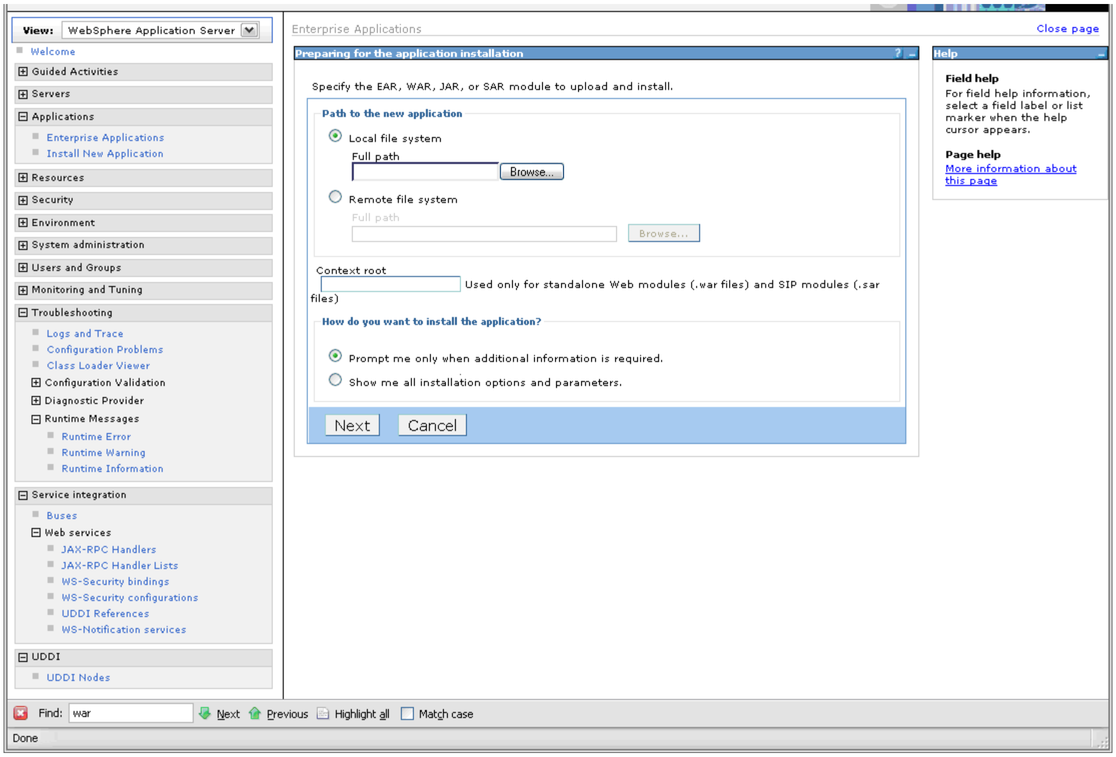
Installing the Adaptive Risk Manager Online Web Applications

1. Log in to the WebSphere Administration Console by pointing your browser to http://*server.name*:9060/admin.

   The default URL uses the default port.

2. Enter your credentials in the login.
3. From console's left pane, select **Applications** and click **Install New Application**.
4. Upload the WAR file and specify the **Context root** parameter.

   For example, specify "/oarm" for the **oarm.war** file.



Preparing for the application installation

Specify the EAR, WAR, JAR, or SAR module to upload and install.

Path to the new application

● Local file system

Full path [ ] Browse...

○ Remote file system

Full path [ ] Browse...

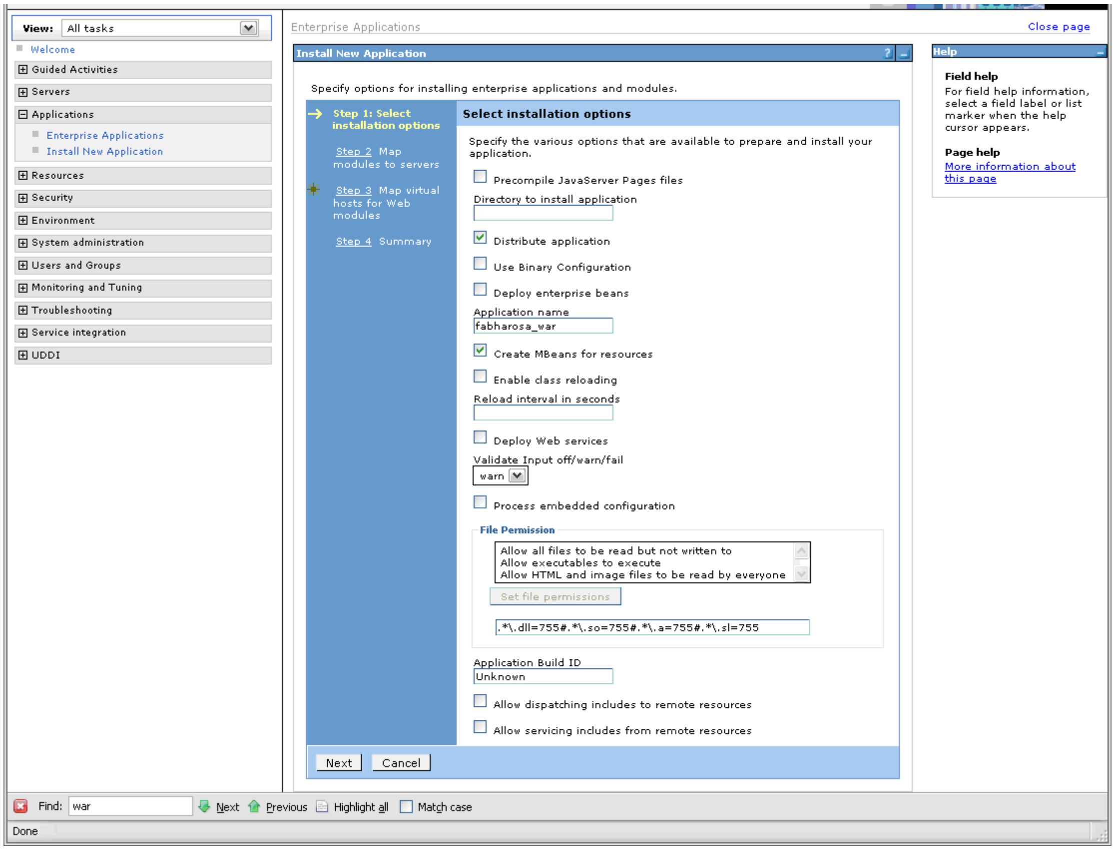
Context root [ ] Used only for standalone Web modules (.war files) and SIP modules (.sar files)

How do you want to install the application?

● Prompt me only when additional information is required.

○ Show me all installation options and parameters.

5. In the **Select installation options** section, select the **Distribute application** and **Create MBeans for resources** options as shown in the screen below. Ensure that the default settings for the other options are kept. Then, click **Next**.



Install New Application

Specify options for installing enterprise applications and modules.

Step 1: Select installation options

Step 2 Map modules to servers

Step 3 Map virtual hosts for Web modules

Step 4 Summary

Select installation options

Specify the various options that are available to prepare and install your application.

□ Precompile JavaServer Pages files

Directory to install application:

☑ Distribute application

□ Use Binary Configuration

□ Deploy enterprise beans

Application name: fabharosa_war

☑ Create MBeans for resources

□ Enable class reloading

Reload interval in seconds:

□ Deploy Web services

Validate Input off/warn/fail: warn

□ Process embedded configuration

File Permission

Allow all files to be read but not written to
Allow executables to execute
Allow HTML and image files to be read by everyone

.*\.dll=755#.*\.so=755#.*\.a=755#.*\.sl=755

Application Build ID: Unknown

□ Allow dispatching includes to remote resources

□ Allow servicing includes from remote resources

Field help

For field help information, select a field label or list marker when the help cursor appears.

Page help

More information about this page

6. When the **Map modules to server** screen appears, select the oarm module and click **Next**.
7. When the **Map virtual hosts for Web modules** screen appears, select the Bharosa module and click **Next**.
8. Click **Finish** when the **Summary** screen appears.

   The installation trace screen similar to the one shown below is run.

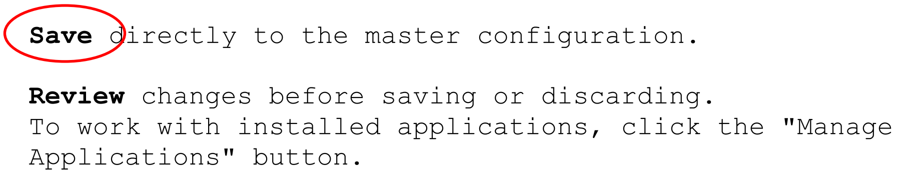
```
Installing...
If there are enterprise beans in the application, the EJB
deployment process can take several minutes. Please do not save
the configuration until the process completes.
Check the SystemOut.log on the Deployment Manager or server
where the application is deployed for specific information
about the EJB deployment process as it occurs.
ADMA5016I: Installation of oarm_war started.
ADMA5067I: Resource validation for application oarm_war
completed successfully.
ADMA5058I: Application and module versions are validated with
versions of deployment targets.
ADMA5005I: The application oarm_war is configured in the
WebSphere Application Server repository.
ADMA5053I: The library references for the installed optional
package are created.
ADMA5005I: The application oarm_war is configured in the
WebSphere Application Server repository.
ADMA5001I: The application binaries are saved in
C:\usr\IBM\WebSphere\AppServer\profiles\AppSrv01\wstemp\-
148432730\workspace\cells\PrakkyNode01Cell\applications\oarm_wa
r.ear\oarm_war.ear
ADMA5005I: The application oarm_war is configured in the
WebSphere Application Server repository.
SECJ0400I: Successfuly updated the application oarm_war with
the appContextIDForSecurity information.
ADMA5011I: The cleanup of the temp directory for application
oarm_war is complete.
ADMA5013I: Application oarm_war installed successfully.
Application oarm_war installed successfully.
To start the application, first save changes to the master
configuration.
Changes have been made to your local configuration. You can:

Save directly to the master configuration.

Review changes before saving or discarding.
To work with installed applications, click the "Manage
Applications" button.

Manage Applications
```

9. Click the **Save** link in the install trace file.

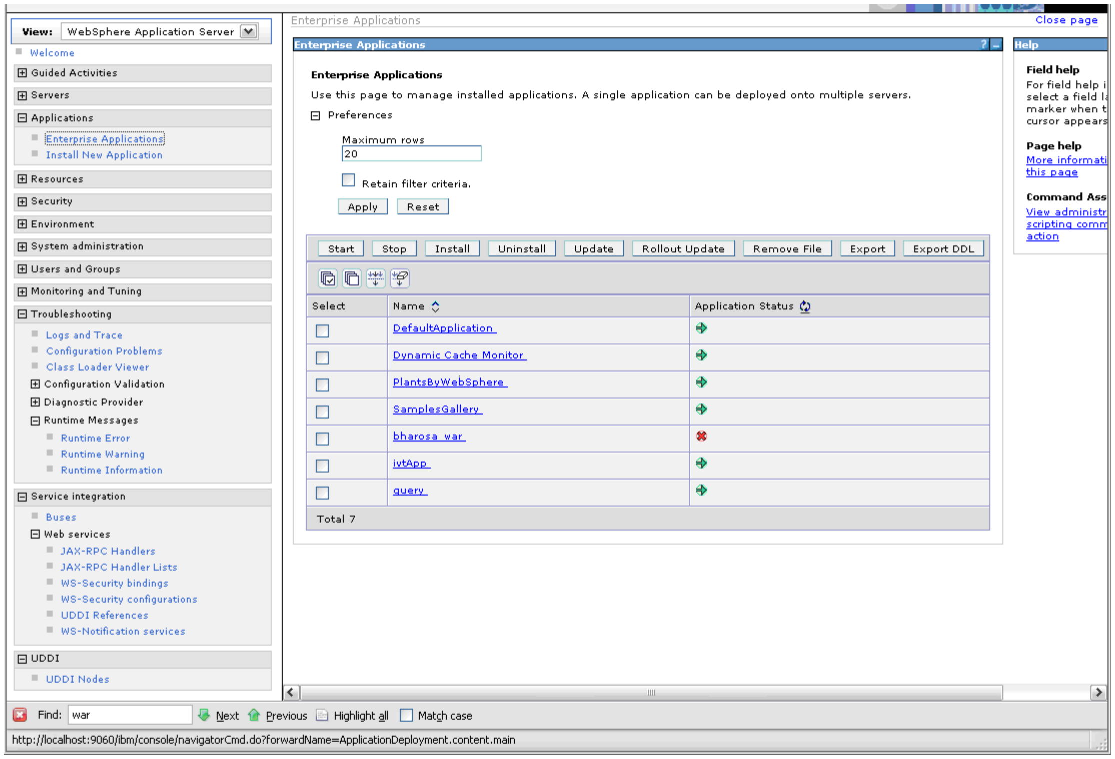


```
Save directly to the master configuration.

Review changes before saving or discarding.
To work with installed applications, click the "Manage
Applications" button.
```

10. From the Console’s left pane, select **Applications,** and then, click **Enterprise Applications** to view a list of the installed applications.

    The **Enterprise Applications** page appears, as shown below.



Enterprise Applications

Use this page to manage installed applications. A single application can be deployed onto multiple servers.

Preferences

Maximum rows: 20

□ Retain filter criteria.

Select	Name	Application Status
□	DefaultApplication	➜
□	Dynamic Cache Monitor	➜
□	PlantsByWebSphere	➜
□	SamplesGallery	➜
□	bharosa_war	✖
□	ivtApp	➜
□	query	➜
Total 7		

Find: war

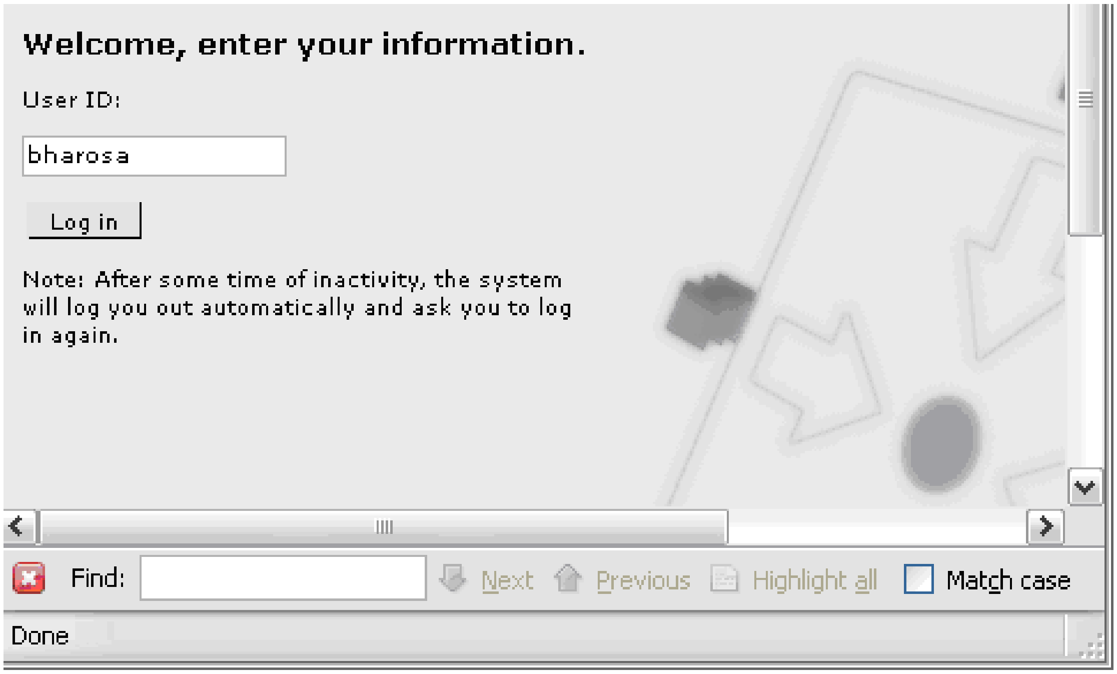
http://localhost:9060/ibm/console/navigatorCmd.do?forwardName=ApplicationDeployment.content.main

Creating Users and User Groups

1. Launch the **Administrative Console** from the **Start** menu.

   Start > **IBM WebSphere** > **Application Server V6.1** > **Profiles** > **AppSrv01** > **Administrative console**.

2. Login to the **WebSphere Application Server Administrative Console**.

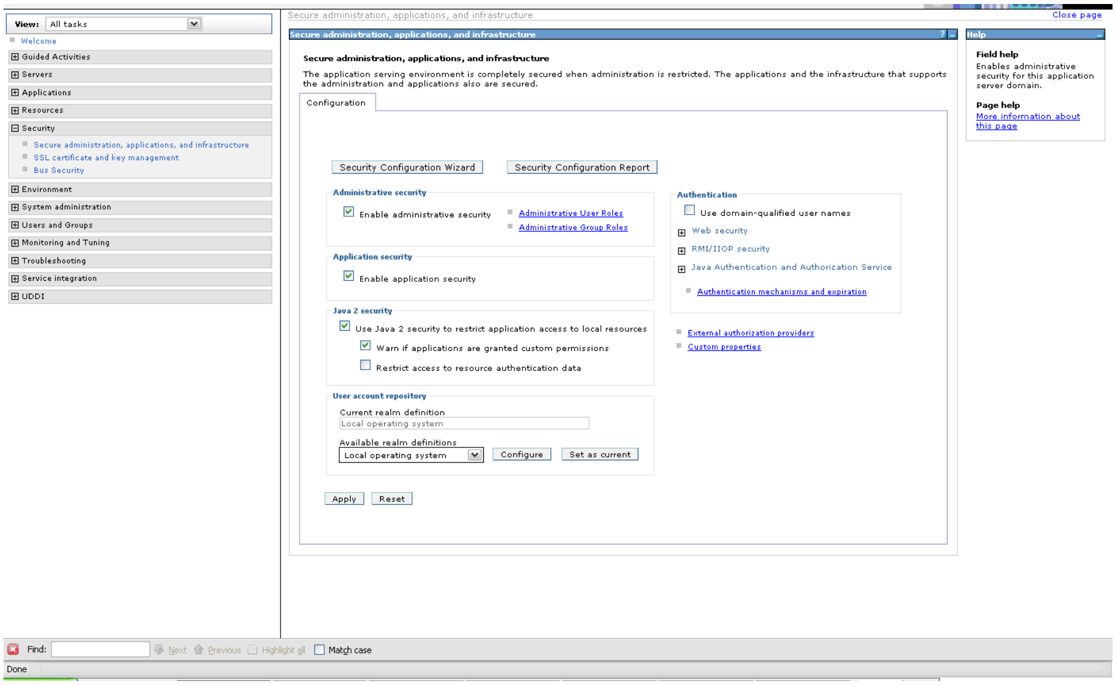


Welcome, enter your information.

User ID: bharosa

Note: After some time of inactivity, the system will log you out automatically and ask you to log in again.

3. From the Console’s left pane, select **Security**, and then, click **Secure administration, applications, and infrastructure**.
4. In the **Secure administration, applications, and infrastructure** page, select **Apply**.



Secure administration, applications, and infrastructure

Secure administration, applications, and infrastructure

The application serving environment is completely secured when administration is restricted. The applications and the infrastructure that supports the administration and applications also are secured.

Configuration

Security Configuration Wizard | Security Configuration Report

Administrative security

☑ Enable administrative security
- Administrative User Roles
- Administrative Group Roles

Application security

☑ Enable application security

Java 2 security

☑ Use Java 2 security to restrict application access to local resources

☑ Warn if applications are granted custom permissions

□ Restrict access to resource authentication data

User account repository

Current realm definition: Local operating system

Available realm definitions: Local operating system | Configure | Set as current

Authentication

□ Use domain-qualified user names

⊞ Web security

⊞ RMI/IIOP security

⊞ Java Authentication and Authorization Service

- Authentication mechanisms and expiration

- External authorization providers
- Custom properties

Apply | Reset

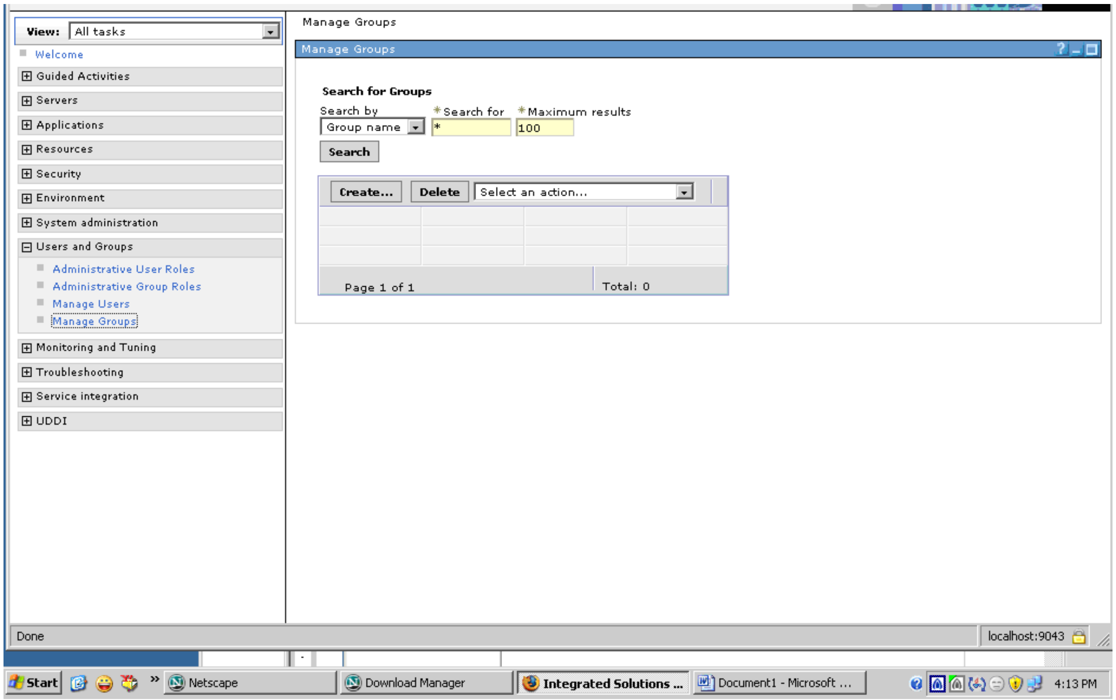
Field help

Enables administrative security for this application server domain.

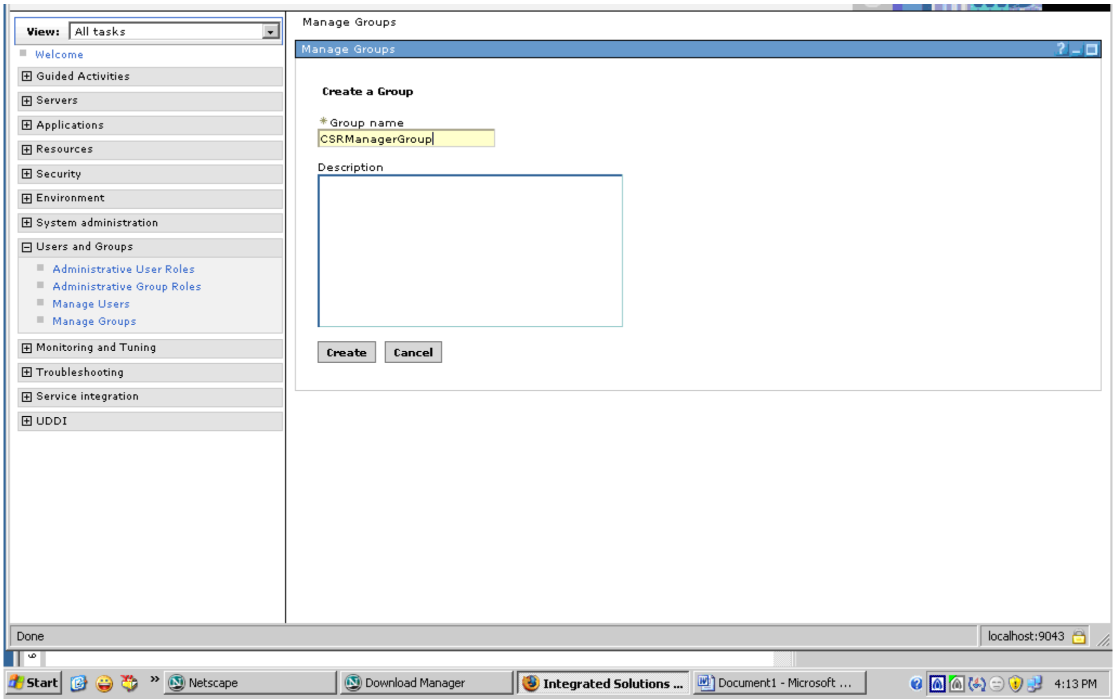
Page help

More information about this page

5. From the left pane, select **Users and Groups,** and then, click **Manage Groups**.
6. In the **Manage Groups** page, click **Create**.



The page for creating a group appears.

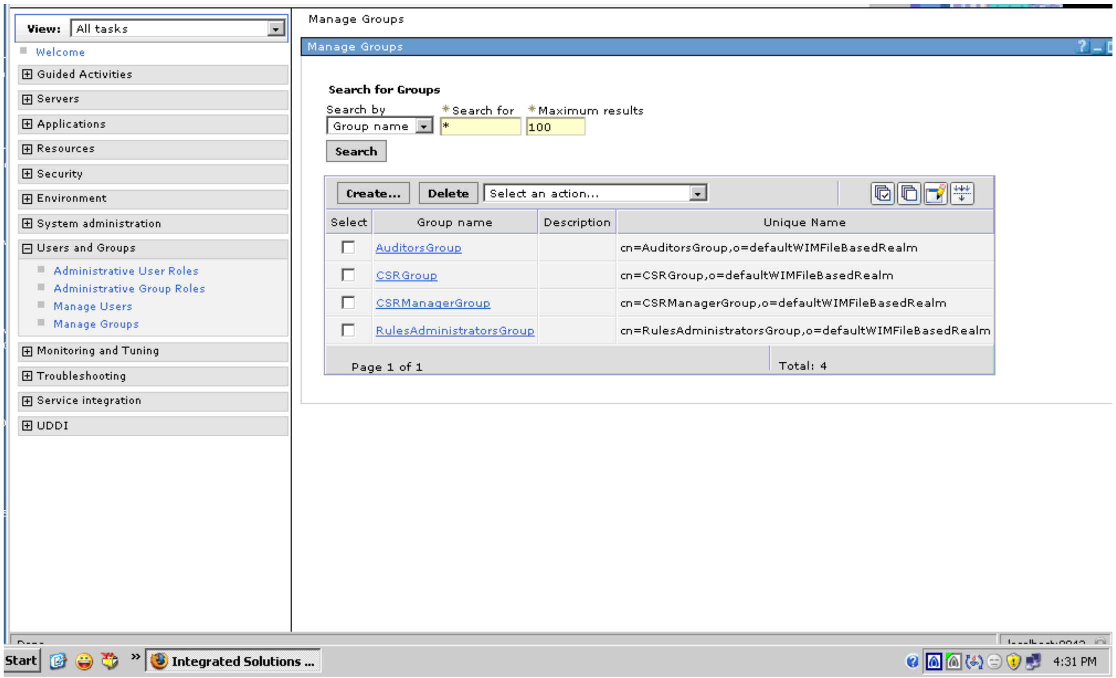


Create a Group

* Group name: CSRManagerGroup

Description

7. Create following groups:
   - CSRManagerGroup
   - CSRGroup
   - RuleAdministratorsGroup
   - AuditorsGroup



Manage Groups

Search for Groups

Search by: Group name

* Search for: *

* Maximum results: 100

Search

Select	Group name	Description	Unique Name
□	AuditorsGroup		cn=AuditorsGroup,o=defaultWIMFileBasedRealm
□	CSRGroup		cn=CSRGroup,o=defaultWIMFileBasedRealm
□	CSRManagerGroup		cn=CSRManagerGroup,o=defaultWIMFileBasedRealm
□	RulesAdministratorsGroup		cn=RulesAdministratorsGroup,o=defaultWIMFileBasedRealm

Page 1 of 1 Total: 4

8. **Optional:** Create users using the **Manage Users** option and assign these users (or existing users) to the groups previously created.

   For example, create:

   - csrm1
   - csr
   - ruleAdmin1
   - auditor1

   Then, assign:

   - csrm1 to CSRManagerGroup
   - csr to CSRGroup
   - ruleAdmin1 to RuleAdministratorsGroup
   - auditor1 to AuditorsGroup

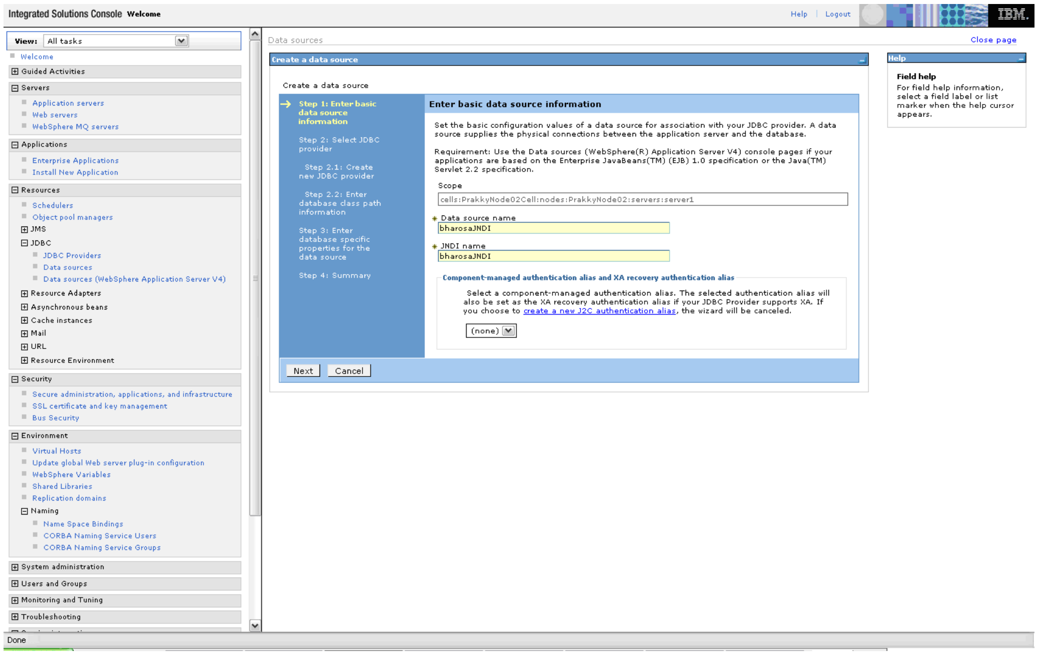
   For more information about groups, refer to the "Adaptive Risk Manager Online User Groups Reference" section of this manual.

Configuring JNDI for Adaptive Risk Manager Online on the WebSphere Application Server

1. From the Console's left pane, select **Resources**, and then, click **JDBC**.
2. Select **JDBC Providers**.
3. Enter the values as shown in the **Enter basic data source information** screen below and click **Next**.

   Data source name: bharosaJNDI

   JNDI name: bharosaJNDI



Create a data source

Enter basic data source information

Set the basic configuration values of a data source for association with your JDBC provider. A data source supplies the physical connections between the application server and the database.

Requirement: Use the Data sources (WebSphere(R) Application Server V4) console pages if your applications are based on the Enterprise JavaBeans(TM) (EJB) 1.0 specification or the Java(TM) Servlet 2.2 specification.

Scope: cells:PrakkyNode02Cell:nodes:PrakkyNode02:servers:server1

* Data source name: bharosaJNDI

* JNDI name: bharosaJNDI

Component-managed authentication alias and XA recovery authentication alias

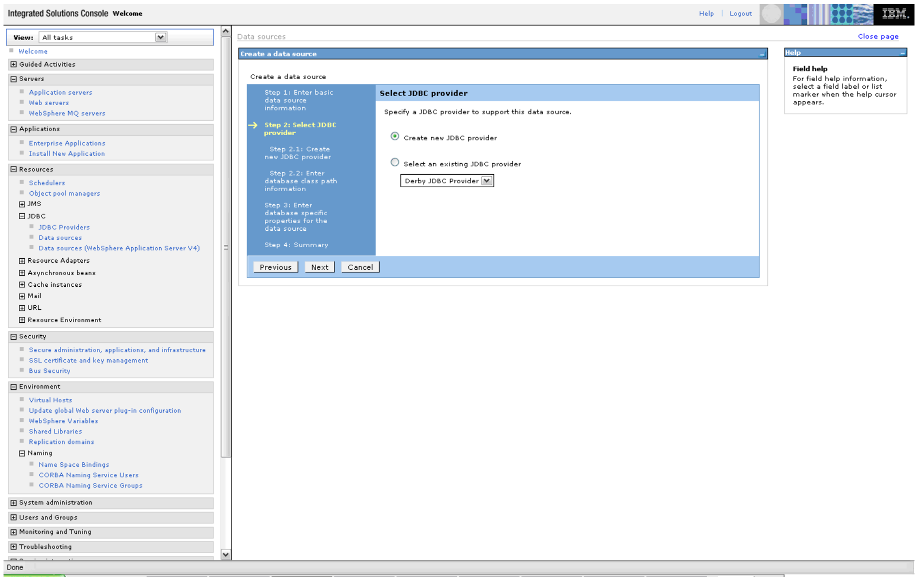
Select a component-managed authentication alias. The selected authentication alias will also be set as the XA recovery authentication alias if your JDBC Provider supports XA. If you choose to create a new J2C authentication alias, the wizard will be canceled.

(none)

Field help

For field help information, select a field label or list marker when the help cursor appears.

4. In the **Select JDBC provider** screen, select **Create new JDBC provider**.



Create a data source

Create a data source

Step 1: Enter basic data source information

→ Step 2: Select JDBC provider

Step 2.1: Create new JDBC provider

Step 2.2: Enter database class path information

Step 3: Enter database specific properties for the data source

Step 4: Summary

Select JDBC provider

Specify a JDBC provider to support this data source.

● Create new JDBC provider

○ Select an existing JDBC provider

Derby JDBC Provider

Help

Field help

For field help information, select a field label or list marker when the help cursor appears.

5. In the **Create new JDBC provider** screen, provide the following information:

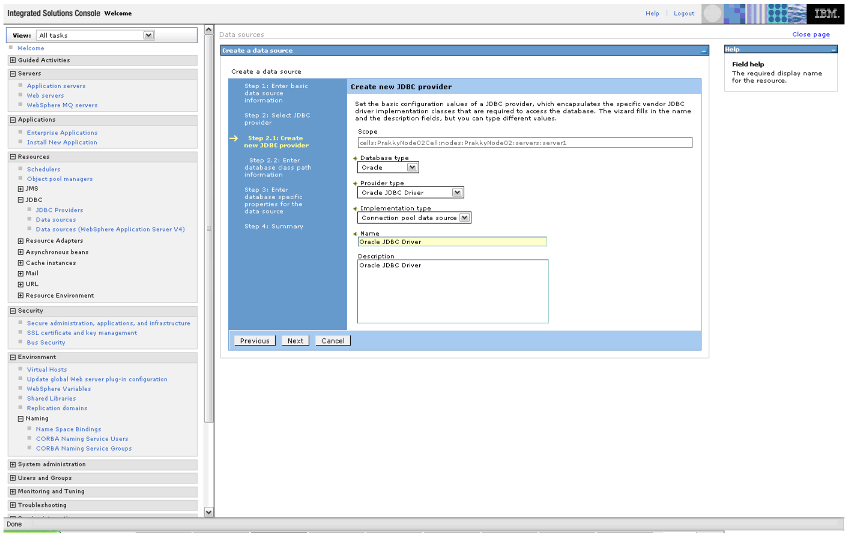
   Database type: Oracle

   Provider type: Oracle JDBC Driver

   Implementation type: Connection pool data source

   Name: Oracle JDBC Driver

   Description: Oracle JDBC Driver



Create a data source

Create a data source

Step 1: Enter basic data source information

Step 2: Select JDBC provider

→ Step 2.1: Create new JDBC provider

Step 2.2: Enter database class path information

Step 3: Enter database specific properties for the data source

Step 4: Summary

Create new JDBC provider

Set the basic configuration values of a JDBC provider, which encapsulates the specific vendor JDBC driver implementation classes that are required to access the database. The wizard fills in the name and the description fields, but you can type different values.

Scope
cells:PrakkyNode02Cell:nodes:PrakkyNode02:servers:server1

* Database type
Oracle

* Provider type
Oracle JDBC Driver

* Implementation type
Connection pool data source

* Name
Oracle JDBC Driver

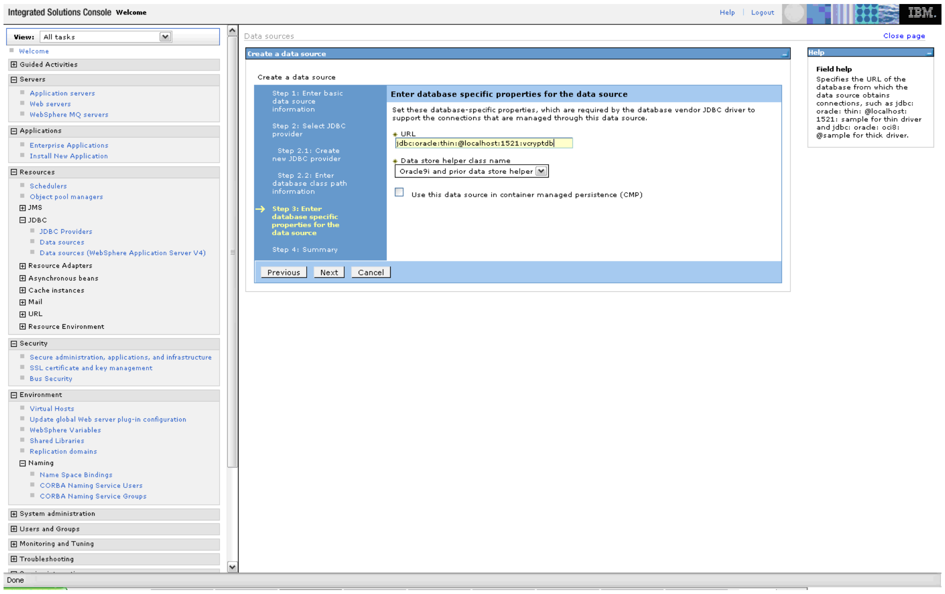
Description
Oracle JDBC Driver

Help

Field help

The required display name for the resource.

6. In the database specific properties for the data source screen, specify the directory location for "ojdbc14.jar" which is saved as a WebSphere variable ${ORACLE_JDBC_DRIVER_PATH}



Create a data source

Create a data source

Step 1: Enter basic data source information

Step 2: Select JDBC provider

Step 2.1: Create new JDBC provider

Step 2.2: Enter database class path information

→ Step 3: Enter database specific properties for the data source

Step 4: Summary

Enter database specific properties for the data source

Set these database-specific properties, which are required by the database vendor JDBC driver to support the connections that are managed through this data source.

* URL
jdbc:oracle:thin:@localhost:1521:vcryptdb

* Data store helper class name
Oracle9i and prior data store helper

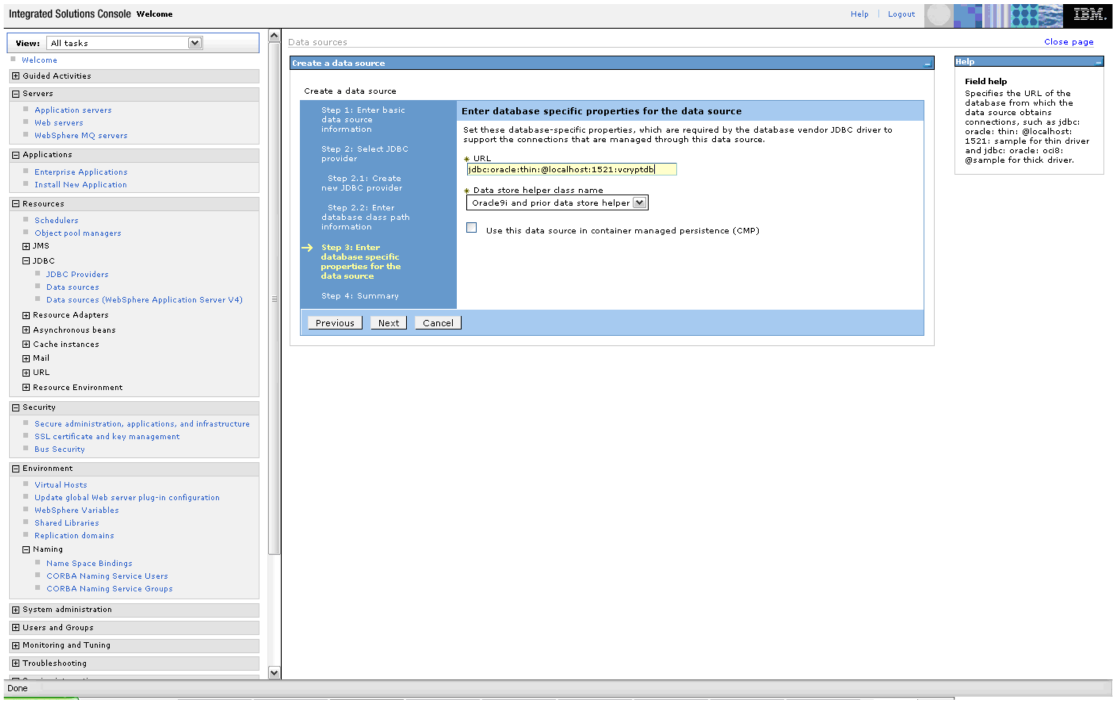
□ Use this data source in container managed persistence (CMP)

Previous | Next | Cancel

Help

Field help
Specifies the URL of the database from which the data source obtains connections, such as jdbc: oracle: thin: @localhost: 1521: sample for thin driver and jdbc: oracle: oci8: @sample for thick driver.

7. In the Summary screen, click **Finish**.



Create a data source

Create a data source

Step 1: Enter basic data source information

Step 2: Select JDBC provider

Step 2.1: Create new JDBC provider

Step 2.2: Enter database class path information

→ Step 3: Enter database specific properties for the data source

Step 4: Summary

Enter database specific properties for the data source

Set these database-specific properties, which are required by the database vendor JDBC driver to support the connections that are managed through this data source.

* URL
jdbc:oracle:thin:@localhost:1521:vcryptdb

* Data store helper class name
Oracle9i and prior data store helper

□ Use this data source in container managed persistence (CMP)

Previous | Next | Cancel

Help

Field help
Specifies the URL of the database from which the data source obtains connections, such as jdbc: oracle: thin: @localhost: 1521: sample for thin driver and jdbc: oracle: oci8: @sample for thick driver.

Setting Up Background Images

The Adaptive Strong Authenticator device uses personalized images to enhance security. Oracle provides you with a compressed file of images.

1. Uncompress the image archive to a directory inside a file system that can be accessed by Adaptive Risk Manager Online. Ensure that the directory is secure with restricted access privileges.
2. In the Adaptive Risk Manager Online's bharosa_server.properties file, update the path to point to the shared images directory.

   For example, the bharosa_server.properties code in bold type below.

```
#this is to point to the shared image directory, both
bharosa_client.properties and bharosa_server.properties

#should point to the same value

bharosa.image.dirlist=/bharosa_images/allpads/textpad/

vcrypt.user.image.dirlist.property.name=bharosa.image.dirlist
```

Note: Contact the Adaptive Risk Manager Online administrator before modifying the authentication devices information in the bharosa_server.properties file; additional properties may be required for each of the authentication devices. For an example of the bharosa_server.properties file, refer to the section, “Adaptive Risk Manager Online Server Properties Configuration.”

Setting Up Logging

Adaptive Risk Manager Online uses log4j mechanism for logging. You can configure the log output for different levels through the log4j.xml properties. You will not need to restart the application server for changes to take effect.

Possible levels include

- DEBUG
- INFO
- WARN
- ERROR
- FATAL

The recommended default level is WARN.

For more information on the various parameters, refer to <sample.log4j.xml> in the Adaptive Risk Manager Online's deployment directory.

Edits to Log4j.xml Parameters

To edit log4j.xml parameters,

1. Make a copy of <log4j.xml.sample>, which is located in the deployment directory of Adaptive Risk Manager.
2. Update the log output path for each appender.
3. Search for `<param name="File" value="` and change the file path for the logs appropriately.
4. Configure SMTP for emailing warnings and errors (optionally). Refer to the SMTP sample below.

Ensure that you make a backup copy of the `log4j.xml` file in the event that a patch is applied to the installation and you need to perform a restore.

Commonly Edited log4j.xml Parameters

A list of commonly edited log4j.xml parameters is shown below. If you want your log files to be created in a non-default location, please specify the path for log file location. Refer to the highlighted text below.

```
<appender name="FILE"
class="org.apache.log4j.DailyRollingFileAppender">
<param name="File" value="c:/bharosa_server_package/bharosa_logs
/fahost_log.log " />
<param name="DatePattern" value="'.'yyyy-MM-dd-HH" />
<layout class="org.apache.log4j.PatternLayout">
<param name="ConversionPattern" value="%d %-5p
[app=%log4j.webapp.name%] [%t] %c - %m\n" />
</layout>
</appender>
```

```
<appender name="RulePerformance"
class="org.apache.log4j.DailyRollingFileAppender">
<param name="File" value="logs/Bharosa_RulePerformance.log" />
<param name="DatePattern" value="'.'yyyy-MM-dd-HH" />
<layout class="org.apache.log4j.PatternLayout">
<param name="ConversionPattern" value="%d %-5p [%t] %c –
%m\n" />
</layout>
</appender>

<appender name="RulesLog"
class="org.apache.log4j.DailyRollingFileAppender">
<param name="File" value="c:/bharosa_server_package/bharosa_logs
Bharosa_RulesLog.log" />
<param name="DatePattern" value="'.'yyyy-MM-dd-HH" />
<layout class="org.apache.log4j.PatternLayout">
<param name="ConversionPattern" value="%d %-5p [%t] %c - %m\n" />
</layout>
</appender>

<logger name="SystemRulesTest_Performance">
<appender-ref ref=" RulePerformance " />
</logger>

<logger name="RuleLog">
<appender-ref ref="RulesLog" />
</logger>
```

To change the level of logging, update the value in <level value >. Refer to the example below:

```
<logger name="com.bharosa">
<level value="WARN" />
</logger>
```

SMTP sample

The SMTPHost can be an IP address or a hostname.

logs

```
Declare the SMTPAppender
Email appender commented
<appender name="EMAIL"  class="org.apache.log4j.net.SMTPAppender">
     <param name="BufferSize" value="512" />
     <param name="SMTPHost" value="localhost" />
     <param name="From" value="support@bharosa.com" />
     <param name="To" value="support@bharosa.com" />
     <param name="Subject" value="[app=fauio]Log4j:Bharosa" />
     <layout class="org.apache.log4j.PatternLayout">
         <param name="ConversionPattern"
            value="[%d{ISO8601}]%n%n%-5p%n%n%c%n%n%m%n%n" />
     </layout>
     <filter class="org.apache.log4j.varia.LevelRangeFilter">
             <param name="LevelMin" value="WARN"/>
             <param name="LevelMax" value="FATAL"/>
     </filter>
</appender>
```

Fraud Detection

```
     Email Appender for sending emails for alerts generated
     Alert Email appender commented
     <appender name="ALERT_EMAIL"
class="org.apache.log4j.net.SMTPAppender">
              <param name="BufferSize" value="512" />
              <param name="SMTPHost" value="localhost" />
              <param name="From" value="vadmin" />
              <param name="To" value="lenny@localhost" />
              <param name="Subject" value="[app=fauio]Log4j:Bharosa" />
              <layout class="org.apache.log4j.PatternLayout">
                   <param name="ConversionPattern"

value="[%d{ISO8601}]%n%n%-5p%n%n%c%n%n%m%n%n" />
              </layout>
       </appender>
```

Configuring TopLink

Configuring Toplink with JDBC

TopLink converts Java to SQL in order to connect to the database.

To update the sessions.xml file located under its deployment directory.

1. Save a copy of the `sessions.xml.sample` reference file as `sessions.xml` and modify the following tags with the appropriate values for your platform.
   - <platform-class>
   - <driver-class>
   - <connection-url>
   - <user-name>
   - <password>
   - <connection-pools>

   For performance reasons, make sure that the max-connections and the min-connections are set to the same value.

   Note: The password must be a TopLink encrypted password.

2. Comment out all the reference to JDBC or database connectivity in the `bharosa_server.properties` file.

For code change examples, refer to the “TopLink Reference” section.

For information about the <platform-class> properties, refer to the “TopLink Reference” section.

For more information about integrating TopLink with an application server, refer to the *Oracle TopLink Developer's Guide.*

Configuring TopLink with JNDI

To configure TopLink with JNDI,

1. Save a copy of the `sessions.xml.sample` reference file as `sessions.xml` and comment out the following tags:
   - <platform-class>
   - <driver-class>
   - <connection-url>
   - <user-name>
   - <password>

2. Then add the line, **<datasource>jdbc/oarmDS</datasource>**.

Configuring Server Properties

Database access, the scheduling of Adaptive Risk Manager Reports, Multi-tenant functionality as well as other functions can be configured for Adaptive Risk Manager Online by updating the bharosa_server.properties file located under its deployment directory.

You do not need to restart the application for the changes to the `bharosa_server.properties` file to take effect.

1. Save a copy of the bharosa_server.properties.sample reference file as bharosa_server.properties and update the appropriate values for the following entries.
   - Adaptive Risk Manager Online database access parameters
   - Adaptive Strong Authenticator images path
   - Adaptive Risk Manager Reports directory
   - Adaptive Risk Manager Scheduler

2. Comment out all the reference to JDBC or database connectivity in the `bharosa_server.properties` file.

For your reference, sample code is provided below.

```
# Database configuration

#Template start (Comment below lines if you are manually updating the
file) #

#bharosa.db.driver=oracle.jdbc.driver.OracleDriver

#bharosa.db.url=jdbc:oracle:thin:@localhost:1521:BRSADB

#bharosa.db.username=brsa_main

#bharosa.db.password=bharosa

#Template end#


#this is to point to the shared image directory, both
bharosa_client.properties and bharosa_server.properties

#should point to the same value

bharosa.image.dirlist=/bharosa_images/allpads/textpad/

vcrypt.user.image.dirlist.property.name=bharosa.image.dirlist
```

```
# where to save reports. Make sure the directory as been created.
reports.save.dir=reports

# to activate the scheduler and set the fixed rate scan
vcrypt.reports.scheduler.activate=false
vcrypt.reports.scheduler.ratescan=60
```

Loading IP Location Data

Setting Up Location Properties

1. Rename `bharosa_location.properties.sample` to `bharosa_location.properties`.
2. Update bharosa_location.properties file to set appropriate values for the following properties:
   - location.data.provider (quova or ip2location)
   - location.data.file
   - location.data.ref.file
   - location.data.anonymizer.file

A sample `bharosa_location.properties` file is shown below.

```
### IP location loader specific properties go here

### Specify the data provider: quova or ip2location or maxmind
location.data.provider=quova

### Specify the data file, for both quoval and ip2location
location.data.file=test_08132006.dat.gz

### Specify the reference file for quova
location.data.ref.file=test_08132006.ref.gz

### Specify the anonymizer data file for quova
location.data.anonymizer.file=test_anonymizer.dat.gz

### Specify the location data file, for maxmind
location.data.location.file=test_MaxMindLocation.csv
```

```
### Specify the blocks data file, for maxmind

location.data.blocks.file=test_MaxMindBlocks.csv


### Specify the country code data file, for maxmind

location.data.country.code.file=ISO_3166_CountryCode.csv


### Specify the sub country code data file, for maxmind

location.data.sub.country.code.file=FIPS_10_4_SubCountryCode.csv


### Specify the number of database threads

location.loader.database.pool.size=10


### Specify the maximum number of location records to batch before
issuing a database commit

location.loader.database.commit.batch.size=5000


### Specify the maximum time to hold an uncommitted batch

location.loader.database.commit.batch.seconds=30


### Specify the maximum number of location records to be kept in
queue for database threads

location.loader.dbqueue.maxsize=100000


### Specify the maximum number of location records to be kept in
cache

location.loader.cache.location.maxcount=25000


### Specify the maximum number of location split records to be kept
in cache

location.loader.cache.split.maxcount=25000


### Specify the maximum number of anonymizer records to be kept in
cache

location.loader.cache.anonymizer.maxcount=25000
```

Running the loadIPLocationData Script

Note: a single script is provided to load location data from any provider (Quova, IP2Location, MaxMind). The earlier versions separate scripts were used for each provider.

After configuring the property parameters, you must run the loadIPLocationData script.

From the bash shell, execute `loadIPLocationData.sh`.

From the Windows command prompt, execute `loadIPLocationData.cmd`.

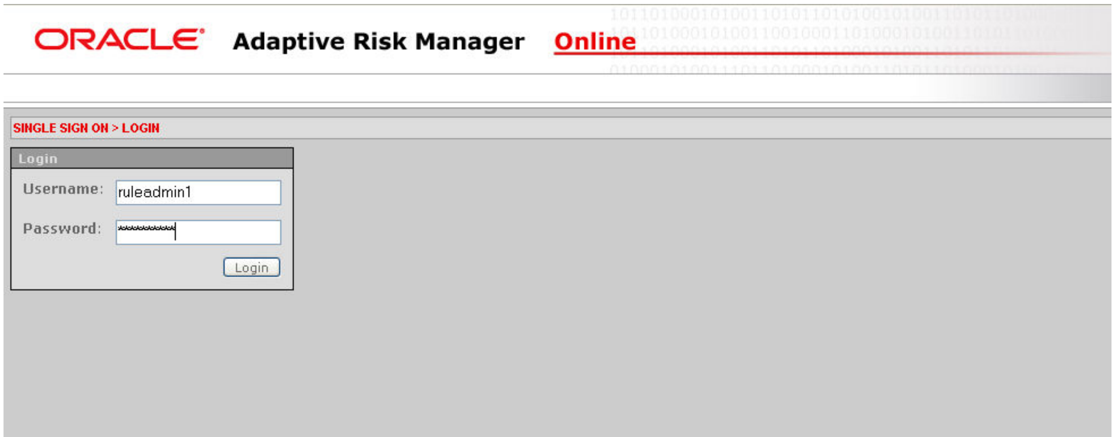
Accessing Adaptive Risk Manager Online

After the installation of Adaptive Risk Manager Online and its components into your application server and configuring your property files, you are ready to launch Adaptive Risk Manager.

WebLogic

1. Log in to Adaptive Risk Manager Online by accessing http://*localhost*:7001/oarm using the credentials of an existing user.

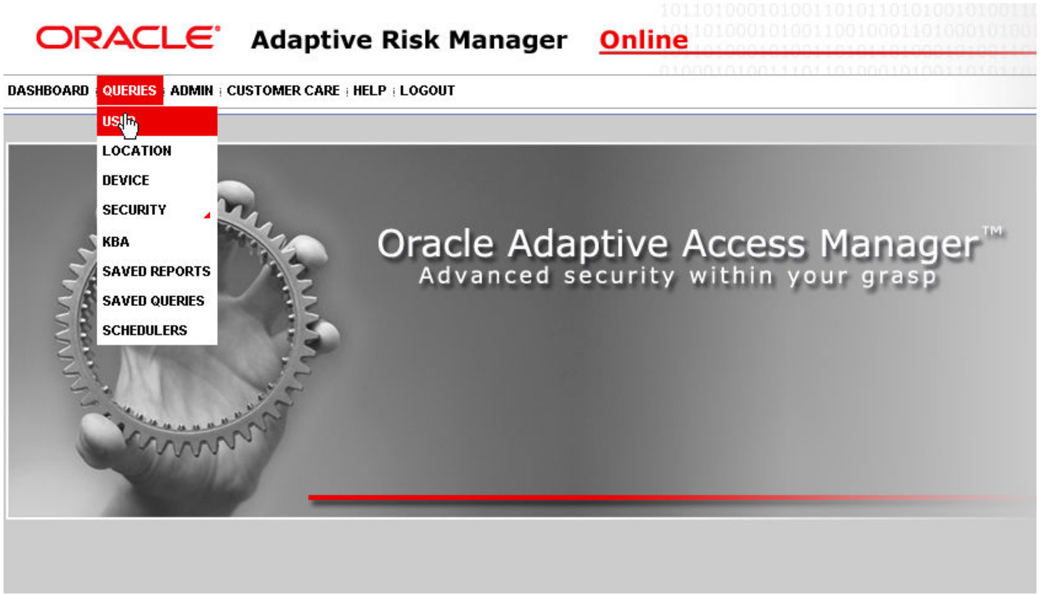
   In the example below, **ruleAdmin1** was used to login.



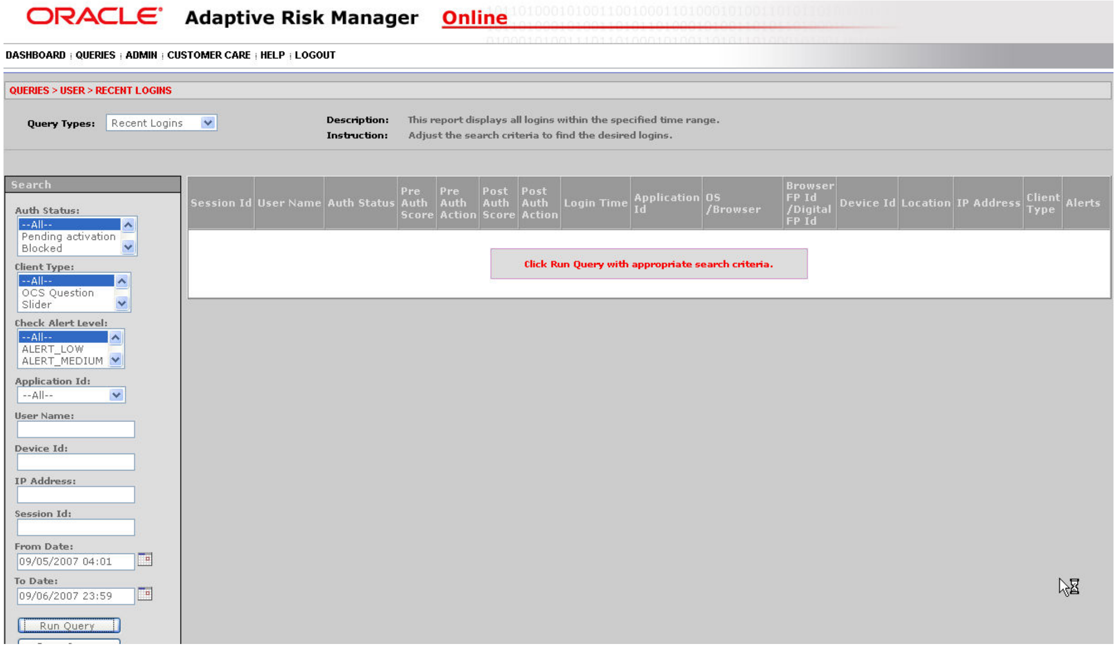
Username: ruleadmin1

Password: **********

2. From the **Queries** menu, select **User**.



3. In the left pane, click the **Run Query** button to get a report with zero or more records of all logins within the specified time range.


ORACLE Adaptive Risk Manager Online
DASHBOARD | QUERIES | ADMIN | CUSTOMER CARE | HELP | LOGOUT
QUERIES > USER > RECENT LOGINS
Search
Run Query

Query Types: Recent Logins

Description: This report displays all logins within the specified time range.

Instruction: Adjust the search criteria to find the desired logins.

Auth Status: --All-- / Pending activation / Blocked

Client Type: --All-- / OCS Question / Slider

Check Alert Level: --All-- / ALERT_LOW / ALERT_MEDIUM

Application Id: --All--

User Name:

Device Id:

IP Address:

Session Id:

From Date: 09/05/2007 04:01

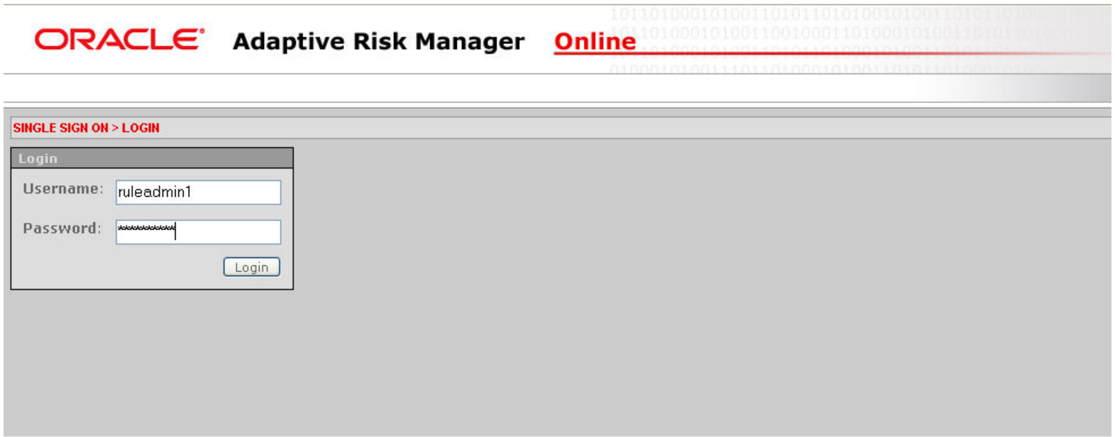
To Date: 09/06/2007 23:59

Session Id	User Name	Auth Status	Pre Auth Score	Pre Auth Action	Post Auth Score	Post Auth Action	Login Time	Application Id	OS /Browser	Browser FP Id /Digital FP Id	Device Id	Location	IP Address	Client Type	Alerts

Click Run Query with appropriate search criteria.

Tomcat

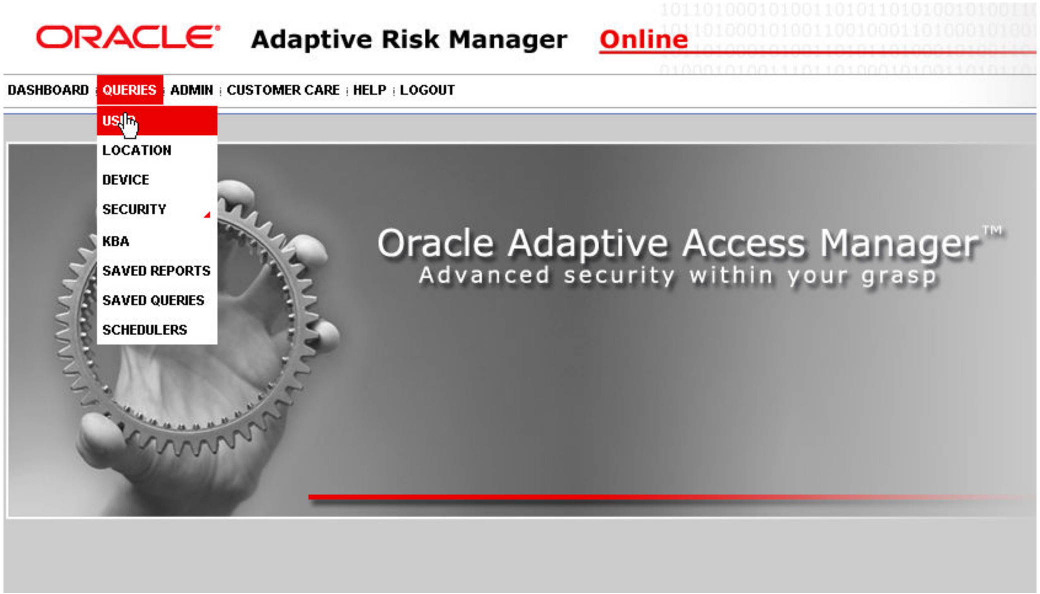
1. Log in to Adaptive Risk Manager Online by accessing http://<*localhost or IP address*>:9090/oarm with username **ruleAdmin1.**



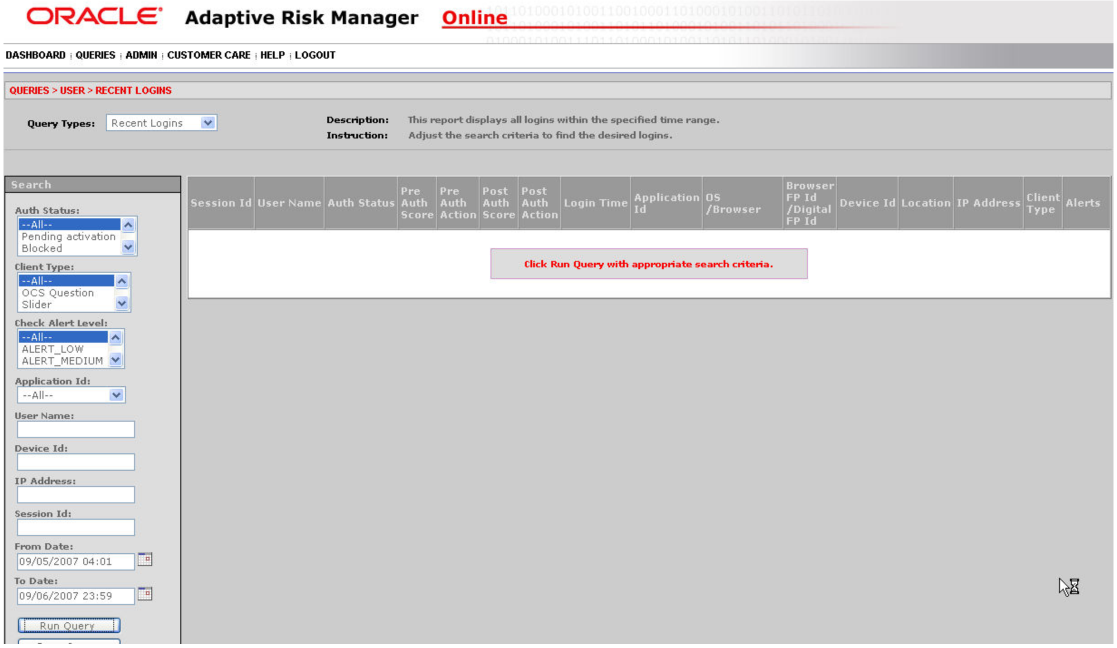
Username: ruleadmin1

Password: **********

2. From the **Queries** menu, select **User**.



3. In the left pane, click the **Run Query** button to get a report with zero or more records of all logins within the specified time range.



ORACLE Adaptive Risk Manager Online
DASHBOARD | QUERIES | ADMIN | CUSTOMER CARE | HELP | LOGOUT
QUERIES > USER > RECENT LOGINS
Search
Run Query

Query Types: Recent Logins

Description: This report displays all logins within the specified time range.

Instruction: Adjust the search criteria to find the desired logins.

Auth Status: --All-- / Pending activation / Blocked

Client Type: --All-- / OCS Question / Slider

Check Alert Level: --All-- / ALERT_LOW / ALERT_MEDIUM

Application Id: --All--

User Name:

Device Id:

IP Address:

Session Id:

From Date: 09/05/2007 04:01

To Date: 09/06/2007 23:59

Session Id	User Name	Auth Status	Pre Auth Score	Pre Auth Action	Post Auth Score	Post Auth Action	Login Time	Application Id	OS /Browser	Browser FP Id /Digital FP Id	Device Id	Location	IP Address	Client Type	Alerts

Click Run Query with appropriate search criteria.

Websphere 6.1

Log in to Adaptive Risk Manager Online by entering the URL, http://*Oracle_Adaptive_Risk_Manager_Online_Hostname* or *IP_address:port*/*Oracle_Adaptive_Risk_Manager_Online_App_Name*

Oracle Application Server

Log in to Adaptive Risk Manager Online by entering the URL, http://*Oracle_Adaptive_Risk_Manager_Online_Hostname* or *IP_address:port*/*Oracle_Adaptive_Risk_Manager_Online_App_Name*

What to Do Next

After installing the Adaptive Risk Manager Online, you should read *The Oracle® Adaptive Risk Manager™ Administrator's Guide*, which provides step-by-step instructions for creating and managing groups, creating models that contain rules, and customizing and managing rules.

Other guides you may want to refer to for setting up and using Adaptive Risk Manager Online are listed below.

- The Oracle® Adaptive Risk Manager™ Dashboard and Reporting Guide, which provides detailed instructions on how to use the dashboard and reporting functionality within the Oracle® Adaptive Risk Manager Online. The Oracle® Adaptive Risk Manager Online includes a dashboard that provides a high-level overview of users and devices that have generated alerts and the alerts themselves, and it contains a comprehensive collection of reports on users, locations, devices, and security alerts.
- The Oracle® Adaptive Risk Manager™ Customer Care Administration Guide, which provides information on creating new customer cases and administering them.

Appendix A - Adaptive Risk Manager Online User Groups Reference

The Adaptive Risk Manager Online users groups can access functionality in Adaptive Risk Manager Online based on the roles they are assigned. The four main user groups are listed as:

- CSR
- CSR Manager
- Rule Administrators
- Auditors

The roles are used to set up user roles and groups in the Application Server container. This section summarizes the main user groups, their roles, functionalities and level of access in Adaptive Risk Manager.

CSR User Group

The CSR user group has limited access.

Adaptive Risk Manager Online Functionality	**Notes**
Dashboard - No access	
Queries - No access	
Admin - No access	
Audit - No access	
Customer Care - Access to search, open and create cases. There are no outward facing hyperlinks in any of the screens. Access to a limited list of actions.	Reset User Information • Image & Phrase • Question Counter • Questions • Questions & Pick set
Preferences - Change password	CSR can change their own password
Help - Customer Care Guide	
Logout - Full access	

CSR Manager User Group

The **CSR Manager** user group has access privileges of CSR and some other limited functionality elsewhere.

CSR Manager Functionality	Notes
Dashboard - Full access	
Queries - No location based queries are allowed. See list of recommended queries below. No access to save/schedule reports.	The recommended queries are listed below. **Queries / User** • Recent Logins • Multiple Devices • First Login • Frequent Logins • Multiple Failures **Queries / Device** • Recent Logins • New Devices • Devices by User • Multiple Successful Logins • Users by Device • Multiple Failures • Multiple Users • Frequent Logins **Queries / Security** Full Access
Admin - No Access	
Audit - No access	
Customer Care - Full access. Access through hyperlinks to detailed information. Bulk close ability on search cases screen.	**Change Status** • New • Pending • Closed **Change Severity** • Low • Medium • High **Temporary Allow** • Single login • 2 hours **Cancel Temporary Allow** **Reset User Info** • Image & Phrase • Question Counter • Questions • Questions & Pick Set • Customer (All)
Preferences – Change password	CSR Manager can change their own password
Help – Customer Care Guide and Dashboard/Reporting Guide.	
Logout – Full access	

Rule Administrators User Group

The Rule Administrator user group has almost unlimited access.

Rule Administrator Functionality	Notes
Dashboard - Full access	
Queries - Full access	
Admin - Full access	
Audit - No access	
Customer Care - Full access	
Preferences - Change password	Administrators can change their own password.
Help - Customer Care Guide, Administration Guide, and Dashboard/Reporting Guide.	
Logout - Full access	

Auditors User Group

The Auditors user group only has access to Audit functionality.

Auditors Functionality	Notes
Dashboard - No access	
Queries - No access	
Admin - No access	
Audit - Full access	
Customer Care - No access	
Preferences - Change password	Auditor can change their own password
Help - No access	
Logout - Full access	

Appendix B - Multi-Tenant Access Levels Reference

A multi-tenant installation of Adaptive Risk Manager is defined as any deployment where a single instance of Adaptive Risk Manager is monitoring more than one application.

A multi-tenant access level is the term used to define access only to a certain group of customers in the customer care section of Adaptive Risk Manager Online.

For example, multiple roles of customer care access (CSR1, CSR2, and so on) would each have visibility of only customer data related to a specific application. Authorization and security policies ensure that each customer's data is kept separate from that of other customers.

Multi-Tenant Configuration Examples

The table below lists examples of a multi-tenant configuration.

User Groups	Roles	Usernames
CSR	Web_CSR, all*	CompanyCSR
	Web_CSR, Company: Bank1	Bank1csr
	Web_CSR, Company: Bank2	Bank2csr
	Web_CSR, Company: Bank3	Bank3csr
CSR Manager	Web_CSRManager, all*	Csm
	Web_CSRManager, Bank1	Csrm1
	Web_CSRManager, Bank2	Csrm2
	Web_CSRManager, Bank3	Csrm3
Rule Administrators	Web_RuleAdministrators .all*	ruleAdmin1
Auditors	Web_Auditors .all	Auditor

*All = Access to all CSR roles

In the table above,

Company: Bank1 is a user group defined for existing role of CSR. Bank1csr is the user tagged to group Company: Bank1.

Similarly Company: Bank2 is a group defined for existing role of CSR. Bank2csr is the user tagged to group Company: Bank2.

The group “all” is a reserved word that is used by the CompanyCSR to access all users in the system.

Both users are bearing the Customer Support Representatives role for different tenants with isolated data and access to customers in the same application and database.

Bank1csr who searches on user cases will get a list of Account Ids of respective Bank1 data only. Bank1csr will not be allowed to create a case on Account Ids that are not related to Bank1 while creation of cases and accessing data for Bank1 are allowed.

Multi-Tenant Configuration

To support the multi-tenant scenario, add the following properties in the bharosa_server.properties file.

```
bharosa.multitenant.boolean=true

bharosa.multitenant.enforce.admin.check=true

bharosa.extgroupid.enum.bharosaUIOGrp=1

bharosa.extgroupid.enum.bharosaUIOGrp.name=bharosaUIOGrp

bharosa.extgroupid.enum.bharosaUIOGrp.description=Bharosa UIO Group

bharosa.extgroupid.enum.bharosaUIOGrp.ldap_groups=web_ldapuser_two,
web_ldapuser_one , web_ldapuser_three

bharosa.extgroupid.enum.bharosaUIOGrp.access_control_adminusers=true
```

Appendix C - TopLink Reference

<platform-class>

Platform specific property that you modify the TopLink <platform-class> tag with are listed below.

Oracle

Oracle - generic

oracle.toplink.platform.database.OraclePlatform

Oracle9i (9.2.0.4)

oracle.toplink.platform.database.oracle.Oracle9Platform

Oracle10g (10.1.0.3)

oracle.toplink.platform.database.oracle.Oracle10Platform features

Oracle10g (10.2.0.1)

oracle.toplink.platform.database.oracle.Oracle10Platform features

Oracle Times Ten In-Memory Database (6.0.2)

oracle.toplink.platform.database.TimesTenPlatform

Microsoft

SQL Server 2005

```
oracle.toplink.platform.database.SQLServerPlatform
```

Encrypt Password Command

To encrypt a given password, use the following command:

```
java -classpath “vcrypt.jar;toplink.jar”
com.bharosa.vcrypt.utility.cmdline.BharosaCmdLine -toplink-password-
encrypt mydbpassword
```

TopLink Configuration Sample Code (JDBC)

For your reference, a sessions.xml file is provided below.

```
<?xml version="1.0" encoding="UTF-8" ?>
- <toplink-sessions version="10g Release 3 (10.1.3.1.0)"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
- <session xsi:type="server-session">
  <name>default</name>
  <event-listener-classes />
  <primary-project xsi:type="xml">BharosaTLMappings.xml</primary-project>
- <login xsi:type="database-login">
  <platform-class>oracle.toplink.platform.database.oracle.Oracle10Platform</platform-
class>
  <user-name>OARMLOAD</user-name>
  <password>bharosa</password>
- <sequencing>
- <default-sequence xsi:type="native-sequence">
  <name>Native</name>
  <preallocation-size>1</preallocation-size>
  </default-sequence>
  </sequencing>
  <driver-class>oracle.jdbc.driver.OracleDriver</driver-class>
  <connection-url>jdbc:oracle:thin:@golan.hyperion.com:1521:brsadb</connection-url>
  </login>
- <connection-pools>
- <read-connection-pool>
  <name>ReadConnectionPool</name>
  <max-connections>5</max-connections>
  <min-connections>5</min-connections>
  </read-connection-pool>
- <write-connection-pool>
  <name>default</name>
```

```
<max-connections>25</max-connections>
<min-connections>25</min-connections>
</write-connection-pool>
</connection-pools>
<connection-policy />
</session>
</toplink-sessions>
```

TopLink Configuration Sample Code (JNDI)

```
  <?xml version="1.0" encoding="UTF-8" ?>
- <toplink-sessions version="10g Release 3 (10.1.3.1.0)"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
- <session xsi:type="server-session">
  <name>default</name>
  <event-listener-classes />
  <primary-project xsi:type="xml">BharosaTLMappings.xml</primary-project>
- <login xsi:type="database-login">
  <platform-class>oracle.toplink.platform.database.oracle.Oracle10Platform</platform-class>
- <sequencing>
  - <default-sequence xsi:type="native-sequence">
      <name>Native</name>
     <preallocation-size>1</preallocation-size>
    </default-sequence>
   </sequencing>
    <datasource>jdbc/oarmDS</datasource>
     </login>
      <connection-policy />
    </session>
  </toplink-sessions>
```

Appendix D - Abbreviation Matcher Properties

Country

Country Name	**Abbreviation**
Canada	CA

State

State Name	**Abbreviation**
Alabama	AL
Alaska	AK
Arizona	AZ
Arkansas	AR
California	CA, cali, cal, calif
Colorado	CO
Connecticut	CT
Delaware	DE
Florida	FL
Georgia	GA
Hawaii	HI
Idaho	ID
Illinois	IL
Indiana	IN
Iowa	IA
Kansas	KS
Kentucky	KY
Louisiana	LA
Maine	ME
Maryland	MD
Massachusetts	MA
Michigan	MI
Minnesota	MN
Mississippi	MS
Missouri	MO
Montana	MT
Nebraska	NE
Nevada	NV
New\ Hampshire	NH
New\ Jersey	NJ
New\ Mexico	NM
New\ York	NY
North\ Carolina	NC
North\ Dakota	ND
Ohio	OH
Oklahoma	OK
Oregon	OR
Pennsylvania	PA
Rhode\ Island	RI
South\ Carolina	SC
South\ Dakota	SD
Tennessee	TN

State Name	Abbreviation
Texas	TX
Utah	UT
Vermont	VT
Virginia	VA
Washington	WA
West\ Virginia	WV
Wisconsin	WI
Wyoming	WY
District\ of\ Columbia	DC
Ontario	ON
Quebec	QC
Nova\ Scotia	NS
New\ Brunswick	NB
Manitoba	MB
British\ Columbia	BC
Prince\ Edward\ Island	PE
Saskatchewan	SK
Alberta	AB
Newfoundland\ and\ Labrador	NL
Northwest\ Territories	NT
Yukon	YT
Nunavut	NU

City

City Name	Abbreviation
Los\ Angeles	LA
San\ Francisco	SF
New\ York	NY
Santa\ Clara	SC
San\ Jose	SJ

Street

Street Name	Abbreviation
Street	St
Drive	Dr
Road	Rd
Avenue	Ave
Line	Ln
Court	Ct
Expressway	Expy
Parkway	Pkwy
Boulevard	Blvd

Car

Car Name	Abbreviation
Volkswagen	VW
Bavarian\ Motor\ Works	BMW

Car Name	**Abbreviation**
four wheel\ drive	4WD
sports\ utility\ vehicle	SUV
General\ Motors\ Corporation	GMC

Video Game

Video Game Name	**Abbreviation**
Role\ playing\ game	RPG
Real\ time	RTS
Heroes\ of\ Might\ and\ Magic	HoMM
World\ of\ warcraft	WoW
Lord\ of\ the\ Rings	LoTR

Appendix E - Troubleshooting

This section describes solutions to common problems you might encounter when installing the Adaptive Risk Manager Online.

Jar command not found

Ensure that the JAVA_HOME environment variable is set to point to the Java installation directory. For example /usr/java.

Also check that the CLASSPATH or PATH environment variable is defined and has the Java core libraries listed (among other items). For example, CLASSPATH=/usr/java/lib/.

Images are not displayed in Adaptive Risk Manager Online

Check the Adaptive Risk Manager Online images path configured in bharosa_server.properties.

Log4j errors

Check the Adaptive Risk Manager Online images path configured in the bharosa_server.properties.

Note that Async Appenders are not recommended in the log4j configuration.

SOAP service calls throws exceptions

Check if the remote calls do not have DNS lookup or network connectivity. Please check DNS lookup capabilities.

Adaptive Risk Manager Online is not accessible

Check the port on which the Application Server is active and serving the Adaptive Risk Manager Online Application.

Make sure DNS entry is correct and/or IP Address is accessible.

Unable to login into Adaptive Risk Manager

Check that the user id has access and is a member of the predefined roles. The roles are defined in the Application Server Container for Adaptive Risk Manager.

Adaptive Risk Manager Online is accessible but queries returns database errors

Check the database access credentials set in the bharosa_server.properties of Adaptive Risk Manager.

Check that the TCP/IP port specified on the database server for database access is correct and the database server is listening on the port.

Adaptive Risk Manager Online Application throws timeout errors

Check the time out settings for the application server. The user session times out after no activity from user value must be equal to the value set in the Application server container settings.

Unable to see all the menus in Adaptive Risk Manager Online

Check that the user id is a member of the predefined roles, which were defined in the Application Server Container for Adaptive Risk Manager.

Unable to reset all User Information from Adaptive Risk Manager Online Customer Care

Check that the user id accessing Adaptive Risk Manager Online customer care is a member of the predefined roles, which were defined in the Application Server Container for Adaptive Risk Manager.

The Adaptive Risk Manager Online sample webapp deployed to latest WebSphere 6.1 throws an error

The following error message appears:

```
The EAR file might be corrupt or incomplete.

org.eclipse.jst.j2ee.commonarchivecore.internal.exception.DeploymentD
escriptorLoadException: WEB-INF/web.xml
```

Solution 1

The error is due to J2EE spec. backward compatibility from IBM Websphere as noted here - http://www-1.ibm.com/support/docview.wss?uid=swg24009603

The following lines from web.xml needs to be changed:

Old snippet:

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<!DOCTYPE web-app
    PUBLIC "-//Sun Microsystems, Inc.//DTD Web Application 2.3//EN"
    "http://java.sun.com/dtds/web-app_2_3.dtd">
```

New snippet:

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE web-app PUBLIC "-//Sun Microsystems, Inc.//DTD Web Application
2.2//EN" "http://java.sun.com/j2ee/dtds/web-app_2_2.dtd">
```

Solution 2

The error is caused by:
org.eclipse.jst.j2ee.commonarchivecore.internal.exception.DeploymentDescriptorLoadException: META-INF/application.xml

Make sure the Web Archive (war) is correctly deployed as an EAR file. It’s recommended to deploy using the WAS Admin Console app.

SunJCE Error

Error Message: com.sun.crypto.provider.SunJCE
Error Code: 500
Target Servlet: action
Error Stack:

```
java.lang.NoClassDefFoundError: com.sun.crypto.provider.SunJCE
    at java.lang.J9VMInternals.verifyImpl(Native Method)
```

Make sure the CLASSPATH has jce.jar included. You may need to change the JAVA_HOME to point to non-default Java (default is from IBM which doesn't contain JCE jars). Set **bharosa.security.provider.use.default=true** in **bharosa_server.properties.**

References:

- ftp://ftp.software.ibm.com/software/webserver/appserv/library/v61/wasv610base_i_devdep.pdf
- http://www-306.ibm.com/software/webservers/appserv/was/library/