Oracle® Adaptive Access Manager
LDAP Configuration in WebSphere 6.1.0.3 with Open LDAP
10*g* (10.1.4.3.0)

December 2007

Oracle Adaptive Access LDAP Configuration in WebSphere 6.1.0.3, 10g (10.1.4.3.0)

Contents

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.

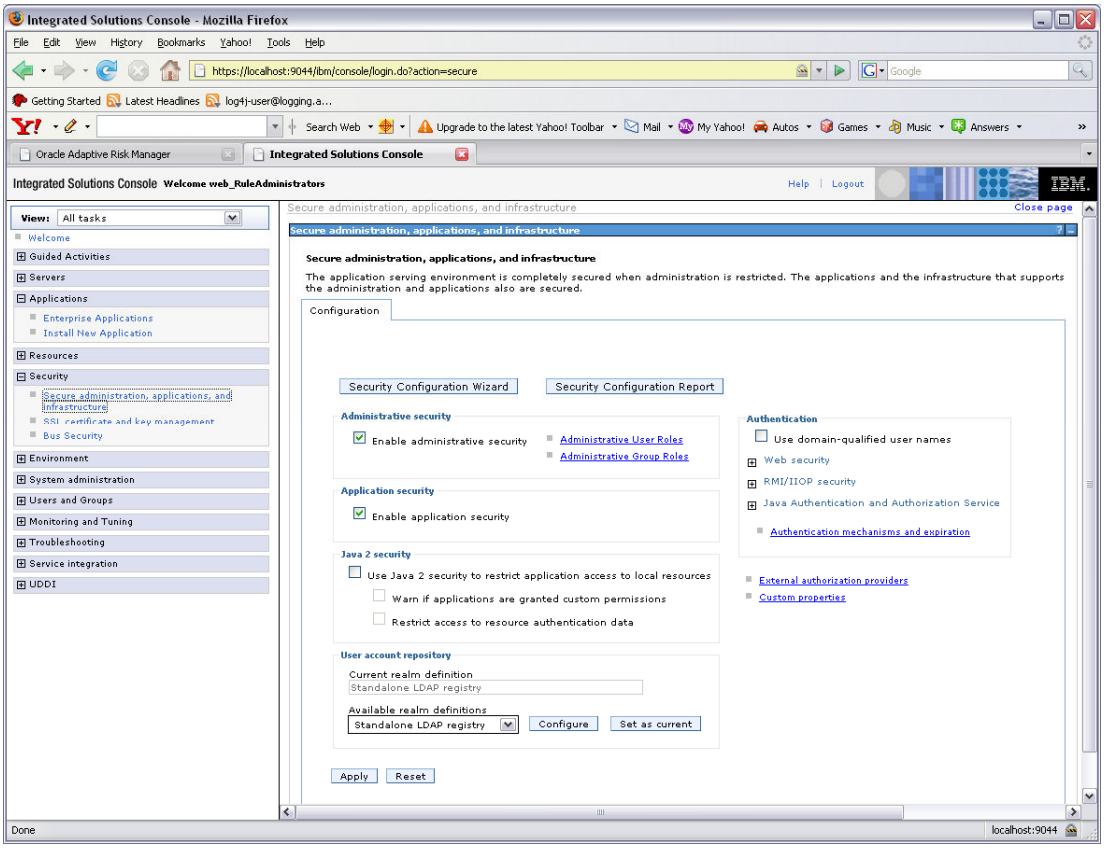
- The Oracle® Adaptive Access Manager Import/Export Manual, which provides information on importing and exporting groups, rule templates, and models to and from the Adaptive Access Manager schema.
- The Oracle® Adaptive Risk Manager Online Customer Care API Guide, which provides information about the 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.

Oracle® Adaptive Access Manager LDAP Configuration in WebSphere 6.1.0.3 with Open LDAP

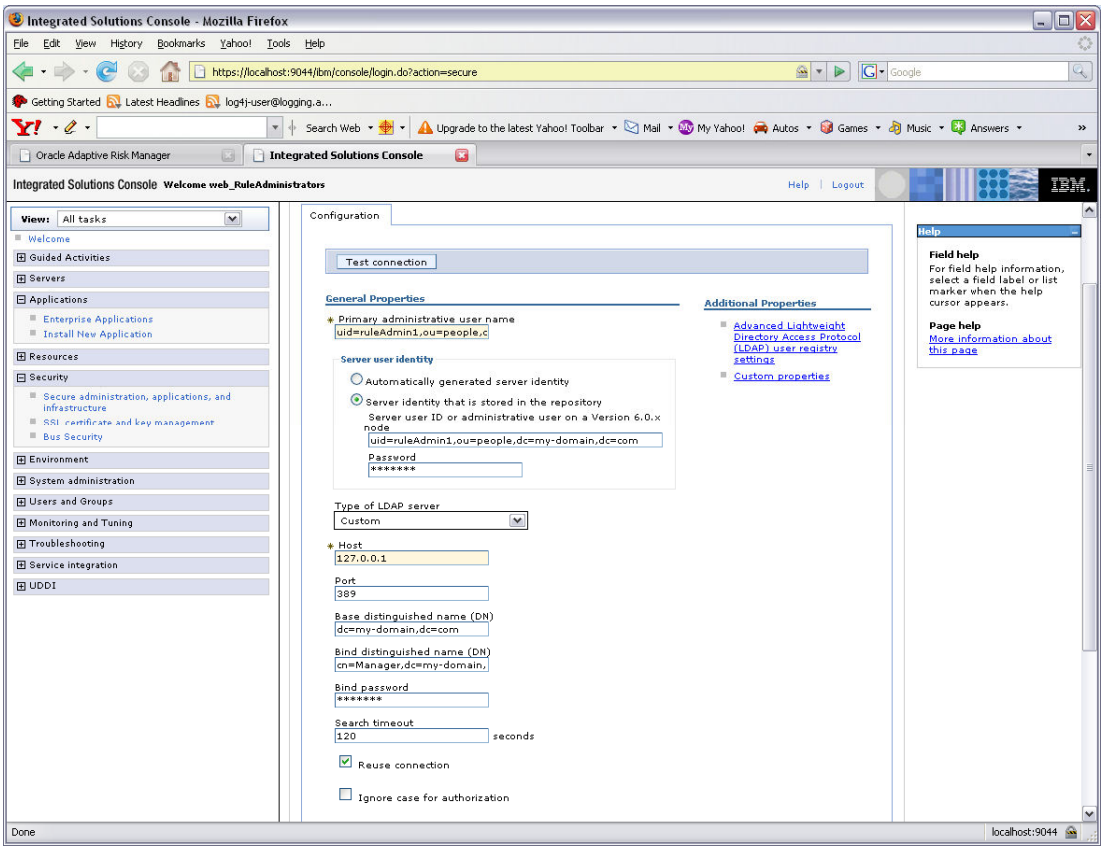
Note: Before making any changes to the authentication realms, make sure to take a backup of the security.xml file as the web admin console would be blocked .

The file is located at C:\Program Files\IBM\WebSphere\<AppServerX>\profiles\AppSrv01\config\cells\<systemnameNodedell>

1. From the Console's left pane, select **Security** and click **Secure administration, applications, and infrastructure**.
2. From the **Available realm definitions** list at the bottom of the main page, choose **Standalone LDAP registry**, and click the **Configure** button.



3. In the General Properties section, enter the values for Primary administrative user name, Type of LDAP server, and all LDAP information.



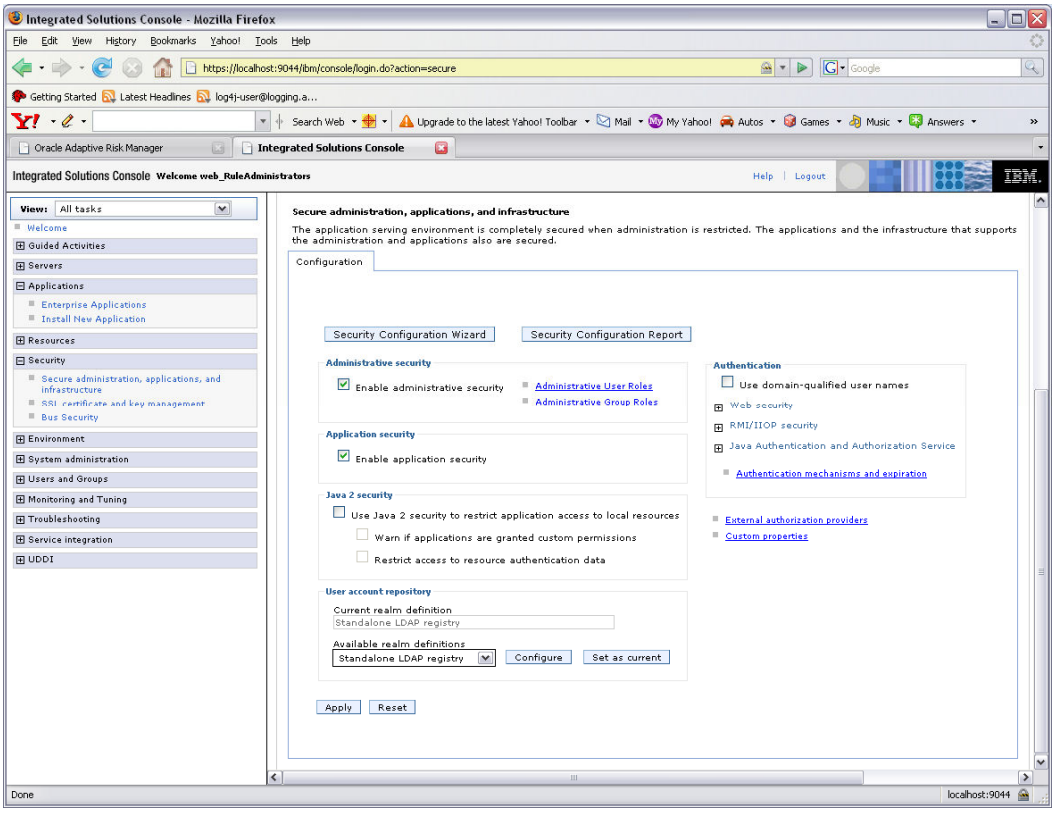
Example values are shown below.

- Primary administrative user name: uid=ruleAdmin1,ou=people,dc=my-domain,dc=com
- Server identity that is stored in the repository Server user ID or administrative user on a Version 6.0.x node: uid=ruleAdmin1,ou=people,dc=my-domain,dc=com
- password: ******
- Type of LDAP server: custom
- Host: 127.0.0.1
- Port: 389
- Base distinguished name (DN): dc=my-domain,dc=com
- Bind distinguished name (DN): cn=Manager,dc=my-domain,dc=com
- Bind password: ********
- Search Timeout: 120
- Reuse connection: checked
- Ignore case for authorization: uncheck
- SSL enabled: uncheck

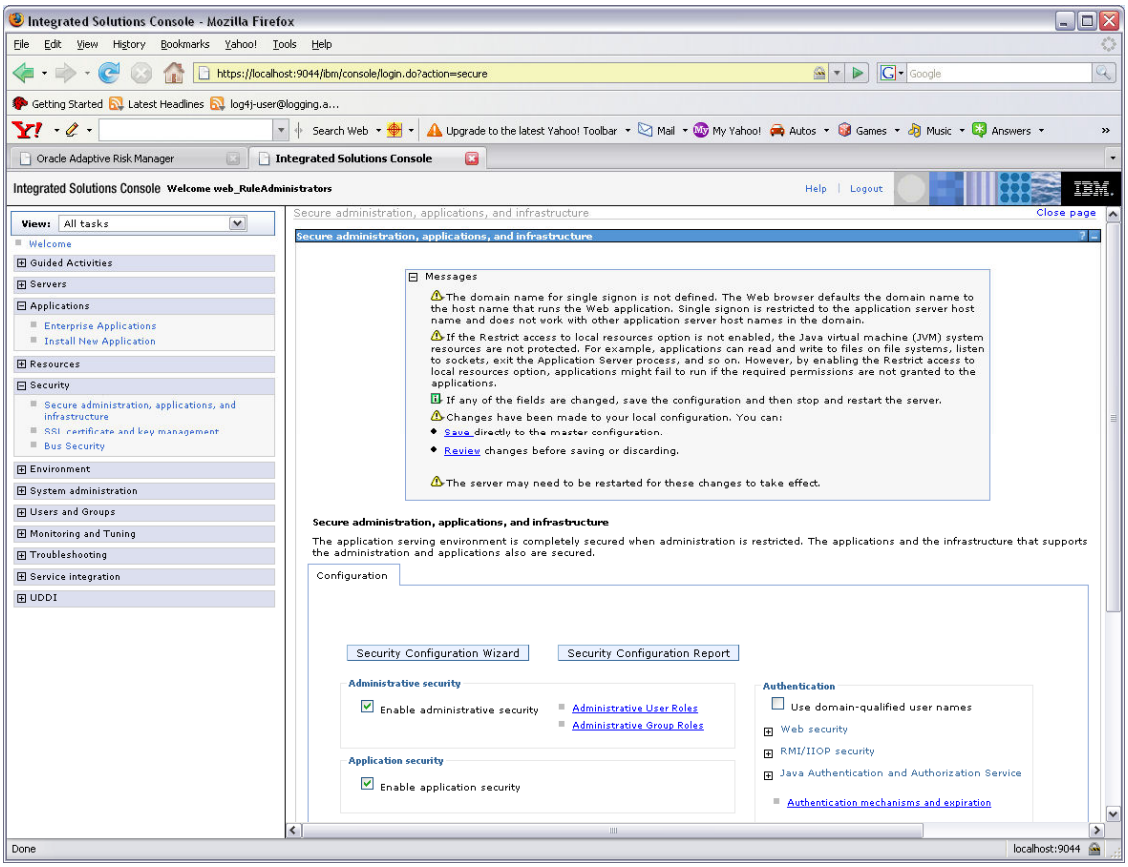
Under the **Additional Properties** section, click the **Advanced Lightweight Directory Access Protocol (LDAP) user registry settings** link.

- User filter: (&(uid=%v)(objectclass=inetOrgPerson))
- Group Filter: (&(cn=%v)(|(objectclass=groupOfNames)(objectclass=groupOfUniqueNames)(objectclass=groupOfURLs)))
- User ID map: uid={0},ou=people,dc=my-domain,dc=com
- Group ID map: ou=roles,dc=my-domain,dc=com
- Group member ID map: uniqueMember
- Perform a nested group search: uncheck (can be checked)
- Certificate map mode: EXACT_DN

4. In **Secure administration, applications, and infrastructure** page's **User account repository** section, click the **Set as Current** button and check that the current realm definition is changed to **Standalone LDAP registry**.

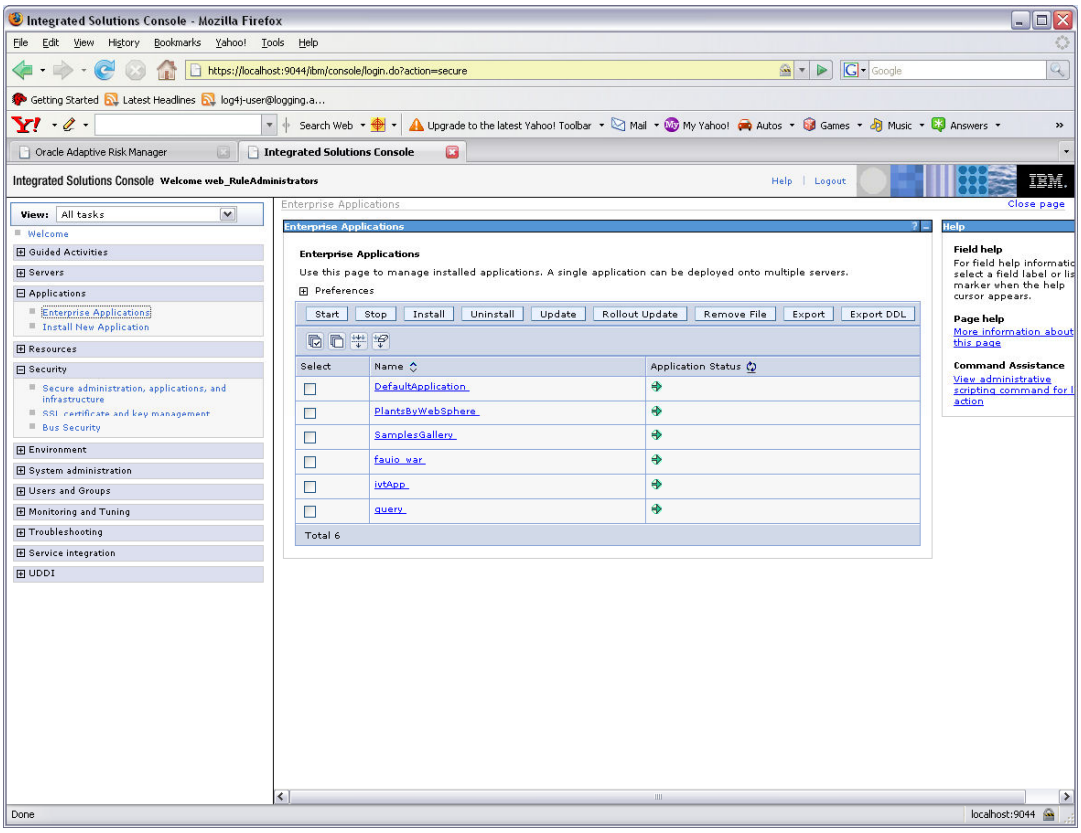


5. Click the **Apply** button to save the master configuration.

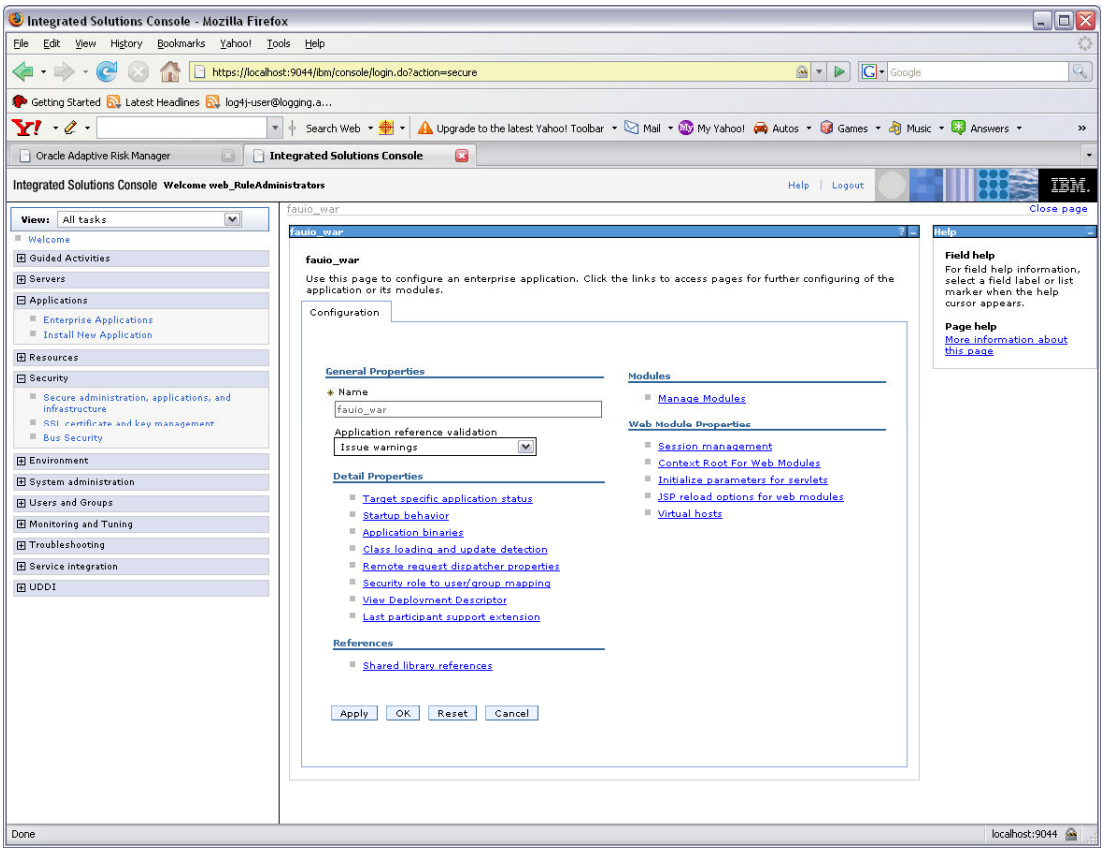


6. From the Console's left pane, select **Applications** and click **Enterprise Application**.

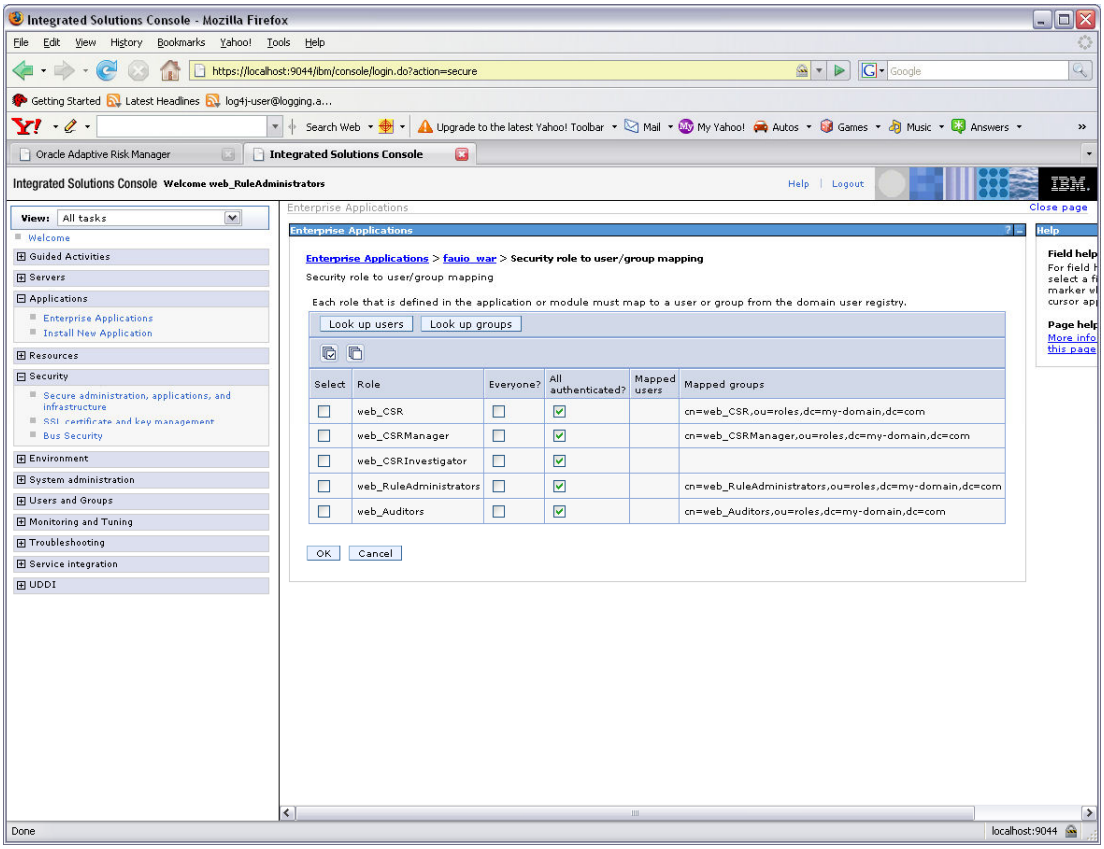
7. On the main page, click the **fauio_war** application link.



8. On the **fauio_war** page, under the **Detailed Properties** section, select **Security role to user/group mapping**.

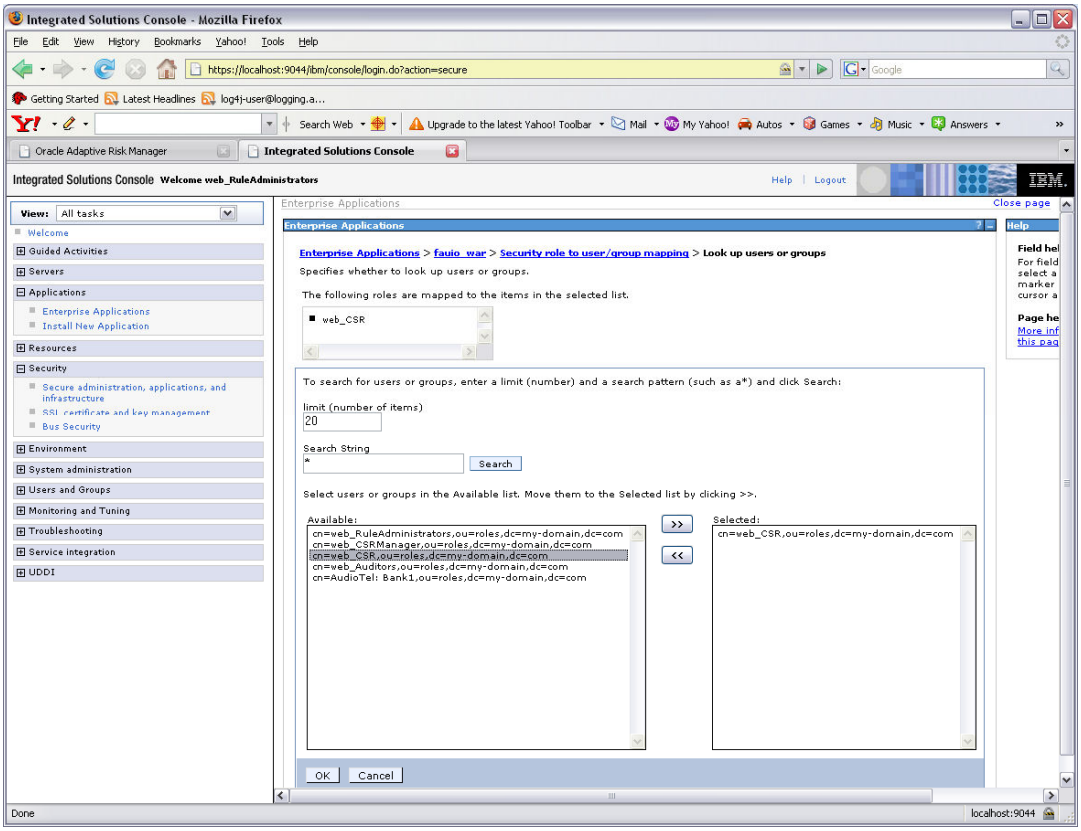


The following page appears.

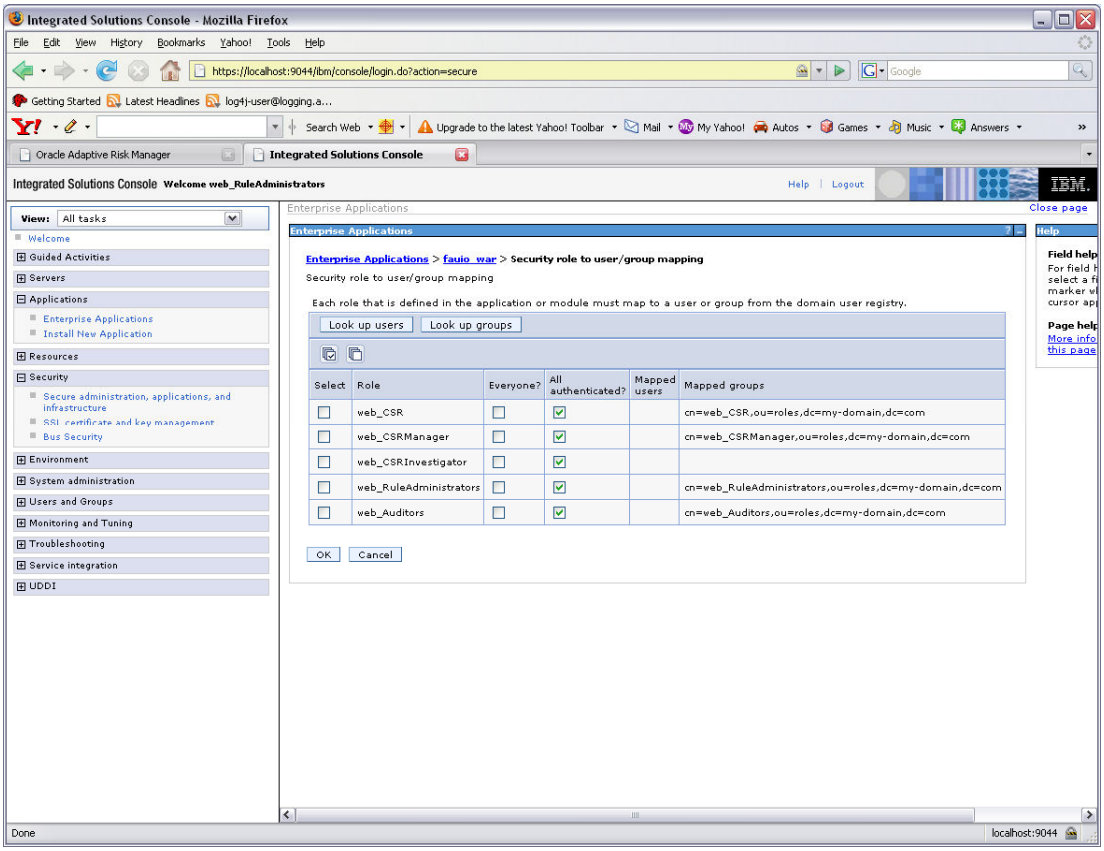


9. Check the **web_CSR** box and click the **Look up groups** button.
10. Perform a search to select and add the groups from the available LDAP groups. If LDAP groups are not present, WebSphere must be restarted.

11. Repeat the process for other application groups and map them to the existing LDAP groups.

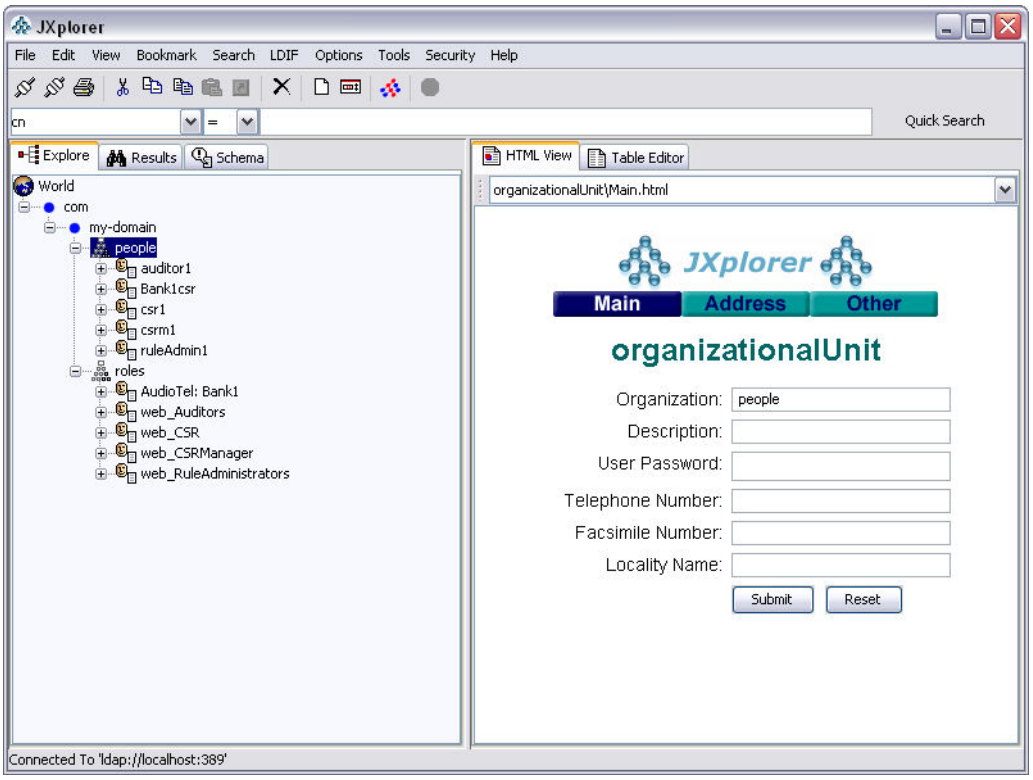


12. Once the groups are mapped check the **All Authenticated** box for each of the groups mapped.

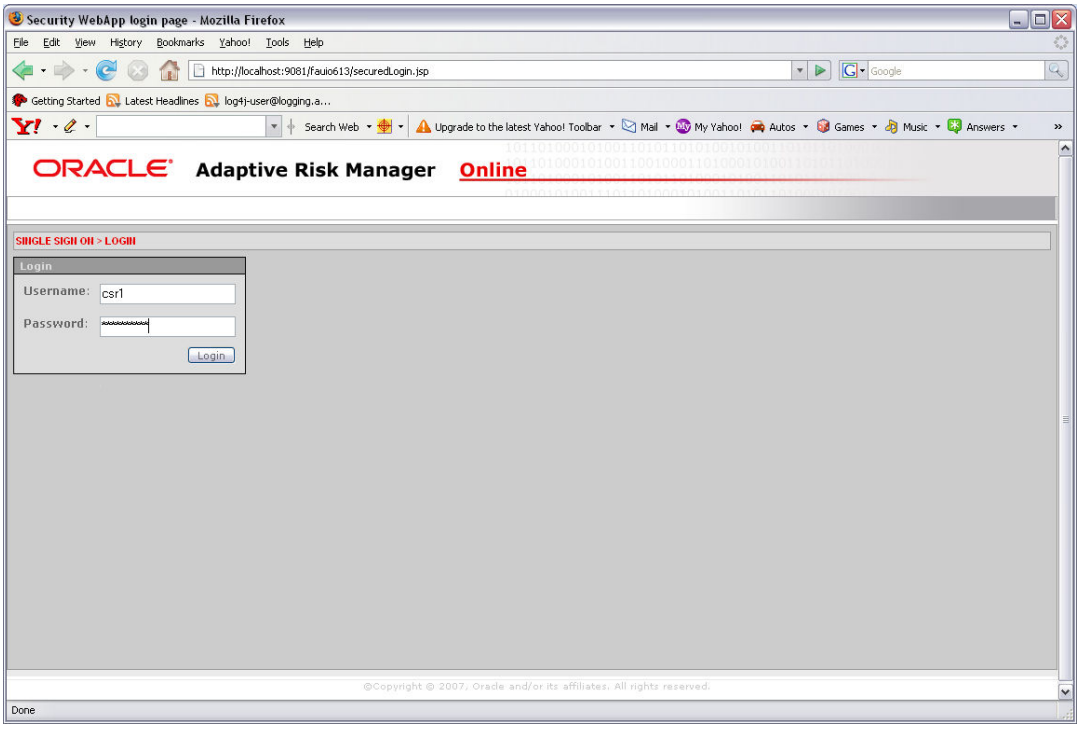


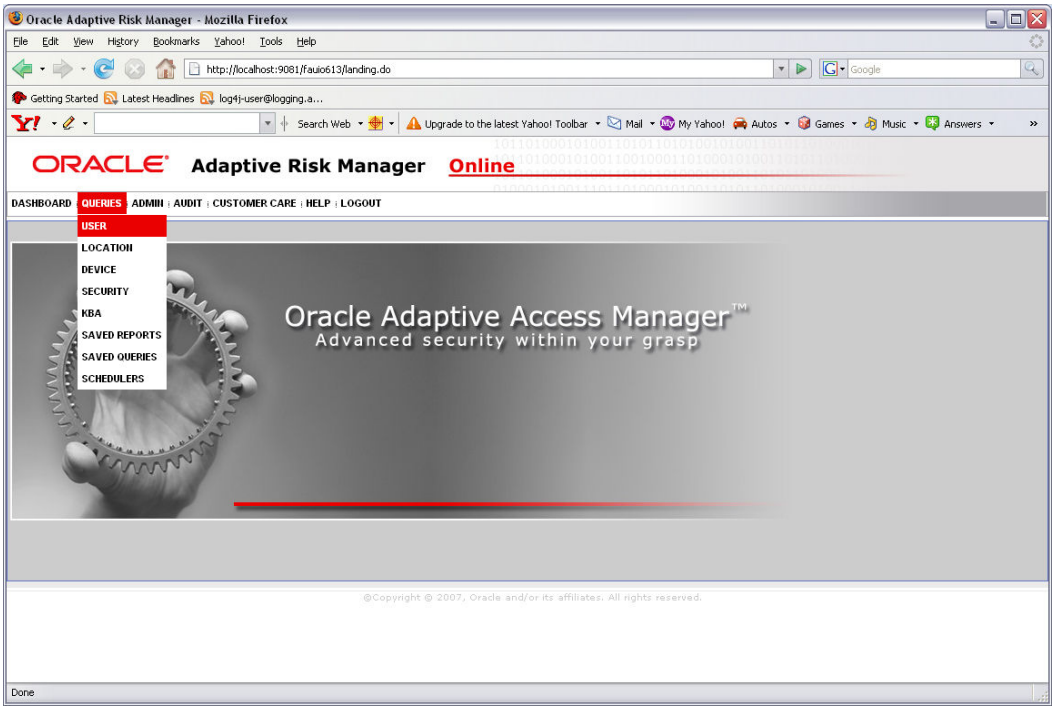
13. Click **OK** to save master configuration: then, restart WebSphere.

Shown below is an example of LDAP in which a user is “picked up“ and the user is a member of one of the groups mapped above



14. Access the application and login with the userid and pswd set in LDAP.





Troubleshooting

Watch for the following error that is displayed after credentials are entered:

Original Exception:

```
Error Message: class loading constraint violated (class:
oracle/xml/parser/v2/XMLNode method:

xdkGetFirstChild()Loracle/xml/parser/v2/XMLNode;) at pc: 0

Error Code: 500

Target Servlet: action

Error Stack:

java.lang.VerifyError: class loading constraint violated (class:
oracle/xml/parser/v2/XMLNode method:

xdkGetFirstChild()Loracle/xml/parser/v2/XMLNode;) at pc: 0

     at java.lang.J9VMInternals.verifyImpl(Native Method)

     at java.lang.J9VMInternals.verify(J9VMInternals.java:59)

     at java.lang.J9VMInternals.verify(J9VMInternals.java:57)

     at java.lang.J9VMInternals.initialize(J9VMInternals.java:120)

     at
oracle.xml.parser.v2.NonValidatingParser.<init>(NonValidatingParser.java:157)

     at oracle.xml.parser.v2.XMLParser.<init>(XMLParser.java:159)

     at oracle.xml.parser.v2.DOMParser.<init>(DOMParser.java:98)

     at oracle.xml.jaxp.JXDocumentBuilder.<init>(JXDocumentBuilder.java:73)

     at
oracle.xml.jaxp.JXDocumentBuilderFactory.newDocumentBuilder(JXDocumentBuilder
Factory.java:79)

     at
oracle.toplink.platform.xml.xdk.XDKParser.getDocumentBuilder(XDKParser.java:1
98)

     at oracle.toplink.platform.xml.xdk.XDKParser.parse(XDKParser.java:160)

     at oracle.toplink.platform.xml.xdk.XDKParser.parse(XDKParser.java:190)

     at


oracle.toplink.tools.sessionconfiguration.XMLSessionConfigLoader.loadDocument
(XMLSessionConfigLoader.java:204)

     at oracle.toplink.tools.sessionconfiguration.XMLSes
```

This error has nothing to do with LDAP settings or OAAM configuration. Ssome of the WAS versions are having issues . WAS 5.x and 6.1.0.0 are few of the ones having issues.

You will have to install updates on the WAS version which have the known issue.