

Adaptive Risk Manager Offline
Installation Guide
10g (10.1.4.3.0)

December 2007

ORACLE®

Copyright © 2007, Oracle. All rights reserved.

The Programs (which include both the software and documentation) contain proprietary information; they are provided under a license agreement containing restrictions on use and disclosure and are also protected by copyright, patent, and other intellectual and industrial property laws. Reverse engineering, disassembly, or decompilation of the Programs, except to the extent required to obtain interoperability with other independently created software or as specified by law, is prohibited.

The information contained in this document is subject to change without notice. If you find any problems in the documentation, please report them to us in writing. This document is not warranted to be error-free. Except as may be expressly permitted in your license agreement for these Programs, no part of these Programs may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose.

If the Programs are delivered to the United States Government or anyone licensing or using the Programs on behalf of the United States Government, the following notice is applicable:

U.S. GOVERNMENT RIGHTS Programs, software, databases, and related documentation and technical data delivered to U.S. Government customers are "commercial computer software" or "commercial technical data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the Programs, including documentation and technical data, shall be subject to the licensing restrictions set forth in the applicable Oracle license agreement, and, to the extent applicable, the additional rights set forth in FAR 52.227-19, Commercial Computer Software--Restricted Rights (June 1987). Oracle USA, Inc., 500 Oracle Parkway, Redwood City, CA 94065.

The Programs are not intended for use in any nuclear, aviation, mass transit, medical, or other inherently dangerous applications. It shall be the licensee's responsibility to take all appropriate fail-safe, backup, redundancy and other measures to ensure the safe use of such applications if the Programs are used for such purposes, and we disclaim liability for any damages caused by such use of the Programs.

Oracle is a registered trademark of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.

The Programs may provide links to Web sites and access to content, products, and services from third parties. Oracle is not responsible for the availability of, or any content provided on, third-party Web sites. You bear all risks associated with the use of such content. If you choose to purchase any products or services from a third party, the relationship is directly between you and the third party. Oracle is not responsible for: (a) the quality of third-party products or services; or (b) fulfilling any of the terms of the agreement with the third party, including delivery of products or services and warranty obligations related to purchased products or services. Oracle is not responsible for any loss or damage of any sort that you may incur from dealing with any third party.

Contents

Preface.....	5
Documentation	5
Introduction	7
Prerequisites and Dependencies.....	8
Requirements.....	9
RAM.....	9
Database	9
Application Server	9
Software	9
Operating System.....	9
Performance	10
Creating Adaptive Risk Manager Offline Database.....	11
Loading IP Location Data	11
Deploying Adaptive Risk Manager Offline	11
Oracle Application Server.....	12
Installing Adaptive Risk Manager Online into Oracle Application Server	12
Creating Groups and Adding Users.....	20
WebLogic.....	24
Creating Groups and Adding Users to Groups from the WebLogic Administration Console.....	24
Deploying the Adaptive Risk Manager Offline Application WAR File.....	28
Tomcat.....	36
Notes on Tomcat	36
Creating Roles and Adding Users from the Tomcat Web Server Administration Tool	36
Deploying the Adaptive Risk Manager Offline Application WAR.....	40
IBM WebSphere Application Server 6.1.....	42
Using the Launchpad to Start the Installation.....	42
Verifying the WebSphere Installation	44
Installing the Oracle Adaptive Risk Manager Offline Web Applications	46
Creating Users and User Groups	50
Configuring JNDI for Adaptive Risk Manager Offline on the WebSphere Application Server	53
Setting Up Logging	56
Edits to Log4j.xml Parameters	56
Commonly Edited log4j.xml Parameters	56
SMTP sample	58
logs	58

Fraud Detection	58
Configuring TopLink.....	59
Configuring Toplink with JDBC.....	59
Configuring TopLink with JNDI.....	59
Configuring Server Properties	60
Accessing Adaptive Risk Manager Offline.....	61
Usage.....	63
Customized Loading Process	63
Appendix A - Adaptive Risk Manager Offline User Groups Reference	64
CSR User Group	64
CSR Manager User Group	65
Rule Administrators User Group	66
Auditors User Group.....	66
Appendix B -TopLink Reference.....	67
<platform-class>	67
Oracle	67
Microsoft	67
Encrypt Password Command.....	68
TopLink Configuration Sample Code (JDBC)	68
TopLink Configuration Sample Code (JNDI).....	70

Preface

Adaptive Risk Manager Offline is an offline fraud analysis tool that evaluates existing transaction data for two main purposes:

- First, Adaptive Risk Manager Offline can be used as a stand alone security tool to analyze, detect and alert high risk transactions.
- Secondly, Adaptive Risk Manager Offline can be used in conjunction with Adaptive Risk Manager Online as a supplemental offline analysis tool and as a way to pre-visualize rules against real customer data without impacting customers in real-time environment.

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

After you have completed the installation procedures, refer to the *Adaptive Risk Manager Offline Administrator's Guide* for information on how to use the Adaptive Risk Manager Offline to evaluates existing transaction data.

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 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 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 Web UIO 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 on importing and exporting groups, rule templates, and models to and 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 Offline is an offline fraud analysis tool that can be used

- As a stand alone security tool to analyze, detect and alert high risk transactions
- In conjunction with Adaptive Risk Manager Online as a supplemental offline analysis tool
- As a way to visualize rules against real customer data without impacting customers in real-time environment

The purpose of this manual is to guide you through the installation and configuration of Adaptive Risk Manager Offline.

Prerequisites and Dependencies

The prerequisites and dependencies for the installation and configuration of Adaptive Risk Manager Offline 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.
Adaptive Risk Manager Offline database	Adaptive Risk Manager Offline has its own database that has an identical schema to that of the Adaptive Risk Manager Online version. Customer login and/or transaction data must be loaded into the Adaptive Risk Manager Offline database, and Adaptive Risk Manager Offline uses this database to perform risk analysis. For the Adaptive Risk Manager Offline database, follow the instructions in the <i>Oracle Adaptive Access Manager Database Installation Guide (Oracle)</i> or the <i>Oracle Adaptive Access Manager Database Installation Guide for SQL Server</i> for creating the database schema and populating it with the default values.
File Write Permission	The Adaptive Risk Manager Offline 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.
Port Configuration	Ensure that the port used by the Adaptive Risk Manager Offline Application server is accessible to the client machine. You are allowed to configure the port number.

Requirements

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.

Creating Adaptive Risk Manager Offline Database

Adaptive Risk Manager Offline has its own database that has an identical schema to that of the Adaptive Risk Manager Online version. Customer login and/or transaction data must be loaded into the Adaptive Risk Manager Offline database, and Adaptive Risk Manager Offline uses this database to perform risk analysis.

For the Adaptive Risk Manager Offline database, 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 database schema and populating it with the default values.

Loading IP Location Data

For information on importing the IP location data into the Adaptive Risk Manager Offline database, refer to the *Oracle® Adaptive Access Manager IP Location Data Import Guide*.

The location data is used by the risk policies framework to determine the risk of fraud associated with a given IP address.

Note: The process of loading the information may take around 5 hours.

Deploying Adaptive Risk Manager Offline

This section provides instructions for the deployment and installation of Adaptive Risk Manager Offline into the following application servers.

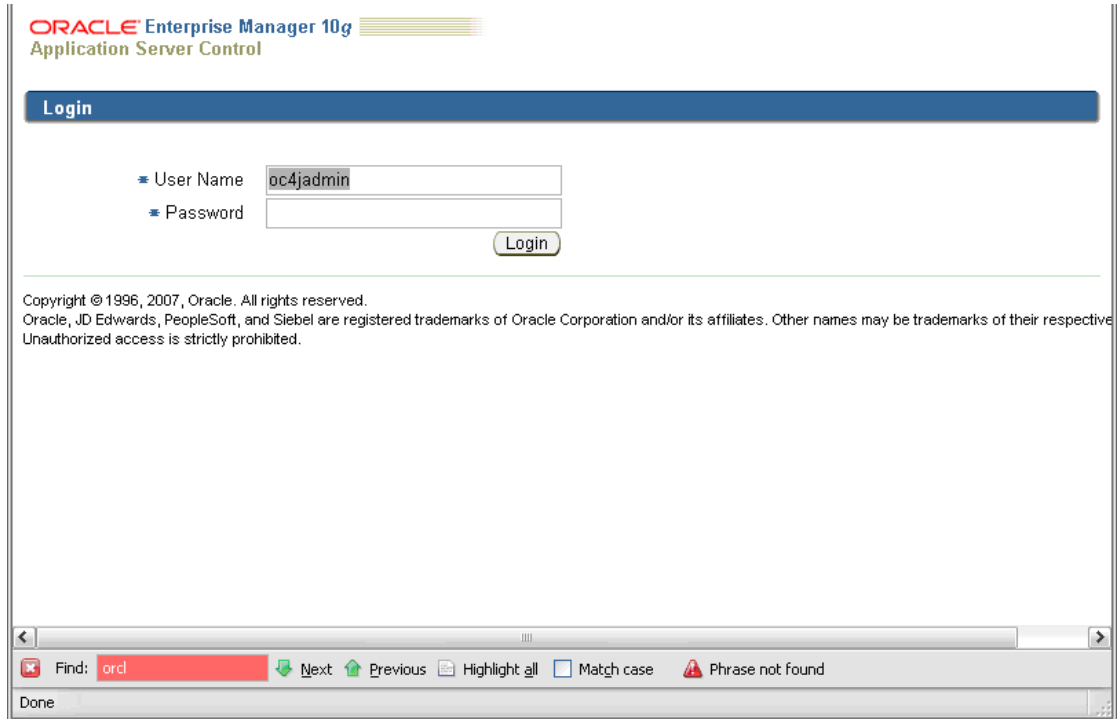
- Oracle Application Server
- WebLogic
- Tomcat
- Websphere 6.1

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

Oracle Application Server

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**.



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

ORACLE Enterprise Manager 10g
Application Server Control

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)
<input type="checkbox"/>		▼ All Application Servers					
<input type="checkbox"/>		▼ oaaminst.localhost.localdomain			localhost.localdomain		
<input type="checkbox"/>		▶ home	↑	OC4J		9.52	129.98
<input type="checkbox"/>		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.

(Start) (Stop)

Select Name ^	Status	Application Server
<input checked="" type="radio"/> home	↑	oaaminst.localhost.localdomain

Related Links

Cluster MBean Browser

Setup | Logs | Help | Logout

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

Done Local intranet 100%

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

ORACLE Enterprise Manager 10g
Application Server Control
Cluster Topology > Application Server: oaaminst1.localhost.localdomain >
OC4J: home

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

Home Applications Web Services Performance Administration

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 [g](#)

Response and Load

10:32:11 AM Dec 13, 2007

Request Processing Time (seconds)
Requests per second

Copyright © 1996, 2005, Oracle. All rights reserved. Setup | Logs | Help | Logout

Done Local intranet 100%

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

ORACLE Enterprise Manager 10g
Application Server Control
Cluster Topology > Application Server: oaaminst1.localhost.localdomain >
OC4J: home

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

Home Applications Web Services Performance Administration

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

View Applications

(Start) (Stop) (Restart) (Undeploy) (Redeploy) (Deploy)

Expand All | Collapse All

Select Name	Status	Start Time	Active Requests	Request Processing Time (seconds)	Active EJB Methods	Application Defined MBeans
▼ All Applications						
○ ascontol	↑	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	
○ hcdj	↑	Dec 13, 2007 12:28:18 PM PST	0	0.00	0	

Home Applications Web Services Performance Administration

Copyright © 1996, 2005, Oracle. All rights reserved. Setup | Logs | Help | Logout

Done Local intranet 100%

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

ORACLE Enterprise Manager 10g
Application Server Control

Setup | Logs | Help | Logout

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

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 j2eeHome

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

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 j2eeHome

Cancel | Step 1 of 3 | Next

Setup | Logs | Help | Logout

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

Done Local intranet 100%

- 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.

ORACLE Enterprise Manager 10g
Application Server Control

Help | Logout

Deploy: **Application Attributes**

Cancel | Back | Step 2 of 3 | Next

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

* Application Name

Parent Application default

Bind Web Module to Site default-web-site

Web Module	Context Root
Oracle Adaptive Risk Manager	fauo

Cancel | Back | Step 2 of 3 | Next

Help | Logout

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

Done Local intranet 100%

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

ORACLE Enterprise Manager 10g
Application Server Control

Help Logout

Select Archive Application Attributes **Deployment Settings**

Deploy: Deployment Settings Cancel Back Step 3 of 3 Deploy

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. Edit Deployment Plan

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. Save Deployment Plan

Cancel Back Step 3 of 3 Deploy

Copyright © 1996, 2005, Oracle. All rights reserved. Help | Logout

Local intranet 100%

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)**
 Archive Location: **/home/bharosa/fauiio.war**
 Deployment Plan: **Creating a new plan**

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

Import Shared Libraries

The following table lists the shared libraries installed in this OCAJ 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				<input type="checkbox"/>
adf-oracle.domain	10.1.3			<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
global.libraries	1.0			<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
global.tag.libraries	1.0			<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
global.wsm.libraries	1.0				<input type="checkbox"/>
oracle.cache	10.1.3			<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
oracle.dms	3.0			<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
oracle.expression-evaluator	10.1.3				<input type="checkbox"/>
oracle.gdk	10.1.0_2			<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
oracle.http.client	10.1.3				<input type="checkbox"/>

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.	<input type="checkbox"/>
Add Another Row	

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

Deploy: Deployment Settings

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

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

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.

[Deploy](#)

12. Click **OK**.

Deployment Settings: Configure Class Loading

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**

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				<input type="checkbox"/>
adf.oracle.domain	10.1.3			<input checked="" type="checkbox"/>	<input type="checkbox"/>
global.libraries	1.0			<input checked="" type="checkbox"/>	<input type="checkbox"/>
global.tag.libraries	1.0			<input checked="" type="checkbox"/>	<input type="checkbox"/>
global.wsm.libraries	1.0				<input type="checkbox"/>
oracle.cache	10.1.3			<input checked="" type="checkbox"/>	<input type="checkbox"/>
oracle.dms	3.0			<input checked="" type="checkbox"/>	<input type="checkbox"/>
oracle.expression-evaluator	10.1.3				<input type="checkbox"/>
oracle.gdk	10.1.0.2			<input checked="" type="checkbox"/>	<input type="checkbox"/>
oracle.http.client	10.1.3				<input type="checkbox"/>

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.	

[Add Another Row](#)

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 12:48:38 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_3/2ee/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 msec
  
```

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 constraints:

```
<!--
  <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

[Add Group](#)

Select Name
No groups found using the specified User Manager

Users

[Add User](#)

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

Security Roles

[Map Role To Principals](#)

Select Name	Assigned Users	Assigned Groups
<input checked="" type="radio"/> web_CSR		
<input type="radio"/> web_RuleAdministrators		
<input type="radio"/> web_CSRManager		
<input type="radio"/> web_Auditors		
<input type="radio"/> web_CSRInvestigator		

[Logs](#) | [Topology](#) | [Preferences](#) | [Help](#)

Copyright © 1996, 2006, Oracle. All rights reserved.
[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

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

Security: Add Group

Name:

Description:

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

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

Security: Add User

General

Name:

Description:

Password:

Confirm Password:

Group Memberships

Select All | Select None

Select Group Name

<input type="checkbox"/>	jazn.com/web_Auditors
<input type="checkbox"/>	jazn.com/web_CSR
<input type="checkbox"/>	jazn.com/web_CSRManager
<input checked="" type="checkbox"/>	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.

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

Page Refresh

Principals

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

Groups Add Group

Remove

Select Name

- jazn.com/web_Auditors
- jazn.com/web_CSR
- jazn.com/web_CSRManager
- jazn.com/web_RuleAdministrators

Users Add User

Remove

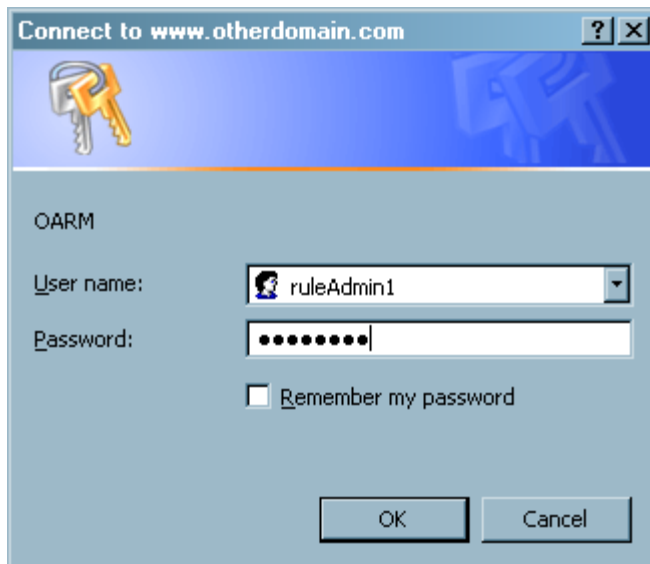
Select Name	Group Memberships
<input checked="" type="radio"/> jazn.com/auditor1	jazn.com/web_Auditors
<input type="radio"/> jazn.com/csr1	jazn.com/web_CSR
<input type="radio"/> jazn.com/csr1	jazn.com/web_CSRManager
<input type="radio"/> jazn.com/ruleAdmin1	jazn.com/web_RuleAdministrators

Security Roles

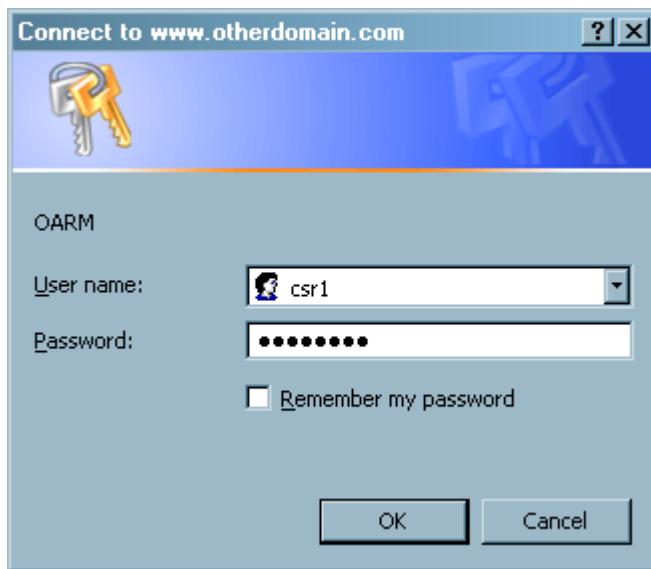
Map Role To Principals

Select Name	Assigned Users	Assigned Groups
<input checked="" type="radio"/> web_CSR		jazn.com/web_CSR
<input type="radio"/> web_RuleAdministrators		jazn.com/web_RuleAdministrators
<input type="radio"/> web_CSRManager		jazn.com/web_CSRManager

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



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



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

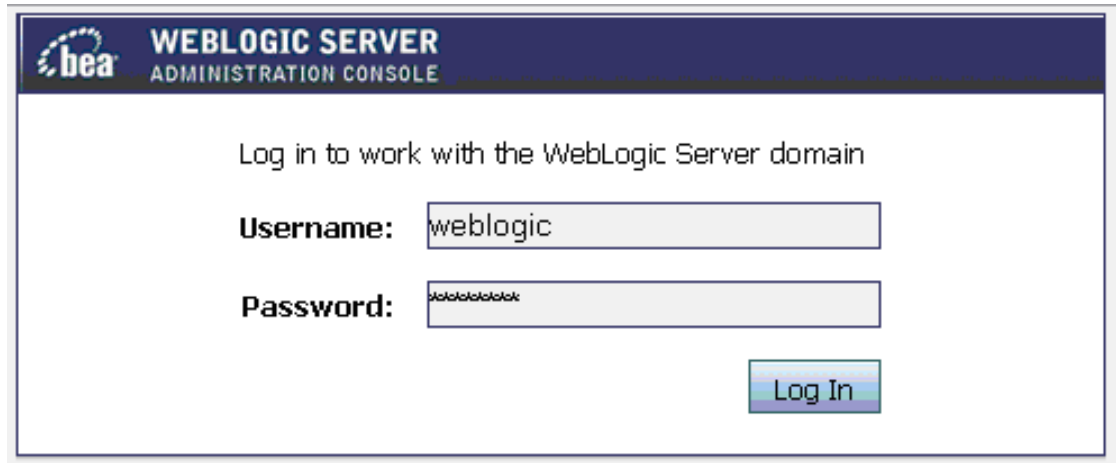
To create groups and add users

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

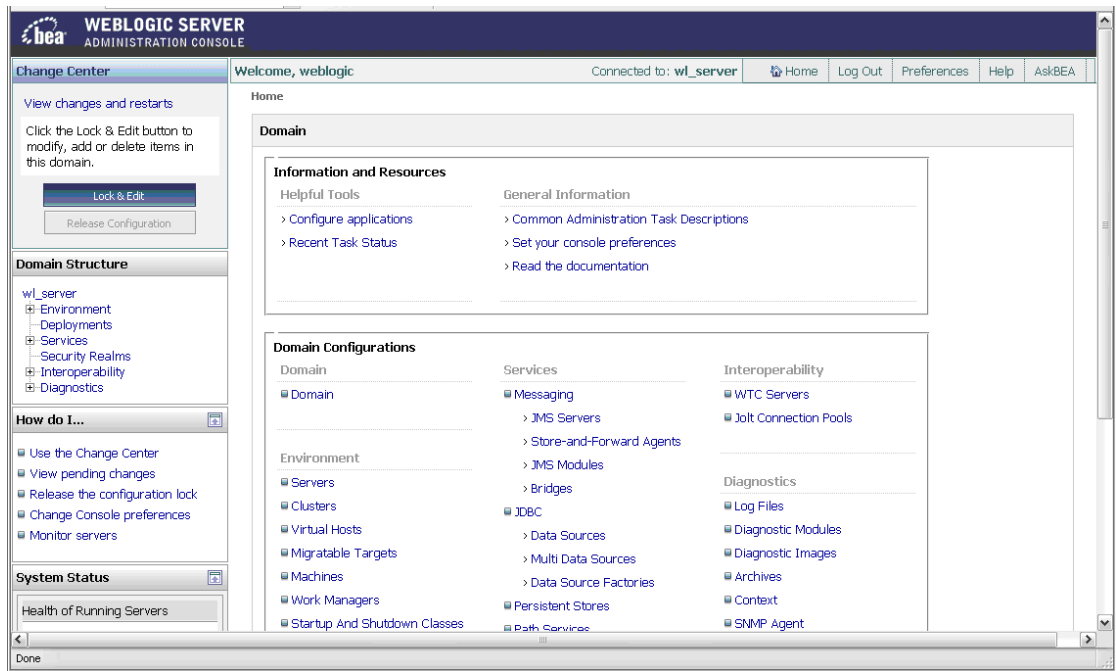
The hostname is the DNS name or IP address of the Administration Server.

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

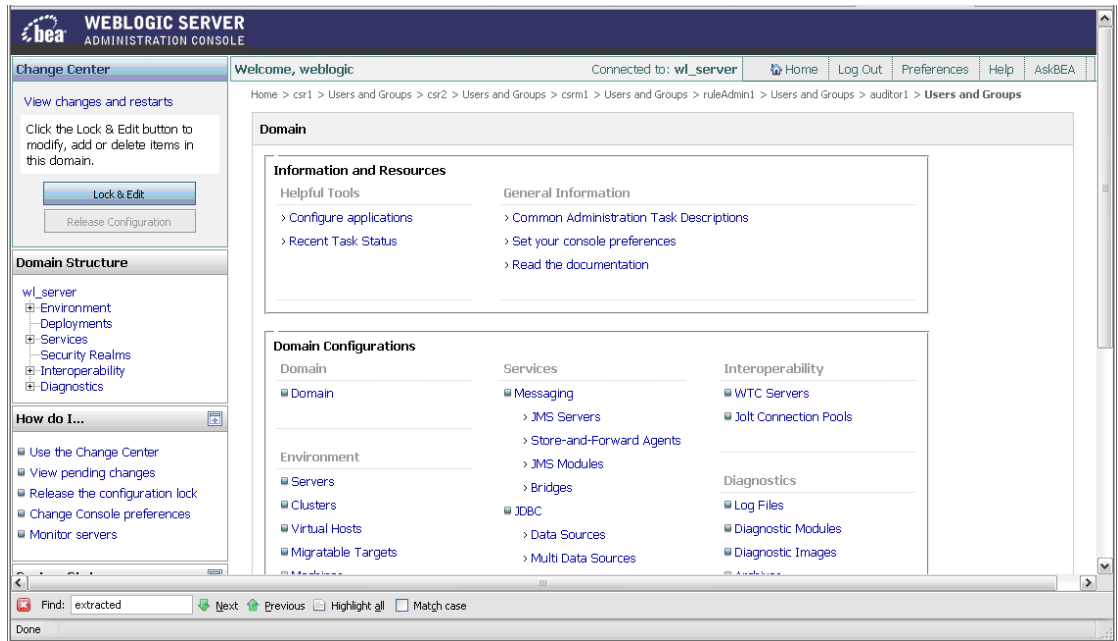
In the example below, **weblogic** was used to log in.



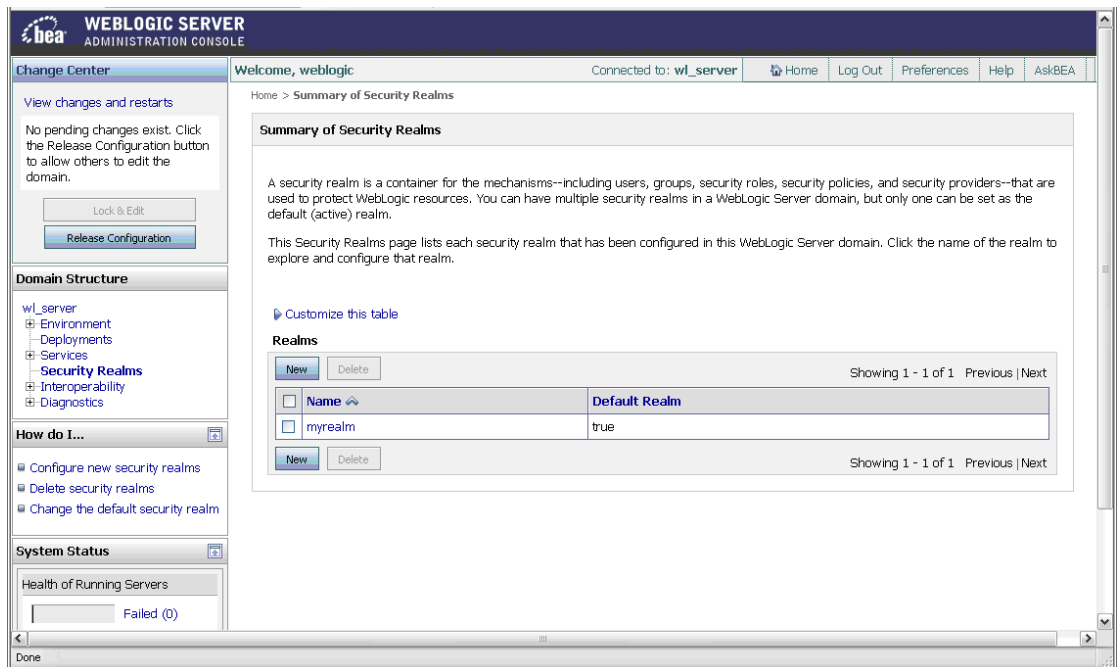
2. In the left pane, click the **Lock & Edit** button under the **Change Center** section.



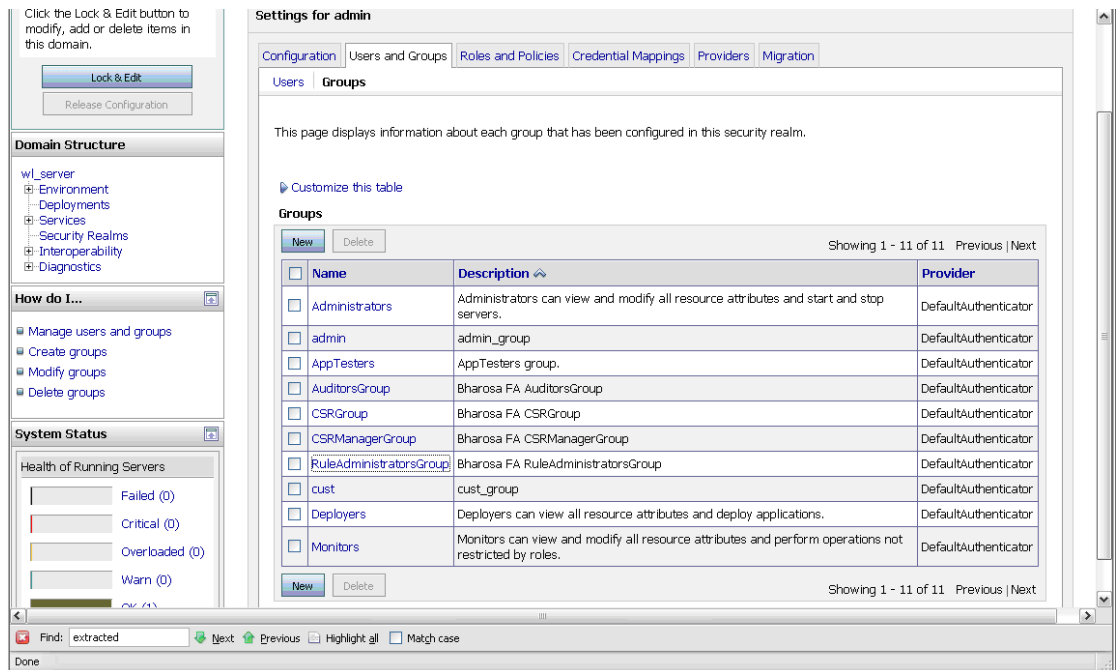
3. From the **Domain Structure** section in left pane, select **Security Realms**.



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

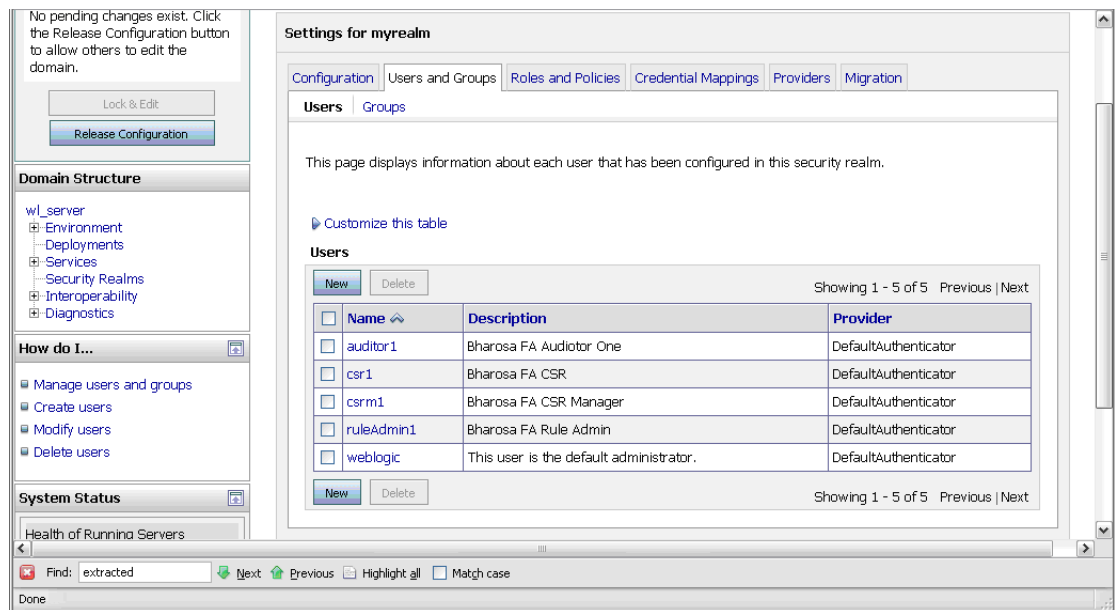


5. In the **Summary of Security Realms** page, click the realm you are using. For example, **myrealm**.
6. Click the **Users and Groups** tab.
7. To display the **Groups** page, click the **Groups** subtab. If you encounter an error, you may have to restart the WebLogic server.
8. Then, click the **New**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



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

- csrcm1
- csr
- ruleAdmin1
- auditor1



10. **Optional:** to assign csrcm1 to CSRManagerGroup, csr to CSRGroup, ruleAdmin1 to RuleAdministratorsGroup, and auditor1 to AuditorsGroup, follow the steps provided below.

- In the left pane select **Security Realms**.
- On the **Summary of Security Realms** page select the name of the realm (for example, **myrealm**).
- On the **Settings for Realm Name** page select **Users and Groups > Users**.
- In the **Users** table click the user you want to add to a group. For example, **csrcm1**.
- On the **Settings for <User Name>** page select the **Groups** subtab.
- 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**.
- Click **Save**.

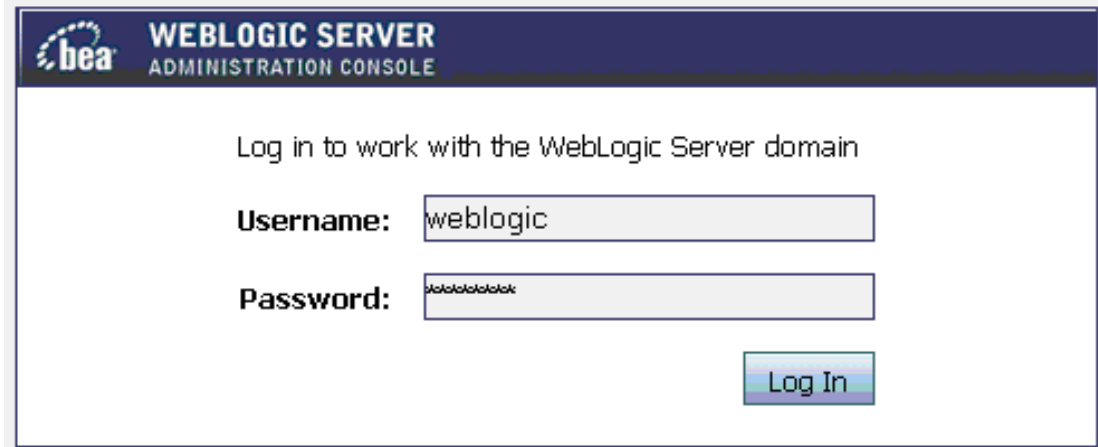
11. Commit the users and groups created by clicking the **Release Configuration** button in the left pane.

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

Deploying the Adaptive Risk Manager Offline Application WAR File

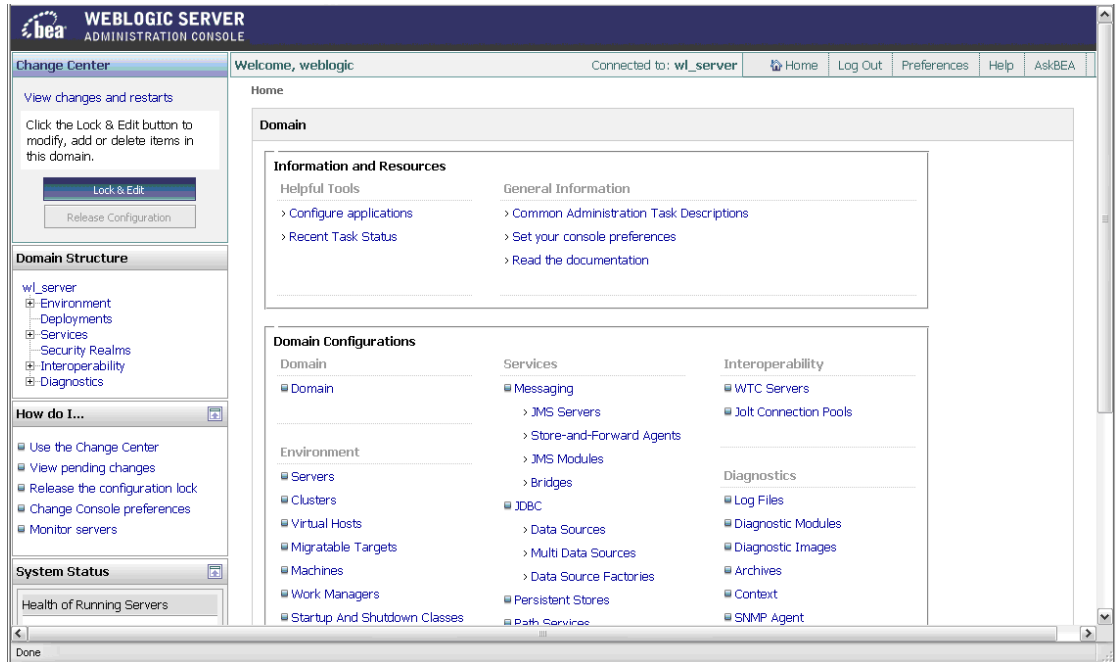
To deploy the Adaptive Risk Manager Offline Application WAR file,

1. Create a directory named `oaam_rm_offline`.
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 Offline WAR file, `oaam_rm_offline.war`, into the `oaam_rm_offline` directory created in the previous step.
The WAR file can be extracted using the command, `jar -xvf oaam_rm_offline.war`, with `oaam_rm_offline` 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 `oaam_rm_offline/WEB-INF/classes/` directory. Refer to the `log4j` configuration and Adaptive Risk Manager Offline server properties configuration sections.
4. Download the SQL Server 2005 JDBC driver (`sqljdbc.jar`) and any other third-party jars into the `oaam_rm_offline/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).

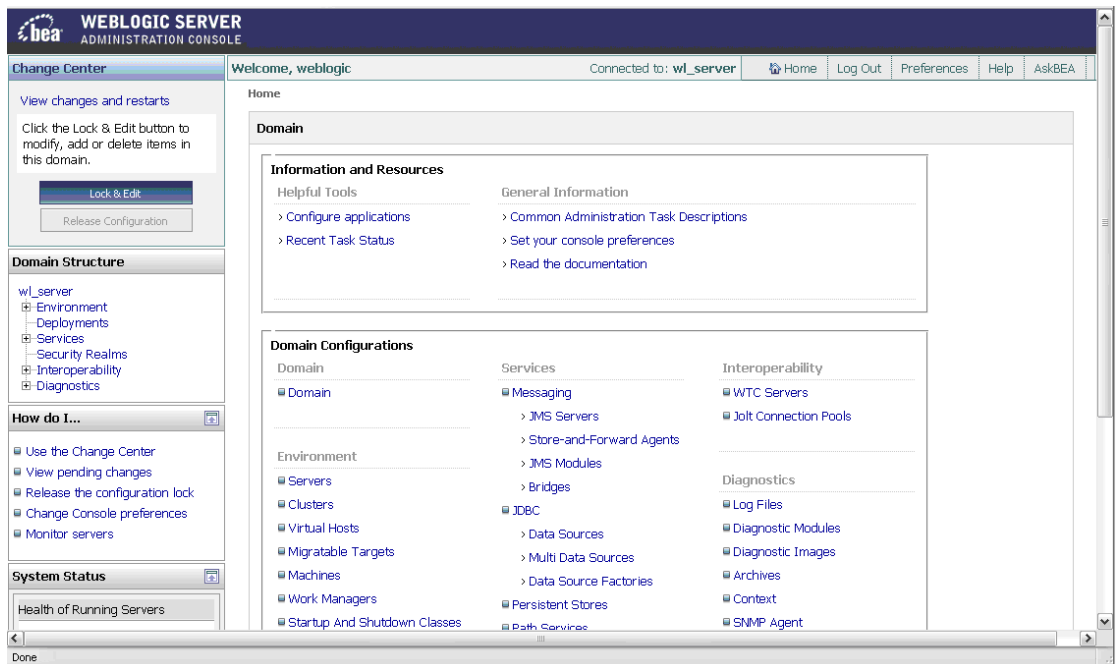


The screenshot shows the WebLogic Server Administration Console login interface. At the top left is the BEA logo. The header text reads "WEBLOGIC SERVER ADMINISTRATION CONSOLE". Below the header, the text "Log in to work with the WebLogic Server domain" is displayed. There are two input fields: "Username:" with the value "weblogic" and "Password:" with masked characters. A "Log In" button is located at the bottom right of the form.

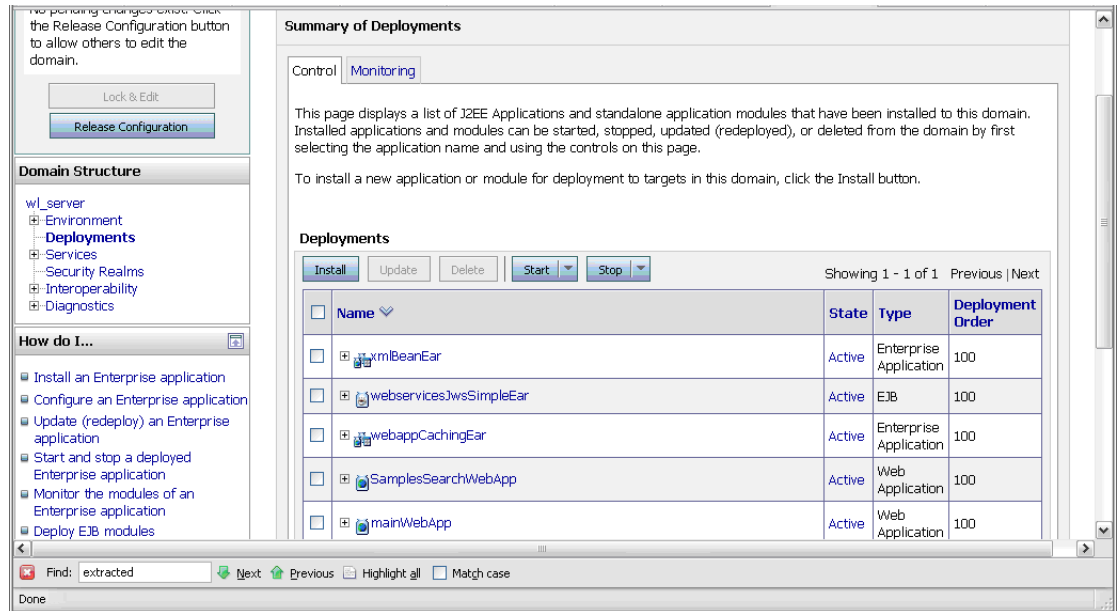
6. In the left pane, click the **Lock & Edit** button under the **Change Center** section.



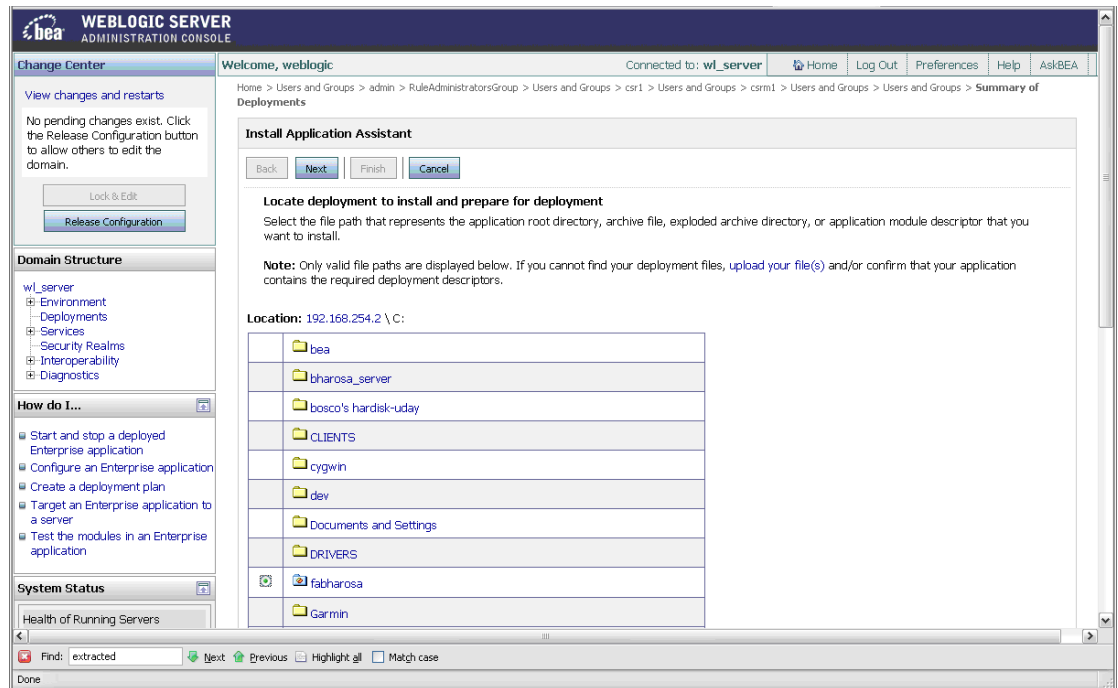
7. From the **Domain Structure** section in the left pane, select **Deployments**.



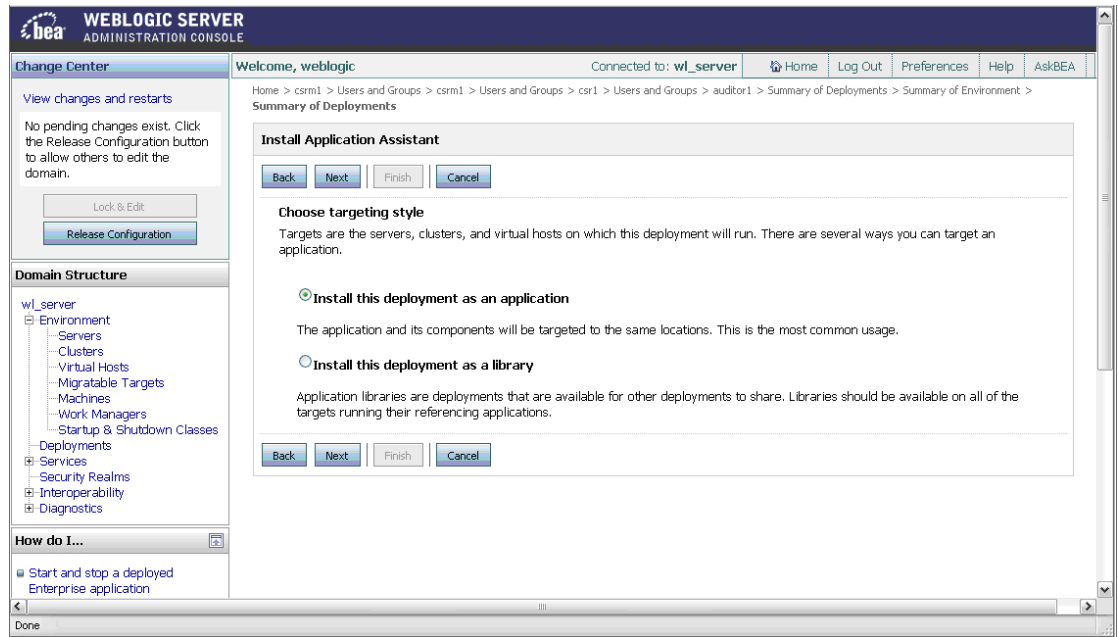
8. From the Summary of Deployments page, select **Control**, and then click **Install**.



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



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

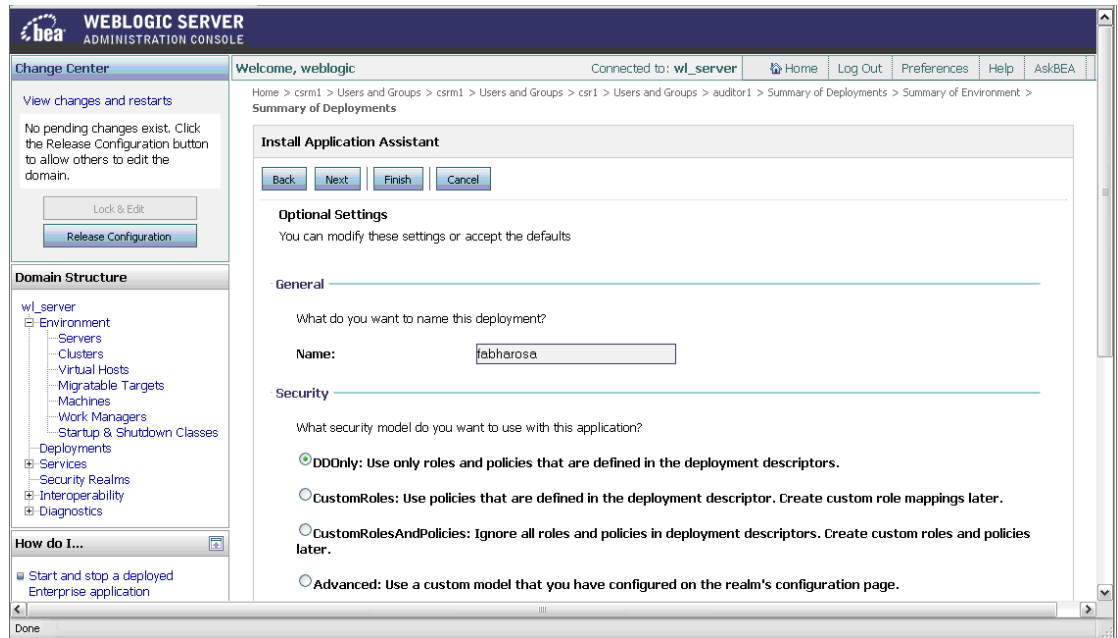


11. (Optional Step) Update additional deployment settings.

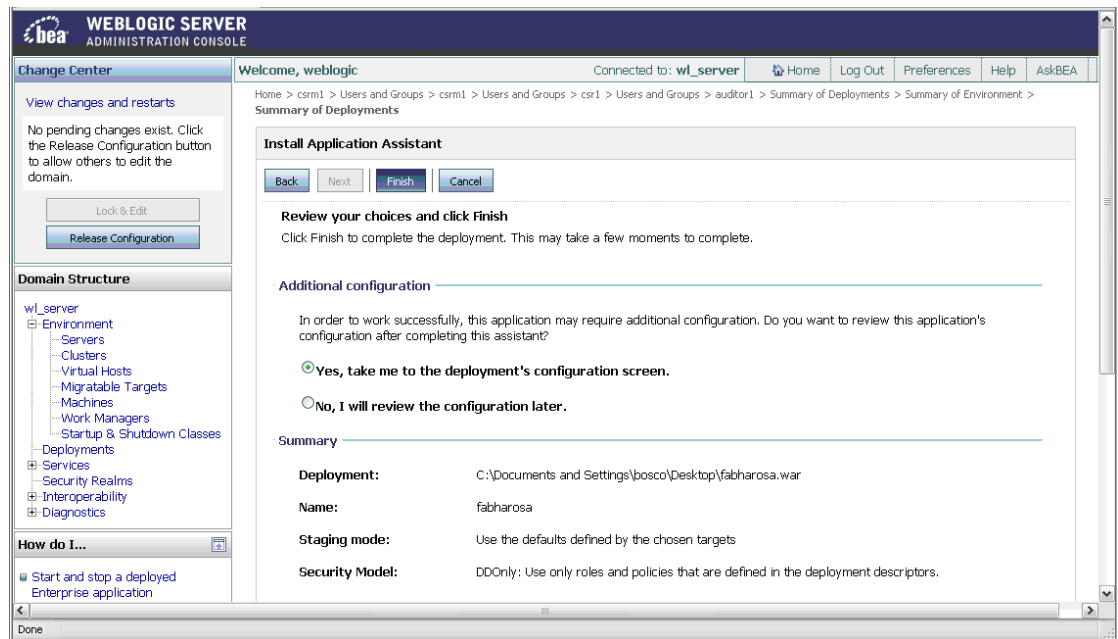
Settings include:

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

Typically, the default values are adequate.

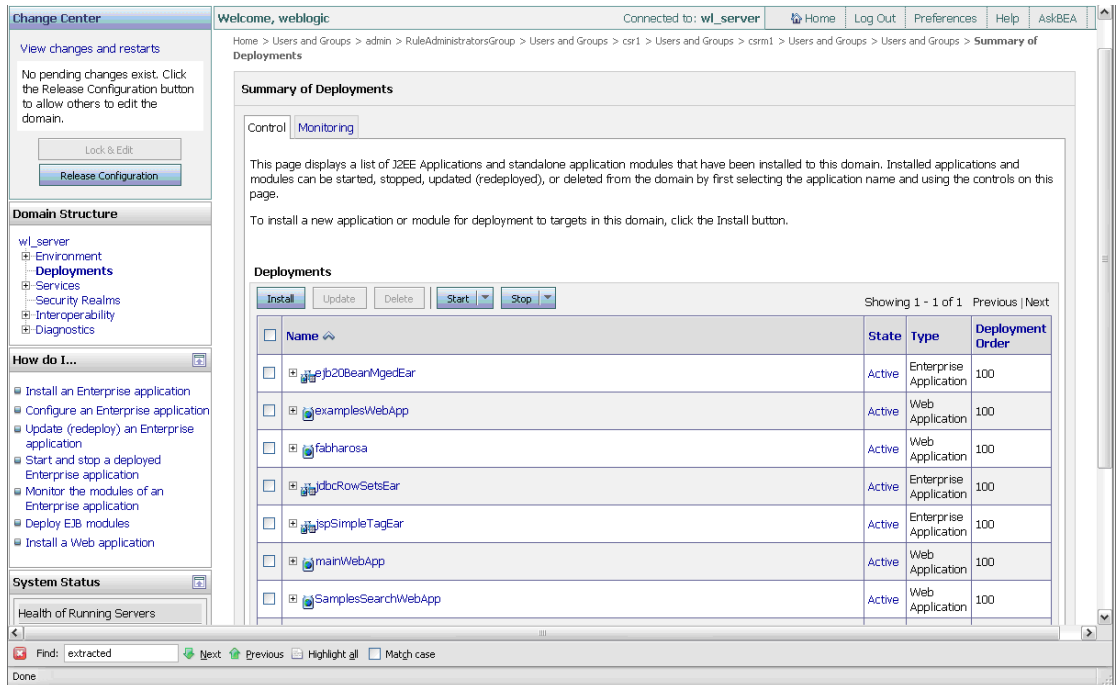


12. Review the configuration settings you specified, and click **Finish** to complete the installation.

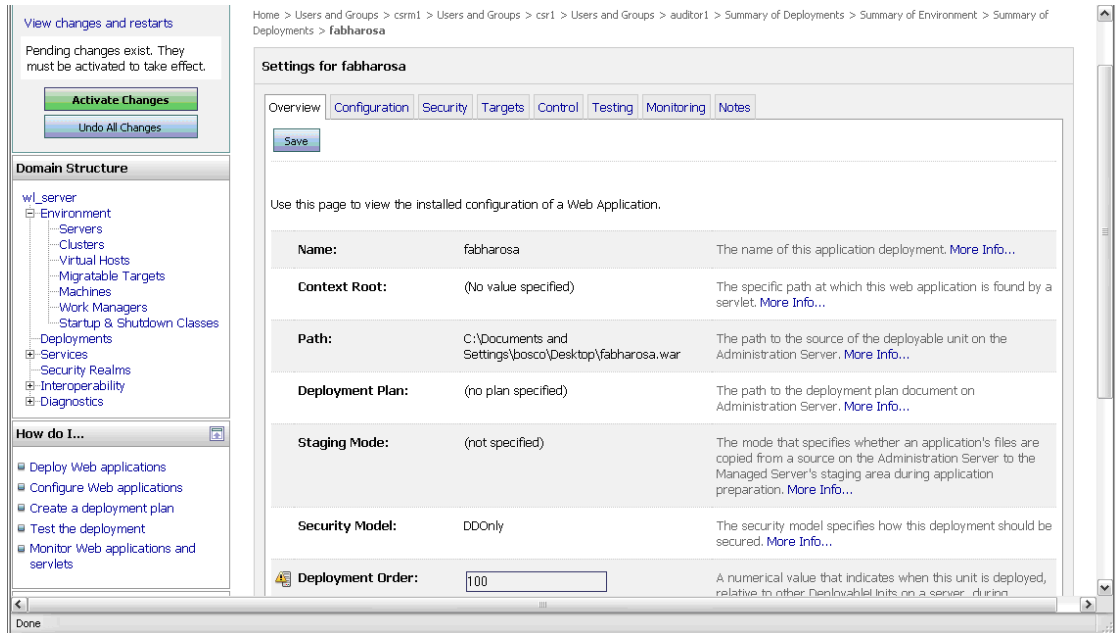


13. In order to work successfully, the application may require additional configuration. In the Additional Configuration section of the Install Application Assistant page, choose from the two options available.
 - Yes, take me to the deployment's configuration screen
 - No, I will review the configuration later

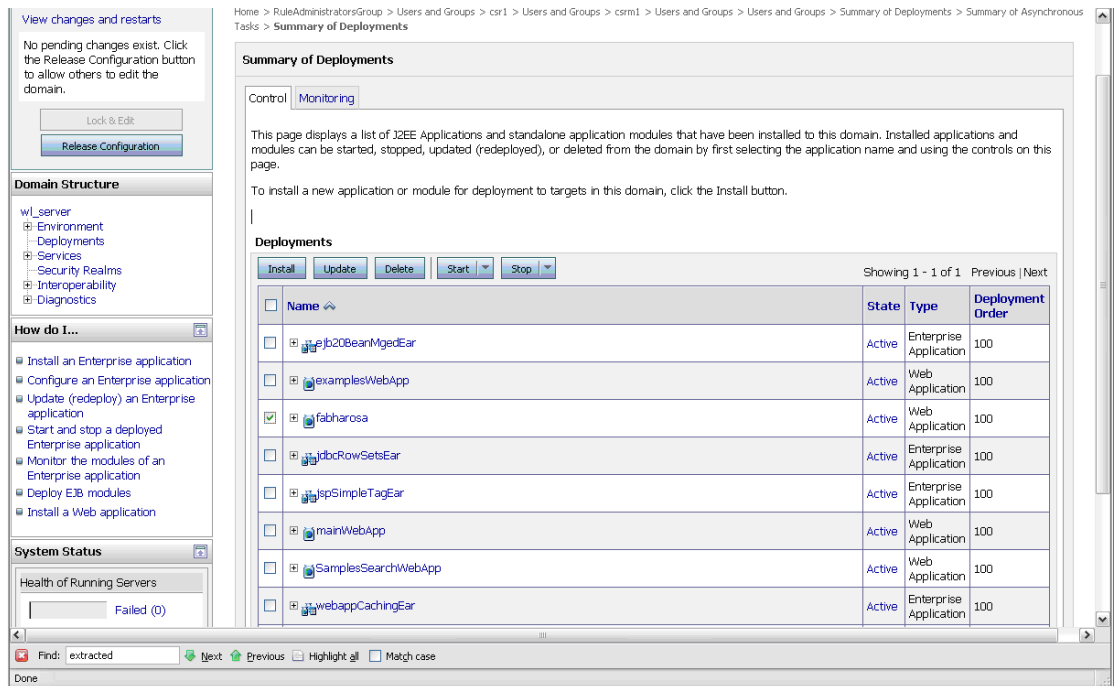
- If you chose the **Yes, take me to the deployment's configuration screen** option, you will go immediately to the deployment's configuration screen where you will be able to click the tabs to set additional configuration settings for the Adaptive Risk Manager Offline Web application.
- If you chose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



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



- From the **Domain Structure** section in the left pane, select **Deployments**.
- Select the Adaptive Risk Manager Offline Web Application Module, **oaam_rm_offline**, and click **Stop**.
- Select the **oaam_rm_offline** module again, click **Start**, and wait for its state to become Active.



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/`

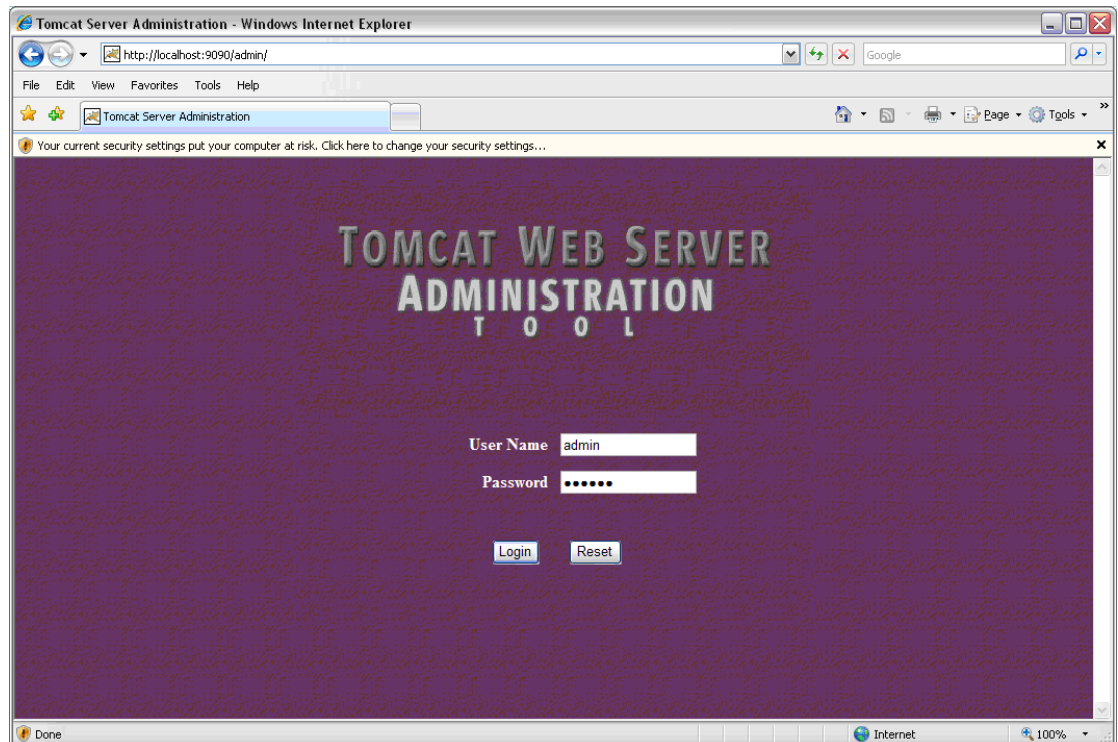
3. Delete the admin directory in the `webapps/ROOT` directory in the Tomcat directory, if any exists.

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

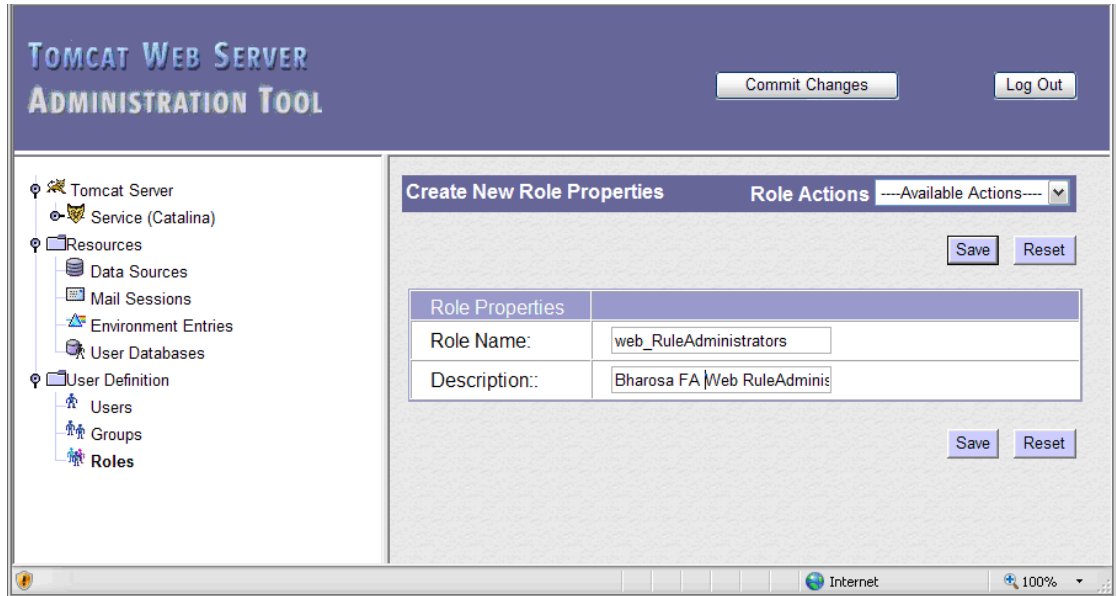
Creating Roles and Adding Users from the Tomcat Web Server Administration Tool

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**.

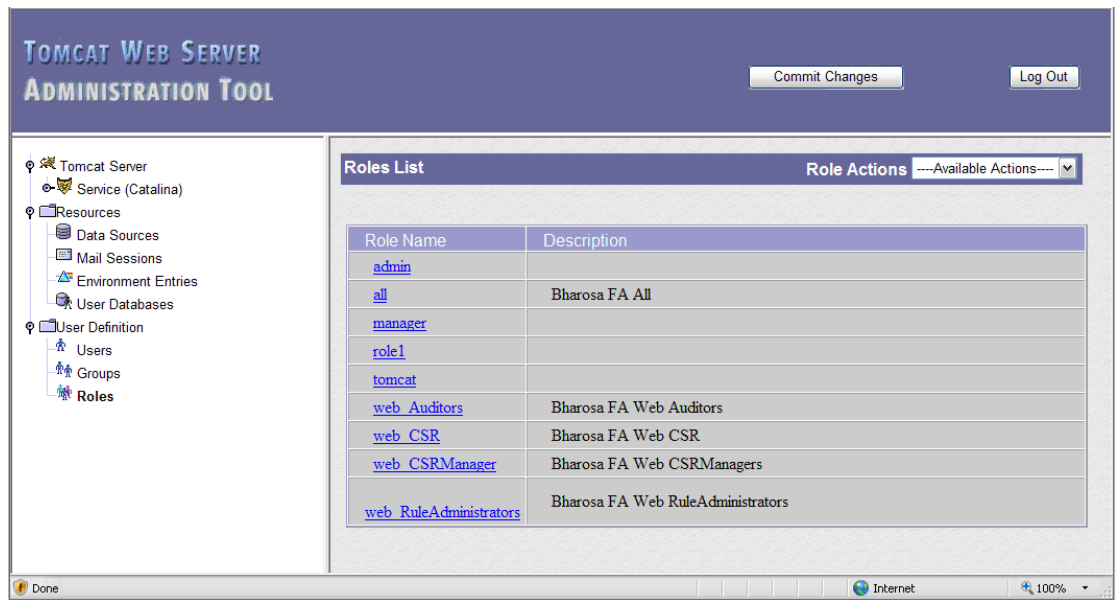


2. From the Administration Tool's left pane, select **User Definition** and click **Roles**.
3. From the **Role Actions** list in the right pane, select **Create New Role**.
4. In the **Role Properties** section, enter `web_RuleAdministrators` in the **Role Name** field and `Bharosa FA Web RuleAdministrators`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

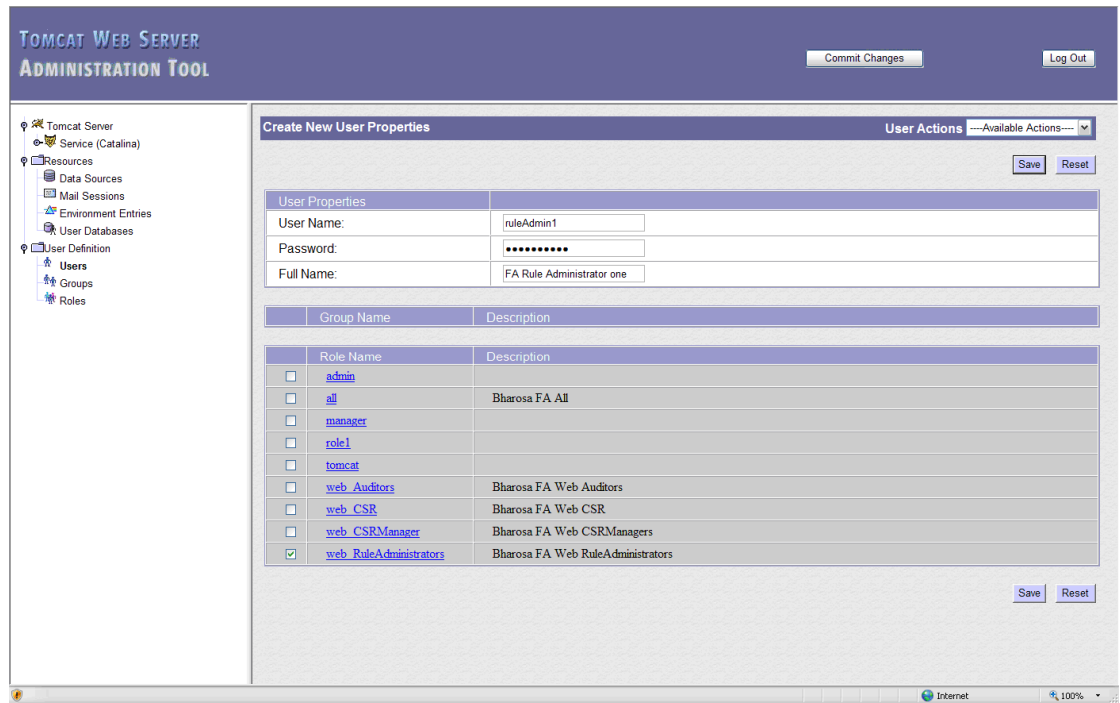


5. Then, repeat the process to create the **web_CSRManager**, **web_CSR**, **web_Auditors**, and **all** roles.

The screen below shows the five user roles created.

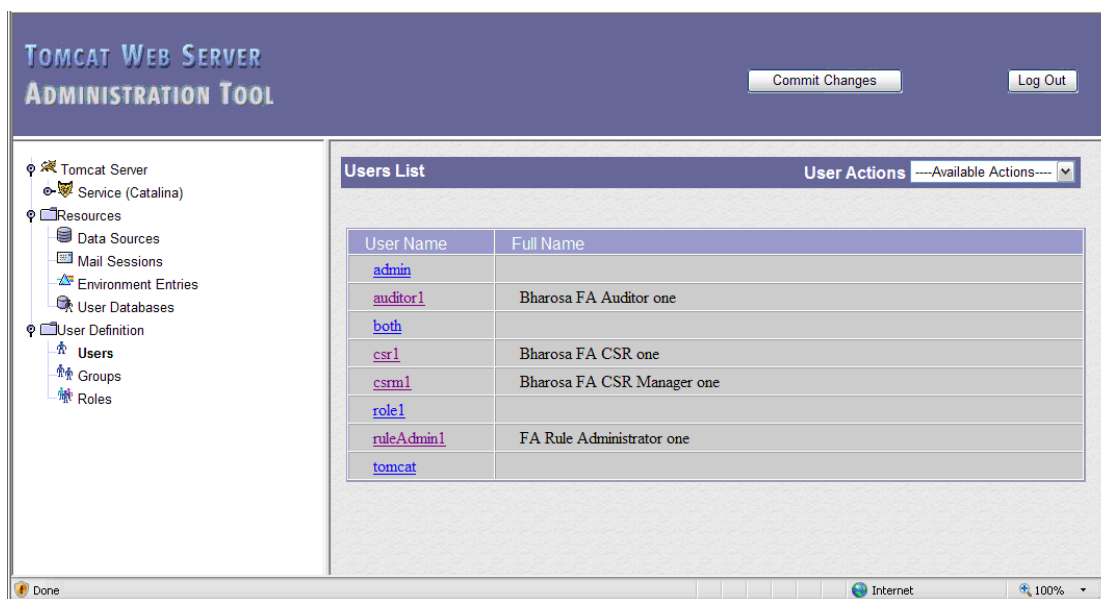


6. From the Administration Tool's left pane, select **User Definition** and click **Users**.
7. From the **User Actions** list in the right pane, select **Create New User**.
8. Enter **ruleAdmin1** in the **User Name** field, values for the **Password** and **Full Name** fields, and select the **web_RuleAdministrators**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

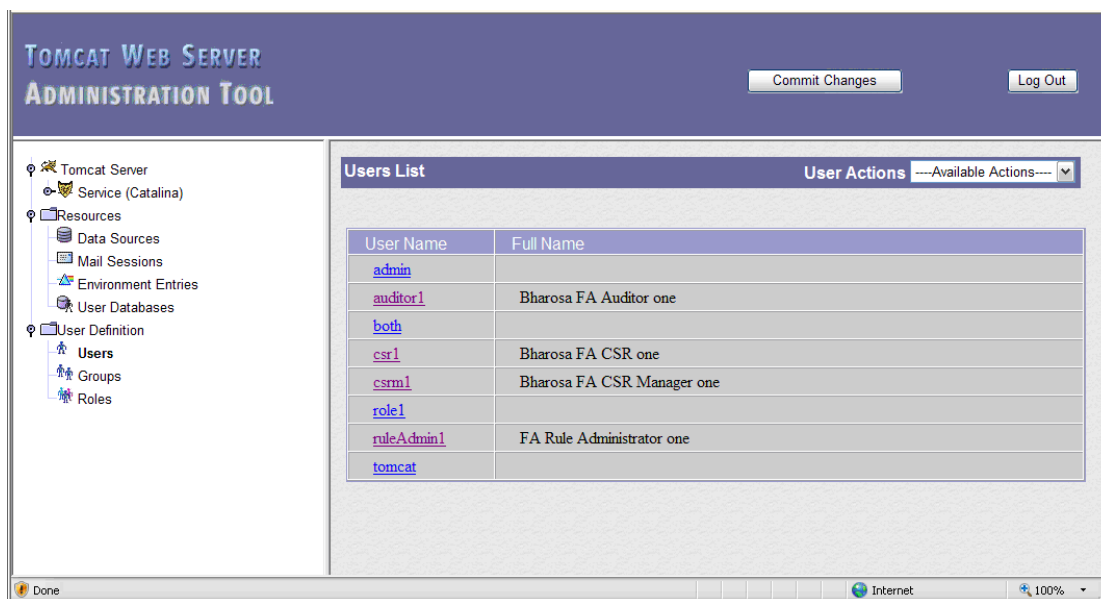


9. Repeat the process for creating users for
 - user **csrm1** with Role **web_CSRManager**
 - user **csr1** with Role **web_CSR**
 - user **auditor1** with Role **web_Auditors**
10. Optionally, you can attach all users created (**ruleAdmin1**, **csrm1**, **csr1**, and **auditor1**) so far to role **all**.

The four users are shown in the following screen.



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



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

Deploying the Adaptive Risk Manager Offline Application WAR

To deploy the Adaptive Risk Manager Offline 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.

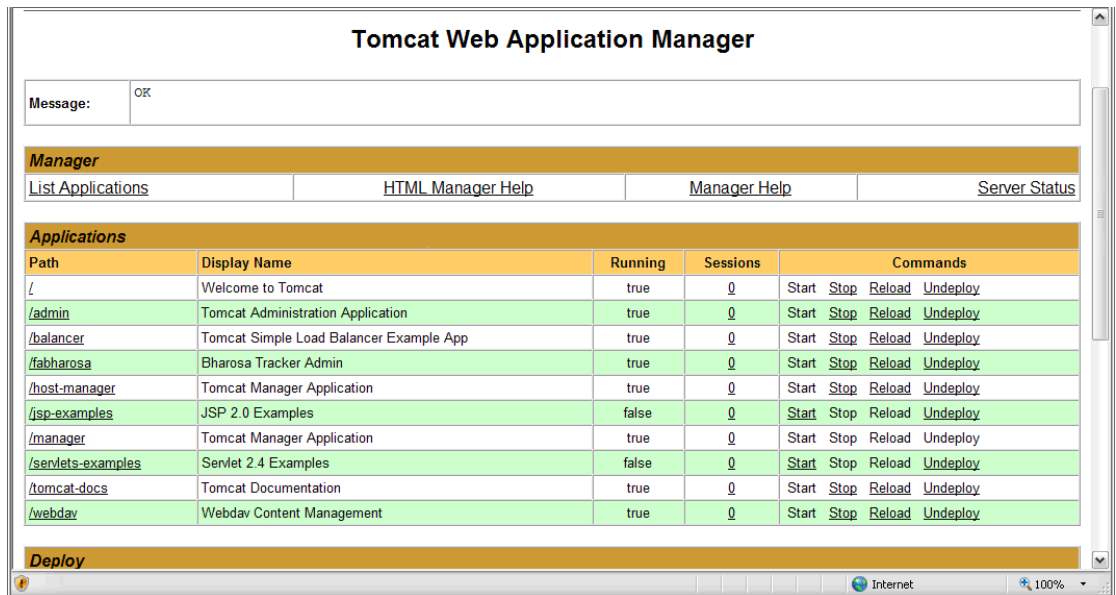
The screenshot displays the Tomcat Web Application Manager interface. At the top left is the Apache Software Foundation logo. The title is "Tomcat Web Application Manager". A message box shows "Message: OK". Below the navigation bar, the "Applications" section contains a table:

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

The "Deploy" section includes input fields for "Context Path (optional)", "XML Configuration file URL", and "WAR or Directory URL", with a "Deploy" button. The "WAR file to deploy" section shows a file path "C:\Documents and Settings\bosco\Desktop\ter" and a "Browse..." button, followed by another "Deploy" button.

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

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



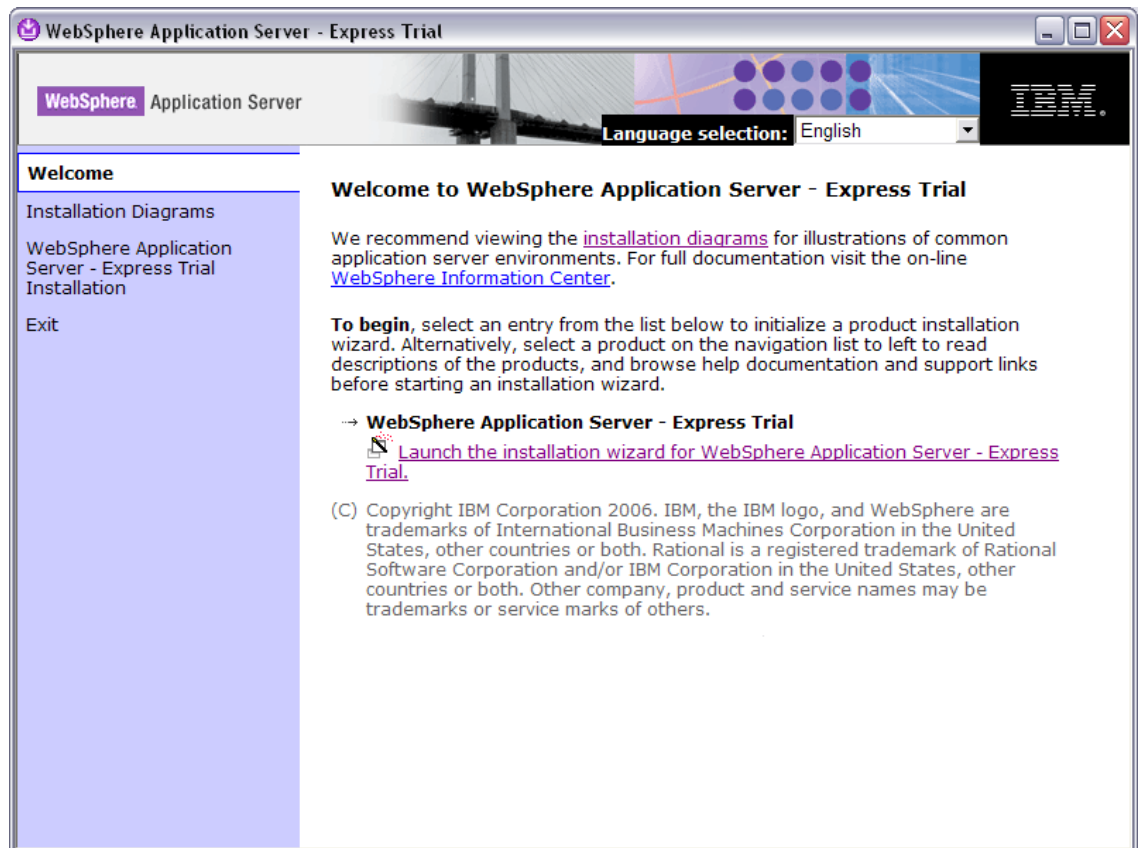
- Edit the files **log4j.xml**, **sessions.xml**, and **bharosa_server.properties** from **TOMCAT_HOME/webapps/oaam_rm_offline/WEB-INF/classes/** for appropriate values as mentioned in log4j configuration, TopLink Configuration Reference, and Server Properties Configuration sections of this document.
- Download any third party jars like **sqljdbc.jar** into **TOMCAT_HOME/webapps/oaam_rm_offline/WEB-INF/lib** directory.
- 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.

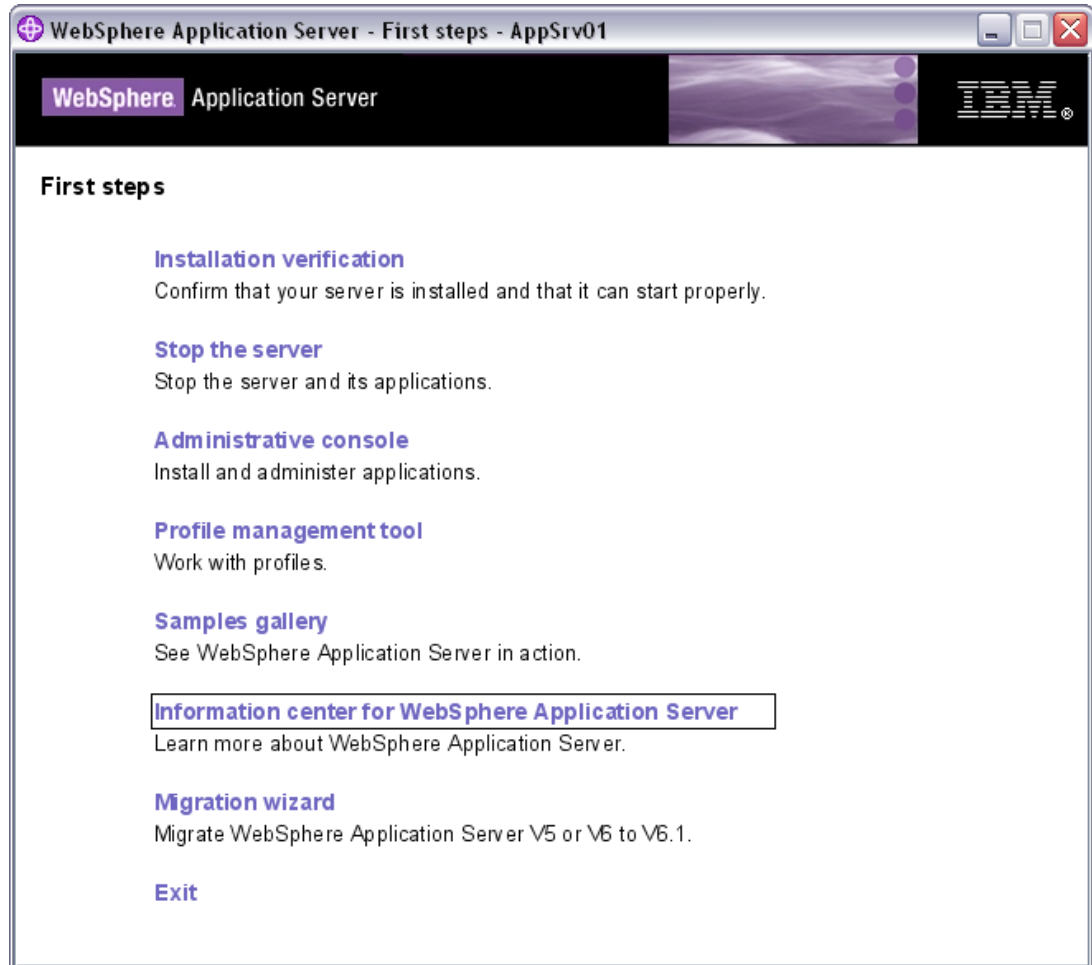


10. When the **Software License Agreement** screen appears, accept the IBM and non-IBM terms and press **Next** to continue.
11. In the **System prerequisite check** screen, click **Next** to continue.
12. In the Install Sample Applications screen, deselect the Install the sample applications option, 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.

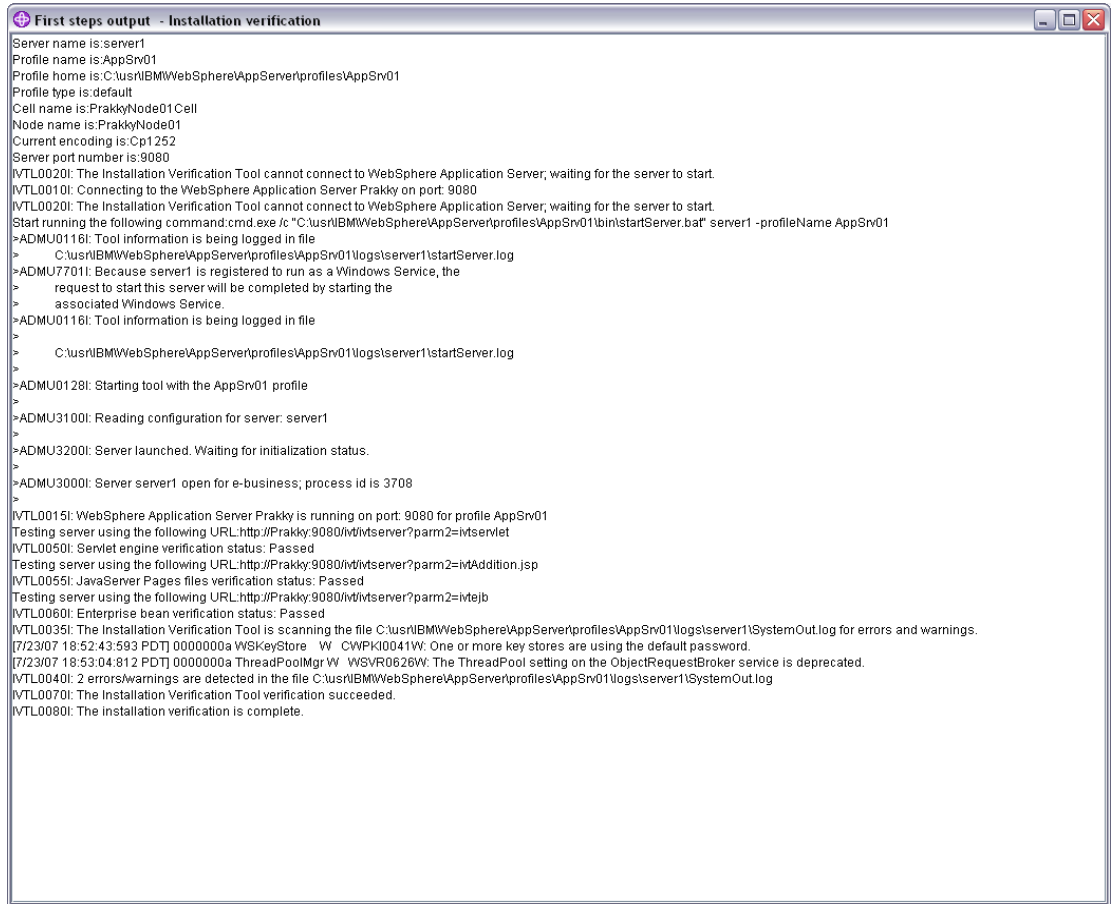
By enabling security, you protect your server from unauthorized users and are then able to provide application isolation and requirements for authenticating application users.
15. In the **Installation Summary** screen, click **Next** to continue.
16. Press the **Finish** button after the installation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



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

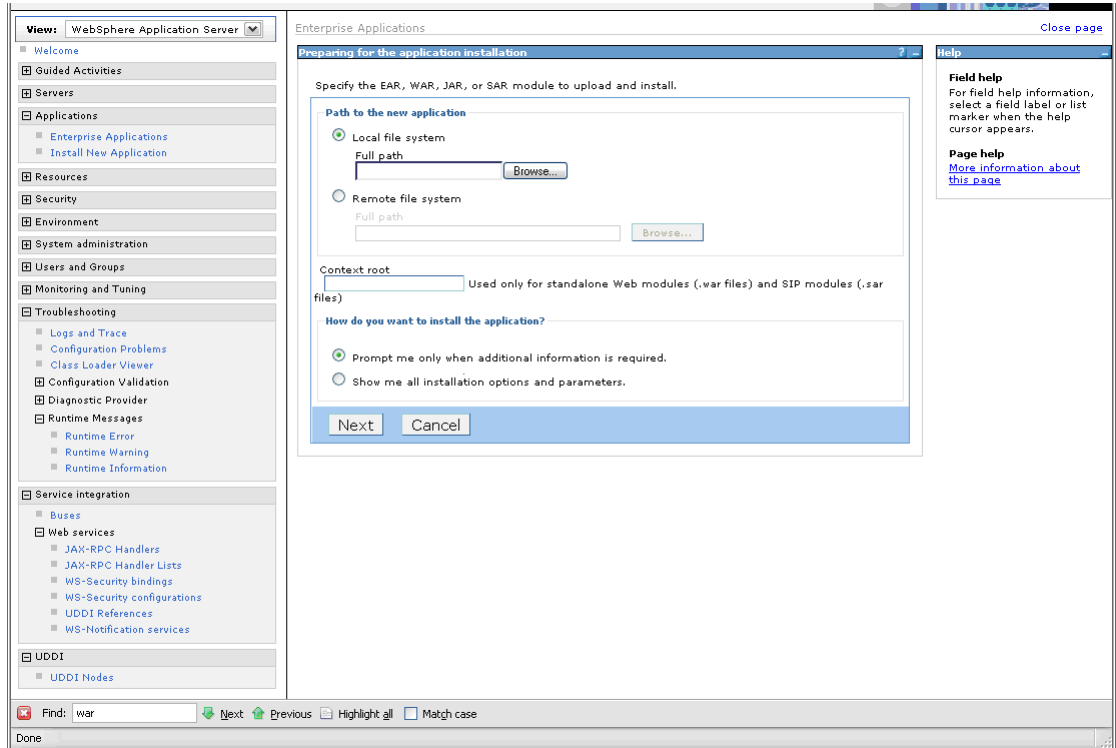


```
First steps output - Installation verification
Server name is:server1
Profile name is:AppSrv01
Profile home is:C:\usr\IBM\WebSphere\AppServer\profiles\AppSrv01
Profile type is:default
Cell name is:PrakkyNode01 Cell
Node name is:PrakkyNode01
Current encoding is:Cp1252
Server port number is:9080
IVTL0020: The Installation Verification Tool cannot connect to WebSphere Application Server, waiting for the server to start.
IVTL0010: Connecting to the WebSphere Application Server Prakky on port: 9080
IVTL0020: 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
>ADMU0116: Tool information is being logged in file
> C:\usr\IBM\WebSphere\AppServer\profiles\AppSrv01\logs\server1\startServer.log
>ADMU7701: 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.
>ADMU0116: Tool information is being logged in file
>
> C:\usr\IBM\WebSphere\AppServer\profiles\AppSrv01\logs\server1\startServer.log
>ADMU0128: Starting tool with the AppSrv01 profile
>
>ADMU3100: Reading configuration for server: server1
>
>ADMU3200: Server launched. Waiting for initialization status.
>
>ADMU3000: Server server1 open for e-business; process id is 3708
>
IVTL0015: 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
IVTL0050: Servlet engine verification status: Passed
Testing server using the following URL:http://Prakky:9080/ivt/ivtserver?parm2=ivtAddition.jsp
IVTL0055: JavaServer Pages files verification status: Passed
Testing server using the following URL:http://Prakky:9080/ivt/ivtserver?parm2=ivtEjb
IVTL0060: Enterprise bean verification status: Passed
IVTL0035: 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 WSKKeyStore W CWPk0041W: 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.
IVTL0040: 2 errors/warnings are detected in the file C:\usr\IBM\WebSphere\AppServer\profiles\AppSrv01\logs\server1\SystemOut.log
IVTL0070: The Installation Verification Tool verification succeeded.
IVTL0080: The installation verification is complete.
```

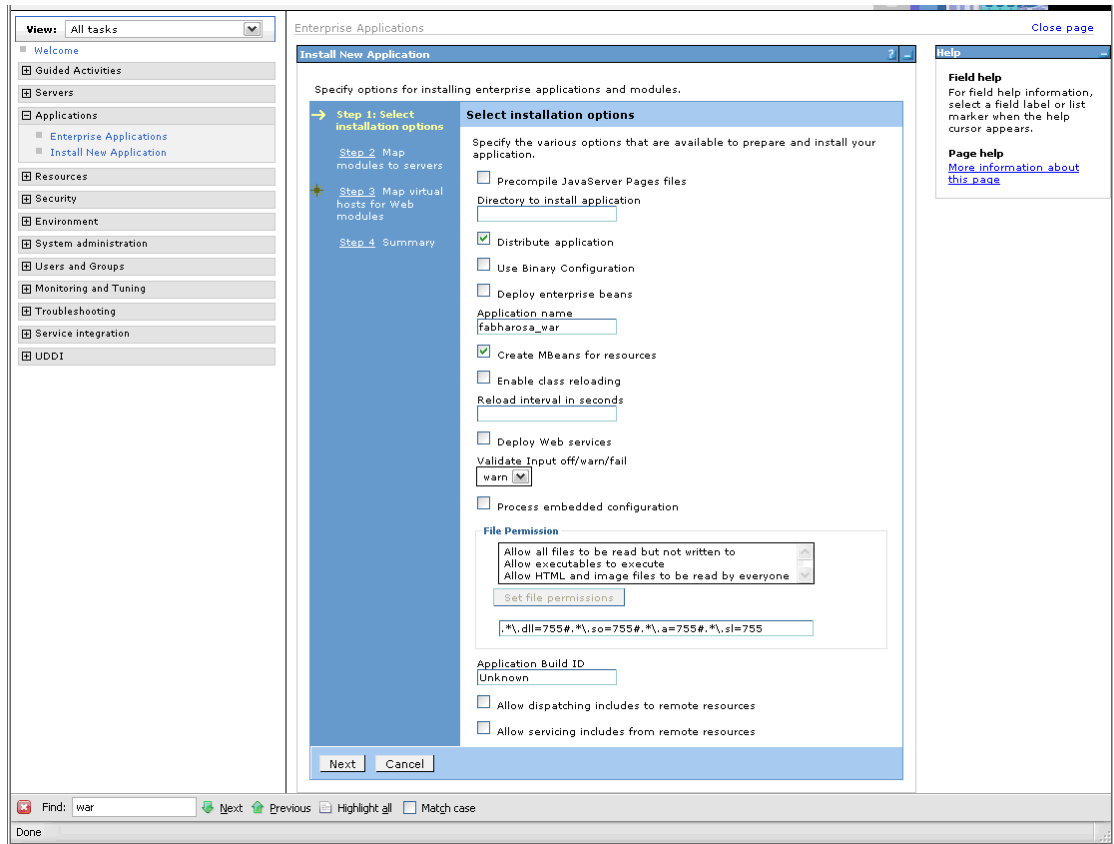
If there are errors during the verification that indicate that the Application Server did not start, you will have to manually start the server before continuing to the next step.

Installing the Oracle Adaptive Risk Manager Offline 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 `"/oaam_rm_offline"` for the `oaam_rm_offline.war` file.



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**.



6. When the **Map modules to server** screen appears, select the Oracle Adaptive Access Manager module and click **Next**.
7. When the **Map virtual hosts for Web modules** screen appears, select the Oracle Adaptive Access Manager module and click **Next**.
8. Click **Finish** when the **Summary** screen appears.
The Installation trace 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 oaam_rm_offline_war started.

ADMA5067I: Resource validation for application oaam_rm_offline_war completed successfully.

ADMA5058I: Application and module versions are validated with versions of deployment targets.

ADMA5005I: The application oaam_rm_offline_war is configured in the WebSphere Application Server repository.

ADMA5053I: The library references for the installed optional package are created.

ADMA5005I: The application oaam_rm_offline_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\oaam_rm_offline_war.ear\oaam_rm_offline_war.ear

ADMA5005I: The application oaam_rm_offline_war is configured in the WebSphere Application Server repository.

SECJ0400I: Successfully updated the application oaam_rm_offline_war with the appContextIDForSecurity information.

ADMA5011I: The cleanup of the temp directory for application oaam_rm_offline_war is complete.

ADMA5013I: Application oaam_rm_offline_war installed successfully.

Application oaam_rm_offline_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.

- 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.

The screenshot shows the WebSphere Administration Console interface. On the left, a navigation pane is visible with the following structure:

- View: WebSphere Application Server
 - Welcome
 - Guided Activities
 - Servers
 - Enterprise Applications
 - Install New Application
 - Resources
 - Security
 - Environment
 - System administration
 - Users and Groups
 - Monitoring and Tuning
 - Troubleshooting
 - Logs and Trace
 - Configuration Problems
 - Class Loader Viewer
 - Configuration Validation
 - Diagnostic Provider
 - Runtime Messages
 - Runtime Error
 - Runtime Warning
 - Runtime Information
 - Service integration
 - Buses
 - Web services
 - JAX-RPC Handlers
 - JAX-RPC Handler Lists
 - WS-Security bindings
 - WS-Security configurations
 - UDDI References
 - WS-Notification services
 - UDDI
 - UDDI Nodes

The main content area is titled "Enterprise Applications" and contains the following information:

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.
- Buttons: Apply, Reset

Below the preferences are several action buttons: Start, Stop, Install, Uninstall, Update, Rollout Update, Remove File, Export, and Export DDL.

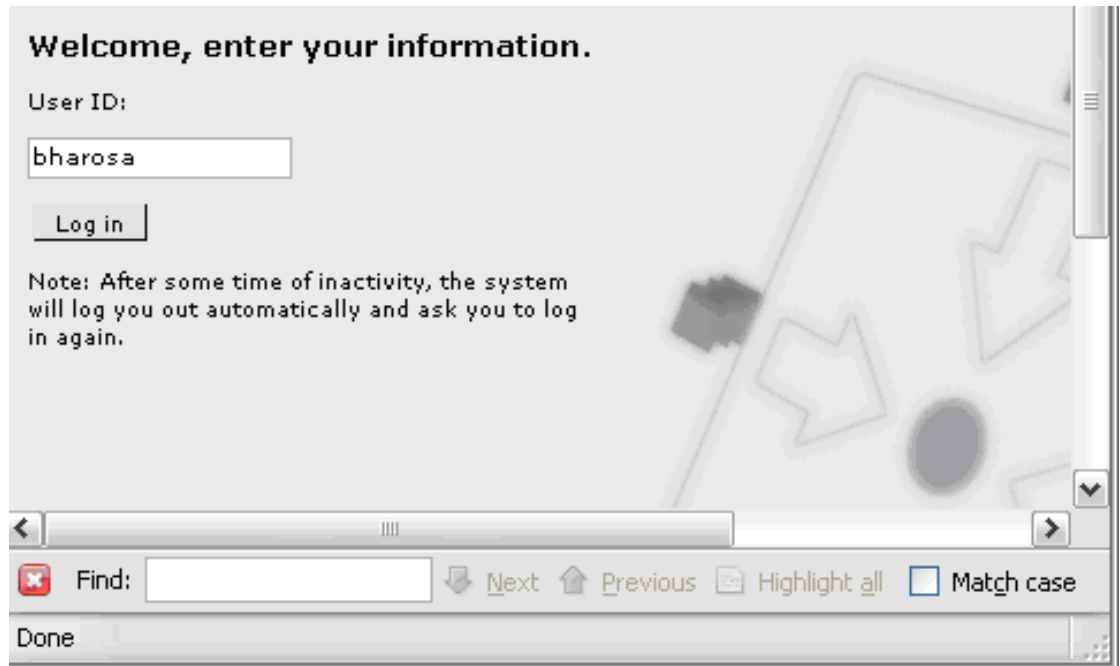
The main table lists the installed applications:

Select	Name	Application Status
<input type="checkbox"/>	DefaultApplication	➔
<input type="checkbox"/>	Dynamic Cache Monitor	➔
<input type="checkbox"/>	PlantsByWebSphere	➔
<input type="checkbox"/>	SamplesGallery	➔
<input type="checkbox"/>	bharosa_war	✖
<input type="checkbox"/>	jvtApp	➔
<input type="checkbox"/>	query	➔
Total 7		

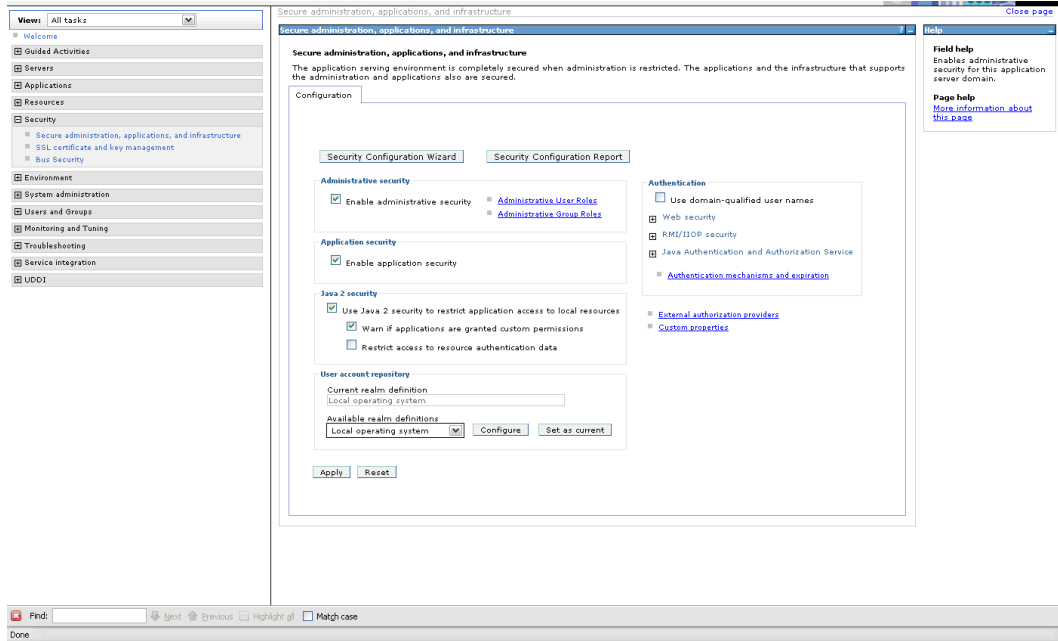
At the bottom of the console, there is a search bar with the text "Find: war" and a list of search options: Next, Previous, Highlight all, Match case. The URL at the bottom of the browser window is: `http://localhost:9060/lbm/console/navigatorCmd.do?forwardName=ApplicationDeployment.content.main`

Creating Users and User Groups

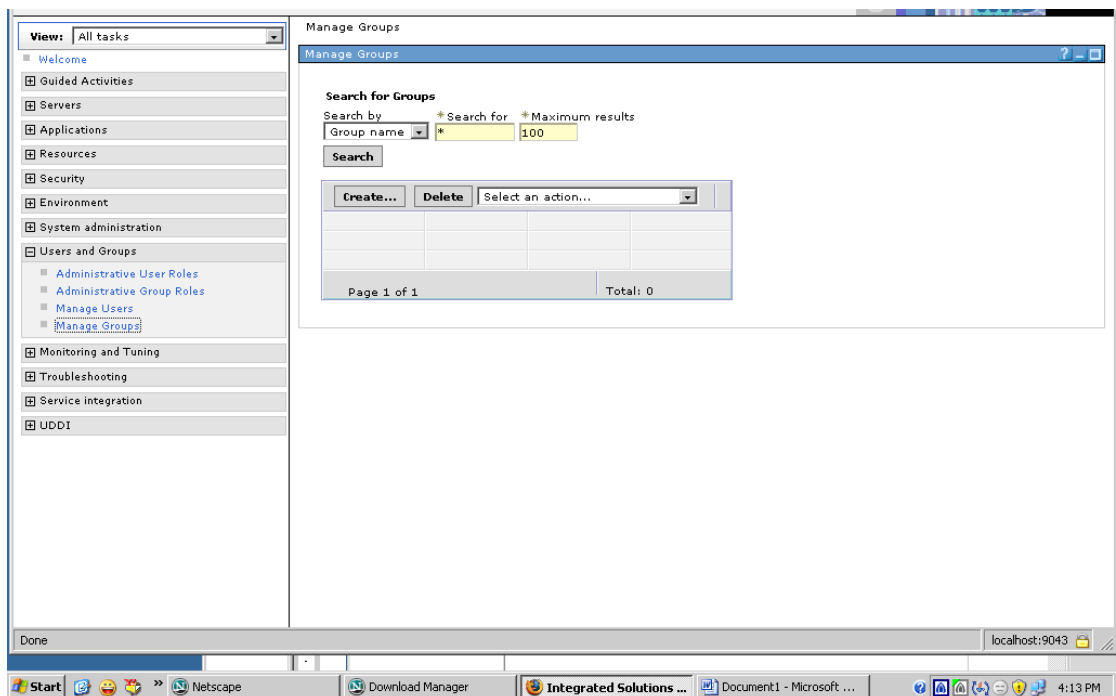
1. Launch the Administrative Console from the Start menu.
Start > IBM WebSphere > Application Server V6.1 > Profiles > AppSrv01 > Administrative console).
2. Login to the WebSphere Application Server Administrative Console.



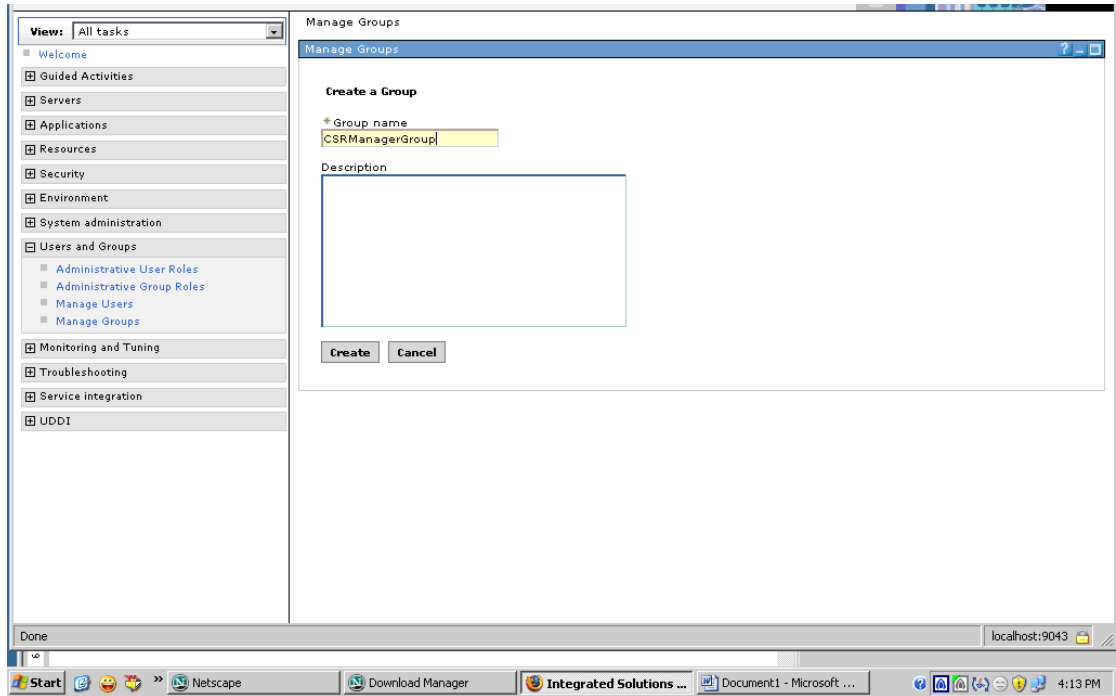
- From the Console's left pane, select **Security**, and then, click **Secure administration, applications, and infrastructure**.
- In the **Secure administration, applications, and infrastructure** page, select **Apply**.



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

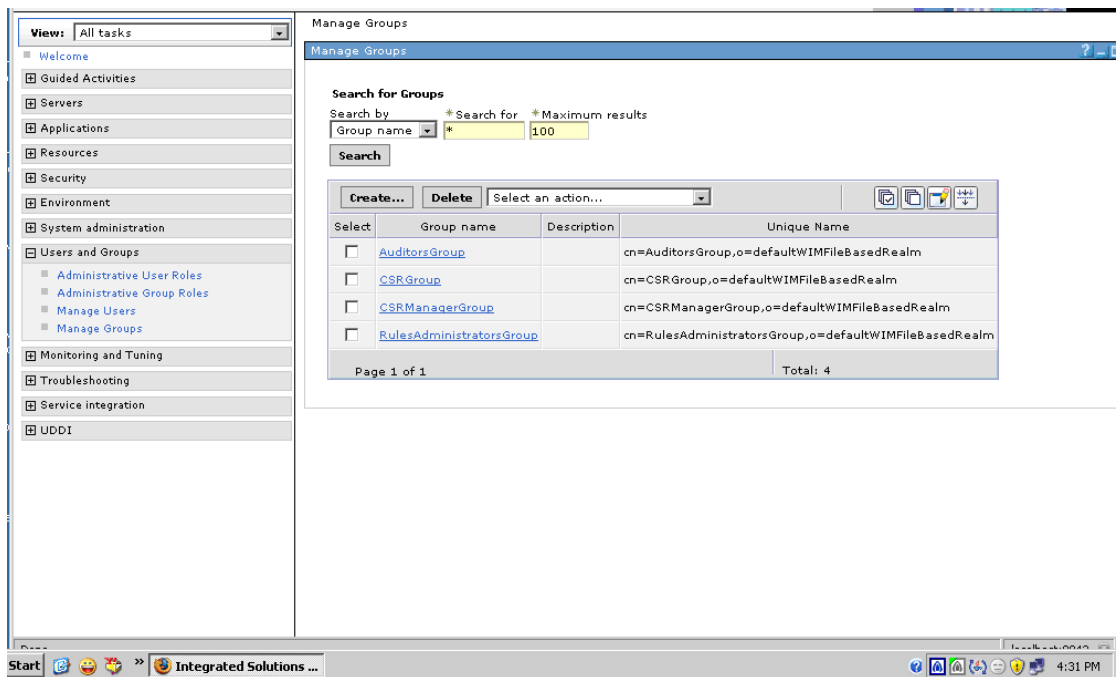


The page for creating a group appears.



7. Create following groups:

- CSRManagerGroup
- CSRGroup
- RuleAdministratorsGroup
- AuditorsGroup



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

For example, create:

- csm1
- csr
- ruleAdmin1
- auditor1

Then, assign:

- csm1 to CSRManagerGroup
- csr to CSRGroup
- ruleAdmin1 to RuleAdministratorsGroup
- auditor1 to AuditorsGroup

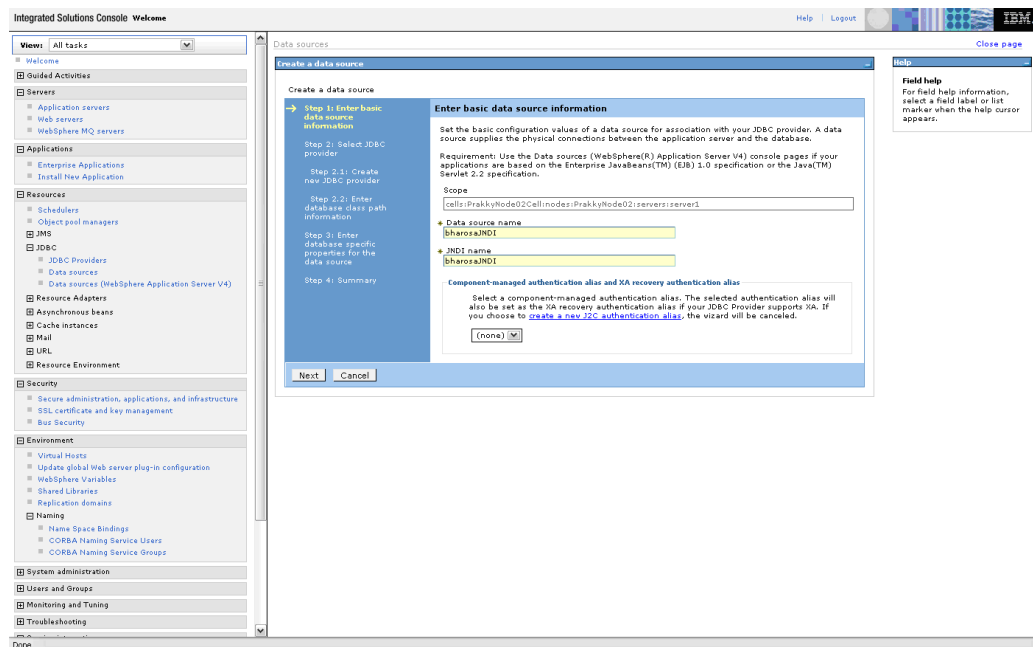
For more information about groups, refer to the “Adaptive Risk Manager Offline User Groups Reference” section of this manual.

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

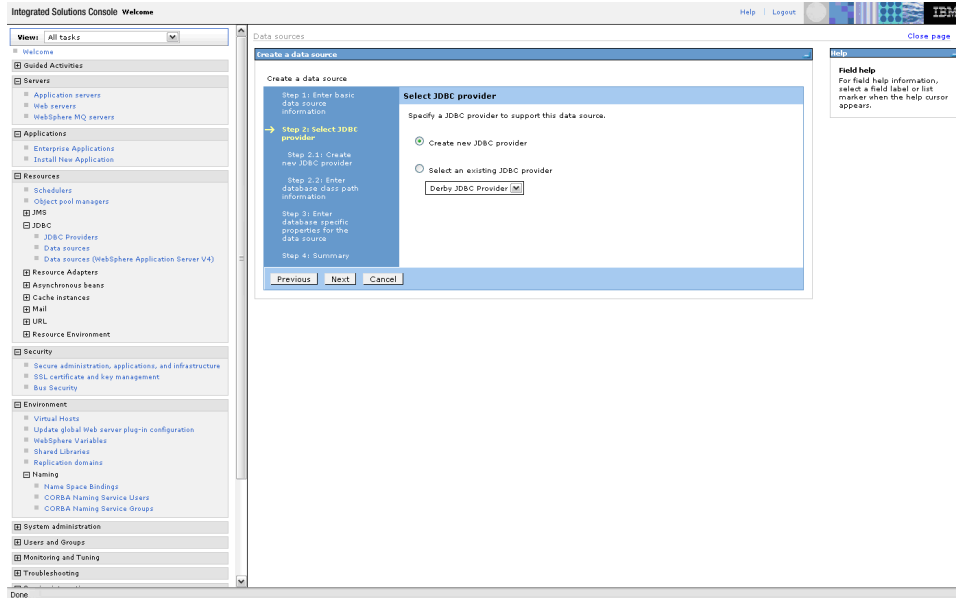
1. From the Console’s left pane, select **Resources**, and then, click **JDBC**.
2. Select JDBC Providers.
3. Enter the values as shown in the Enter basic data source information screen below and click **Next**.

Data source name: bharosaJNDI

JNDI name: bharosaJNDI



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



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

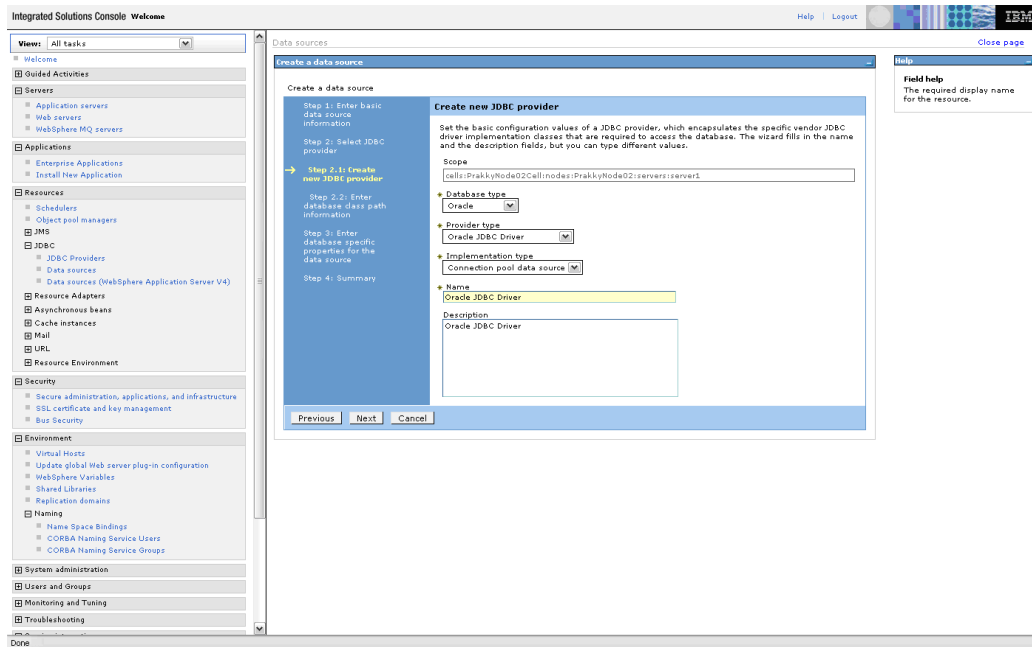
Database type: Oracle

Provider type: Oracle JDBC Driver

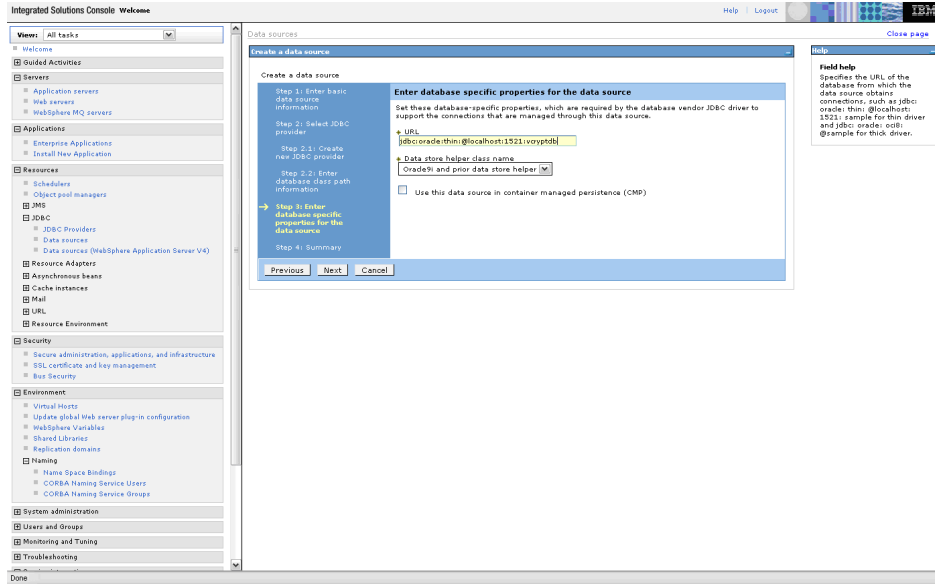
Implementation type: Connection pool data source

Name: Oracle JDBC Driver

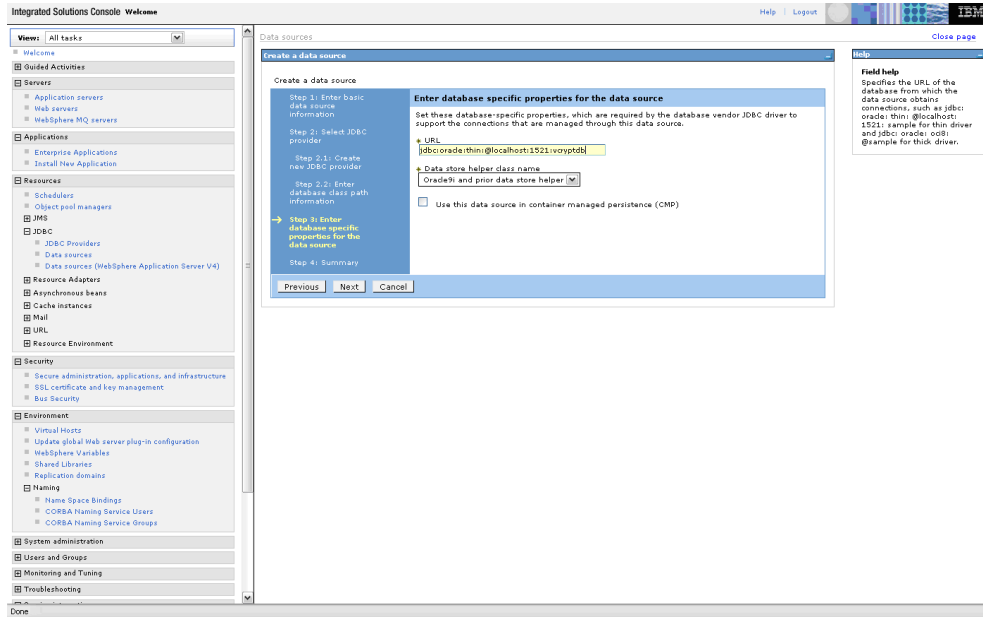
Description: Oracle JDBC Driver



- 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}`



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



Setting Up Logging

Adaptive Risk Manager Offline 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 Offline'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 Offline.
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 information about the `<platform-class>` properties, refer to the “TopLink Reference” section.

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 Offline Reports, as well as other functions, can be configured for Adaptive Risk Manager Offline 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 Offline database access parameters
 - Adaptive Risk Manager Offline Reports directory
 - Adaptive Risk Manager Offline Scheduler
2. Comment out all the reference to JDBC or database connectivity in the `bharosa_server.properties` file.

For your reference, a sample 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#

# 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
```

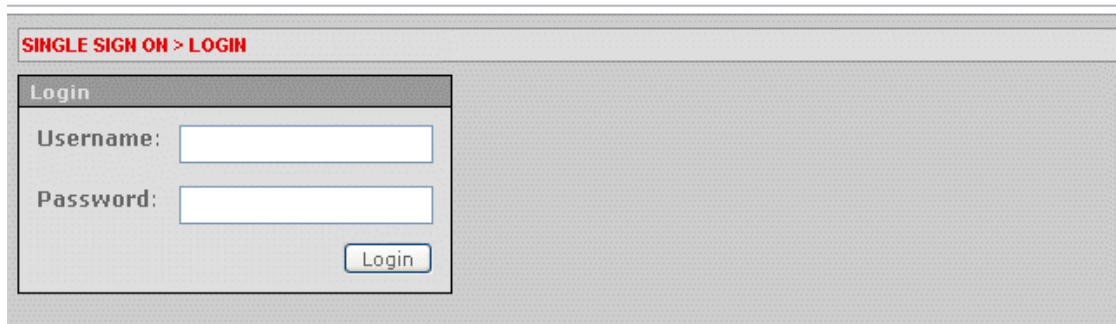
Accessing Adaptive Risk Manager Offline

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

1. Log in to Adaptive Risk Manager Offline by accessing `http://<localhost or IP>:<port>/<ARM_Offline_App_Name>` using the credentials of an existing user.

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

ORACLE Adaptive Risk Manager Offline



SINGLE SIGN ON > LOGIN

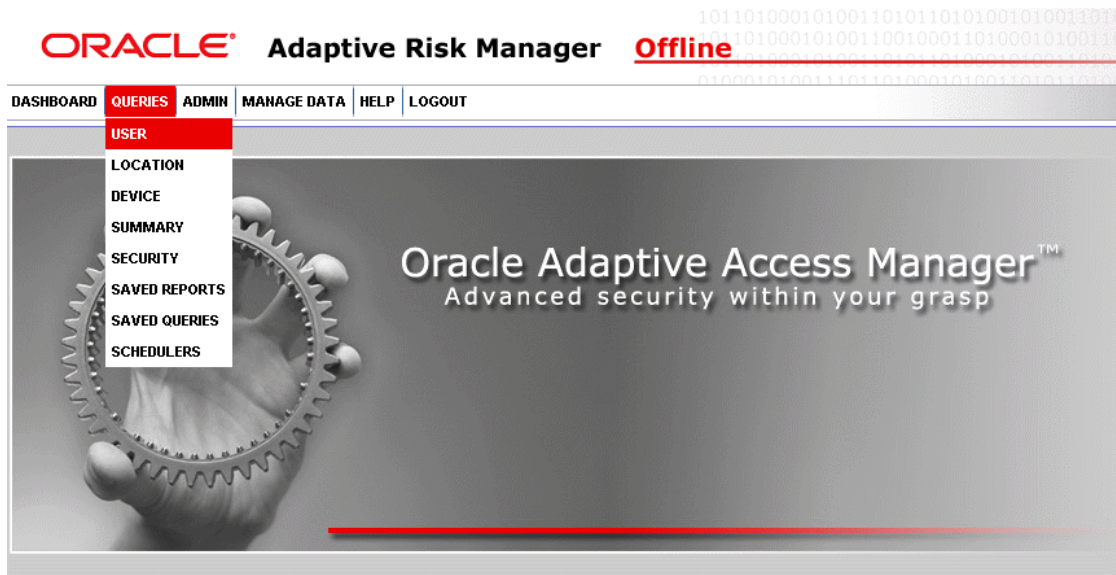
Login

Username:

Password:

Login

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



ORACLE Adaptive Risk Manager Offline

DASHBOARD QUERIES ADMIN MANAGE DATA HELP LOGOUT

USER

LOCATION

DEVICE

SUMMARY

SECURITY

SAVED REPORTS

SAVED QUERIES

SCHEDULERS

Oracle Adaptive Access Manager™
Advanced security within your grasp

- 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.

DASHBOARD | QUERIES | ADMIN | MANAGE DATA | HELP | LOGOUT

QUERIES > USER > RECENT LOGINS

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.

Session Id	User Id	Login Id	Auth Status	Pre Auth Score	Pre Auth Action	Post Auth Score	Post Auth Action	Login Time	Primary Group Id	OS /Browser	Browser FP Id /Digital FP Id	Device Id	Location	IP Address
Click Run Query with appropriate search criteria.														

Search

Auth Status: --All--

Client Type: --All--
OCS Question

Check Alert Level: --All--
ALERT_LOW
ALERT_MEDIUM

Primary Group Id: --All--

User Id:

Login Id:

Device Id:

IP Address:

Session Id:

From Date: 10/24/2007 09:26

To Date: 10/25/2007 23:59

Usage

Refer to the *Adaptive Risk Manager Offline Administrator's Guide* for instructions on

- The Standard Loading Process
- Creating a Load Configuration
- Defining a Session Set
- Starting the Load Process
- Risk Analysis

Customized Loading Process

Please refer to the *Adaptive Risk Manager Offline Customized Loader Framework* manual.

Appendix A - Adaptive Risk Manager Offline User Groups Reference

The Adaptive Risk Manager Offline users groups can access functionality in Adaptive Risk Manager Offline 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 Offline.

CSR User Group

The CSR user group has limited access.

Adaptive Risk Manager Offline 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.	
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	
<p>Queries - No location based queries are allowed. See list of recommended queries below. No access to save/schedule reports.</p>	<p>The recommended queries are listed below.</p> <p>Queries / User</p> <ul style="list-style-type: none"> • Recent Logins • Multiple Devices • First Login • Frequent Logins • Multiple Failures <p>Queries / Device</p> <ul style="list-style-type: none"> • Recent Logins • New Devices • Devices by User • Multiple Successful Logins • Users by Device • Multiple Failures • Multiple Users • Frequent Logins <p>Queries / Security Full Access</p>
Admin - No Access	
Audit - No access	
<p>Customer Care - Full access. Access through hyperlinks to detailed information. Bulk close ability on search cases screen.</p>	<p>Change Status</p> <ul style="list-style-type: none"> • New • Pending • Closed <p>Change Severity</p> <ul style="list-style-type: none"> • Low • Medium • High
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	
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	
Help - No access	
Logout - Full access	

Appendix B -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</platf
orm-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>
```