IBM WEBSPHERE APPLICATION SERVER v5.x – EDUCATION ON DEMAND

Setting up Custom Registry

Introduction

This paper discusses in detail the steps involved in setting up a Custom Registry within WebSphere Application Server and enabling Global Security to work with it. For simplicity purposes, we use a file-based User Registry implementation provided within WebSphere Application Server. The implementation class is **com.ibm.websphere.security.FileRegistrySample.**

The sample User Registry implementation reads the users and user groups information from corresponding text-based property files (users.prop and groups.prop). The users' properties file, for example, contains information about each user, which includes the user name, user id, password and the various user groups the user belongs to. The sample property files that we use for this exercise can be found in the download section of the following URL:

http://www-106.ibm.com/developerworks/websphere/techjournal/0303_barcia/barcia.html

For the exercise, the property files are stored under the directory, ${USER_INSTALL_ROOT} /security, where ${USER_INSTALL_ROOT} is the directory in which WebSphere Application Server has been installed.

Configuring WebSphere to use the Custom Registry

To setup the sample User Registry within WebSphere Application Server:

____ 1. Open a web browser and type in the URL (http://hostname:9090/admin) to launch the Administrative Console for WebSphere Application Server.

____ 2. On the left frame of the console, Select **Security -> User Registries -> Custom** (Figure 1)

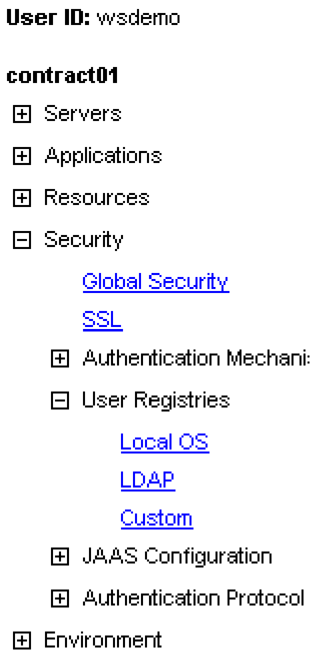
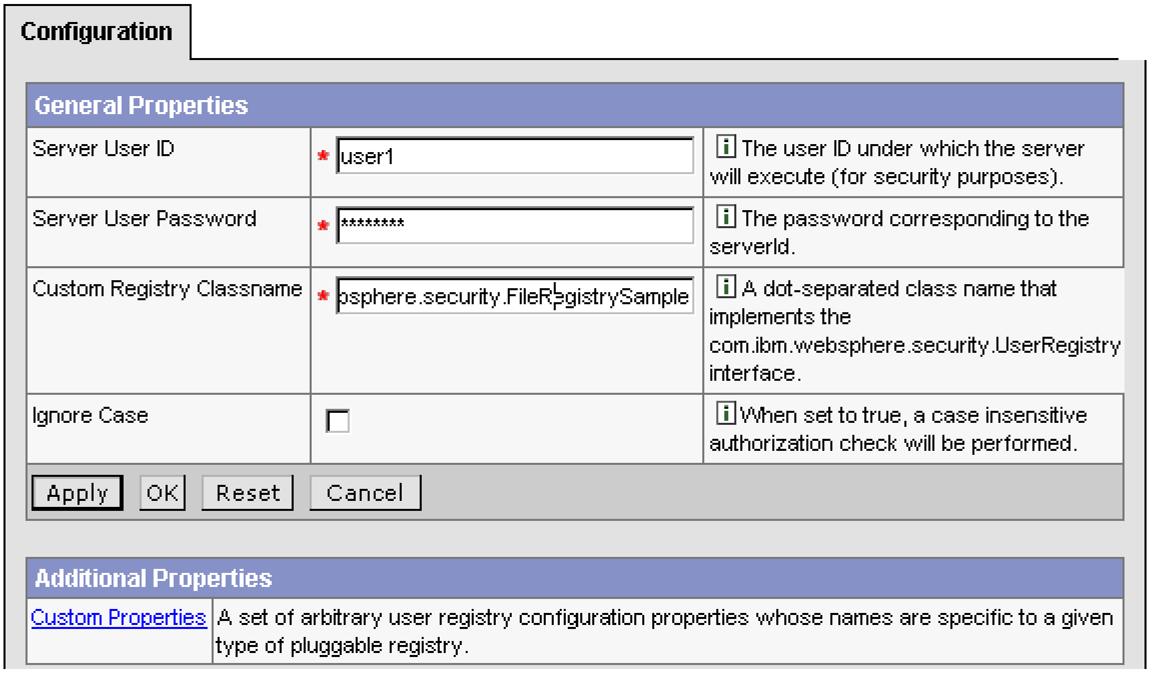


Figure 1

The page for **Custom Registry configuration** is displayed on the right.

____ 3. Provide all the information as shown in the picture below



General Properties		
Server User ID	* user1	The user ID under which the server will execute (for security purposes).
Server User Password	* ********	The password corresponding to the serverId.
Custom Registry Classname	* psphere.security.FileRegistrySample	A dot-separated class name that implements the com.ibm.websphere.security.UserRegistry interface.
Ignore Case	□	When set to true, a case insensitive authorization check will be performed.

Additional Properties	
Custom Properties	A set of arbitrary user registry configuration properties whose names are specific to a given type of pluggable registry.

Figure 2

Server User ID: The User ID to use to configure and administer WebSphere Application Server from the Administrative Console. The User ID used above (user1) is one of the users contained in the users property file. In our case, we use **user1**.

Server User Password: The password for the above user. The password can be read from the **users.prop** file.

Custom Registry classname: The name of the class implementing the WebSphere **UserRegistry** interface. In our case, it is **com.ibm.websphere.security.FileRegistrySample.** This class provides the actual implementation of the Registry that authenticates the user credentials based on the user and user group information in the text-based property files.

____ 4. Click **Apply** to save the settings.

____ 5. As mentioned earlier, the sample User Registry implementation reads the user/group information from the property files. The location of these property files is specified by setting custom properties for this Registry. Scroll down the screen until you see the **Custom Properties** link.

In the **Custom Properties** window, press **New** and then enter the following data (Figure 3) to configure the **usersFile** property:

Name: usersFile

Value: ${USER_INSTALL_ROOT}/security/users.prop

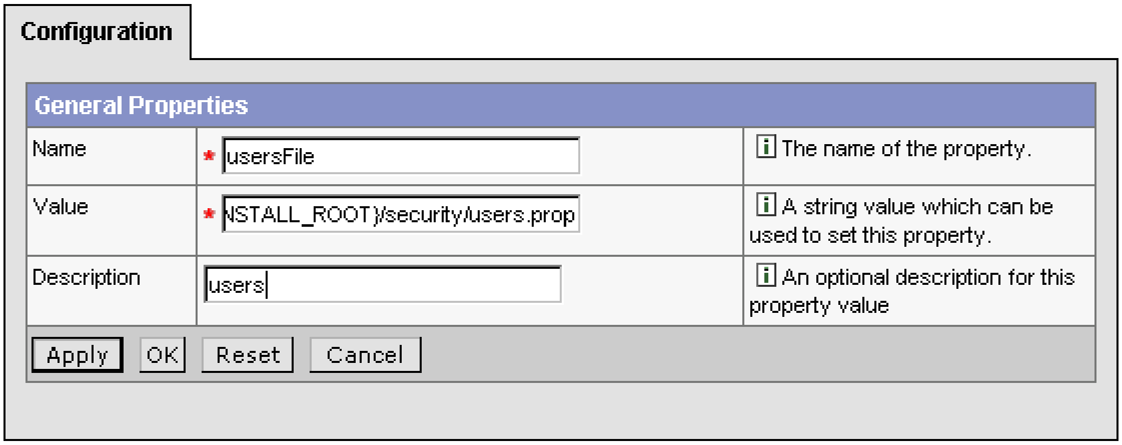
${USER_INSTALL_ROOT} is the directory in which WebSphere Application Server has been installed.

The users' property file consists of entries for each authenticated users of the application. A simple entry in this file looks like the following:

user1:password:123:567,987:User1

The file follows a simple format as shown below:

<user name>:<password>:<unique user identifier>:<identifiers of groups user belongs to commas separated>:<Display Name>



Configuration

General Properties

Name	* usersFile	The name of the property.
Value	* NSTALL_ROOT}/security/users.prop	A string value which can be used to set this property.
Description	users	An optional description for this property value

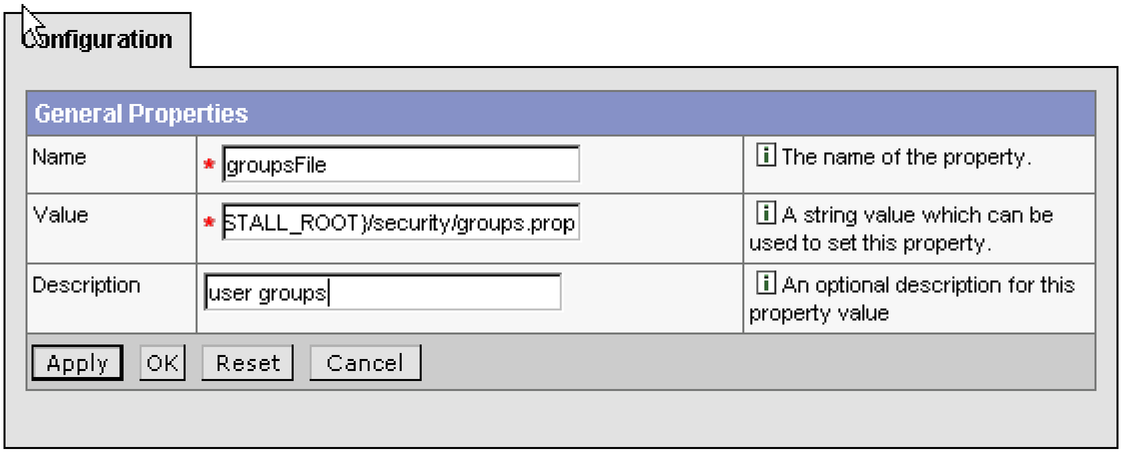
Figure 3

____ 6. Click **OK**.

____ 7. Similarly, add new custom property to set the location of the user groups property file. In the **Custom Properties** window, click **New** and enter the following data (Figure 4):

Name: groupsFile

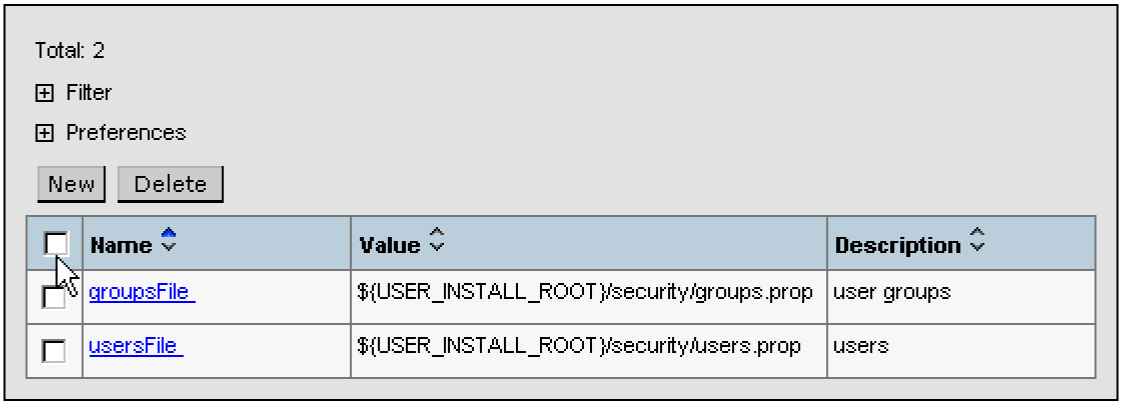
Value: ${USER_INSTALL_ROOT}/security/groups.prop



Name	* groupsFile	The name of the property.
Value	* STALL_ROOT}/security/groups.prop	A string value which can be used to set this property.
Description	user groups	An optional description for this property value

Figure 4

Click **OK**. The users and groups properties should now be properly configured, as shown in Figure 5 below:

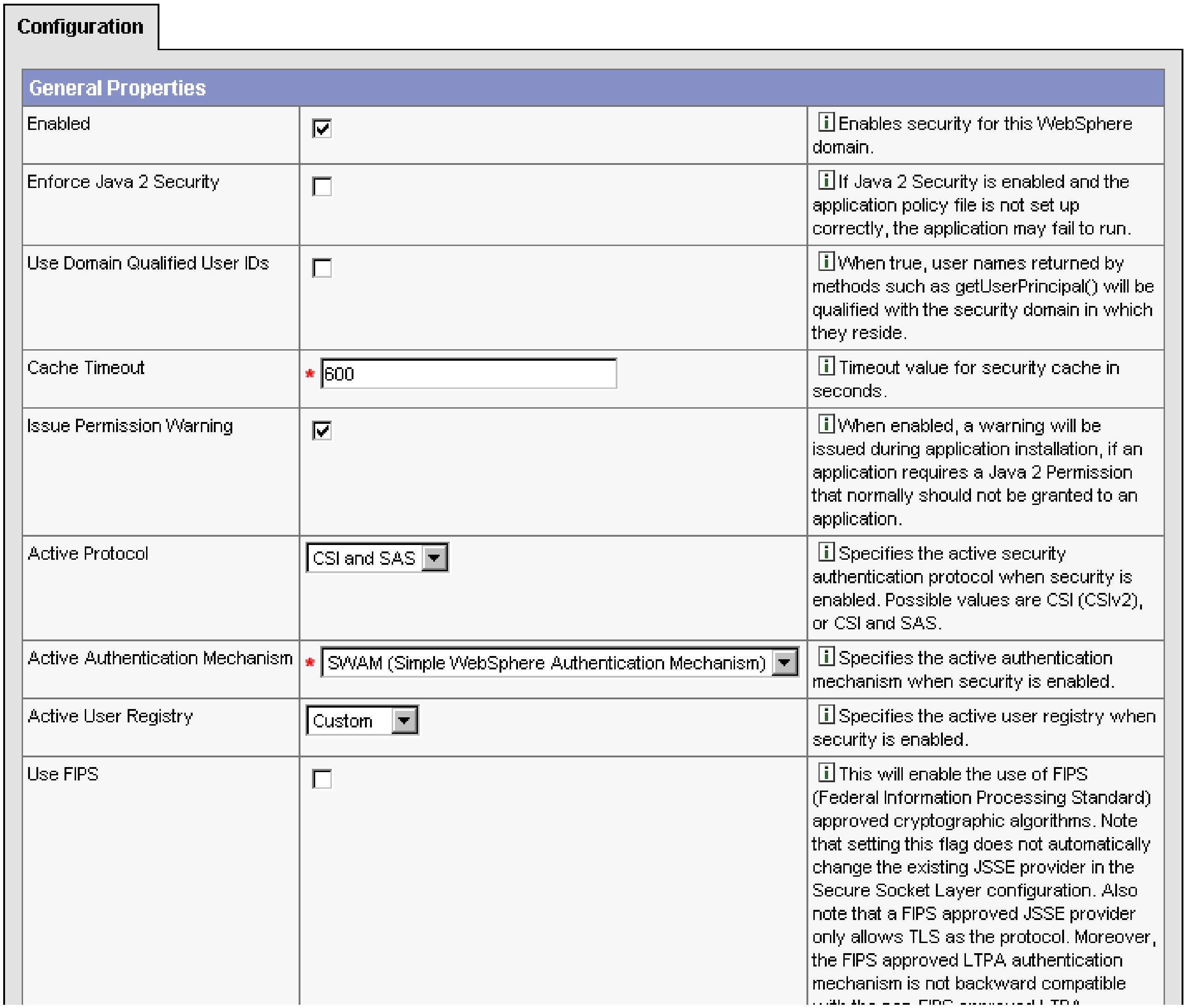

Total: 2

□	Name	Value	Description
□	groupsFile	${USER_INSTALL_ROOT}/security/groups.prop	user groups
□	usersFile	${USER_INSTALL_ROOT}/security/users.prop	users

Figure 5

____ 8. With the custom registry successfully configured, we now need to enable our Global Security. From the navigation menu on the left of the Administration Console, select **Security -> Global Security**.

____ 9. In the Global Security window (Figure 6), check the **Enabled** box to enable Global Security. De-select Enforce Java 2 Security. Java 2 Security enforces policy files to protect different resources, but such strict requirements are not necessary for our implementation.



Configuration

General Properties

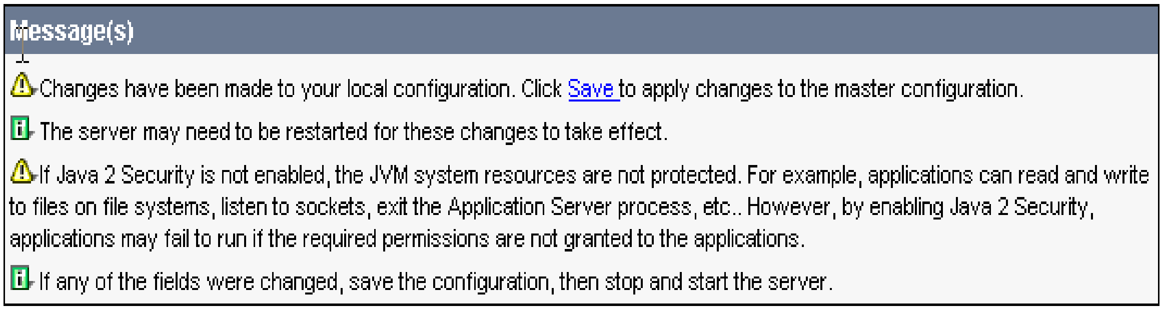
Enabled	☑	Enables security for this WebSphere domain.
Enforce Java 2 Security	□	If Java 2 Security is enabled and the application policy file is not set up correctly, the application may fail to run.
Use Domain Qualified User IDs	□	When true, user names returned by methods such as getUserPrincipal() will be qualified with the security domain in which they reside.
Cache Timeout	* 600	Timeout value for security cache in seconds.
Issue Permission Warning	☑	When enabled, a warning will be issued during application installation, if an application requires a Java 2 Permission that normally should not be granted to an application.
Active Protocol	CSI and SAS	Specifies the active security authentication protocol when security is enabled. Possible values are CSI (CSIv2), or CSI and SAS.
Active Authentication Mechanism	* SWAM (Simple WebSphere Authentication Mechanism)	Specifies the active authentication mechanism when security is enabled.
Active User Registry	Custom	Specifies the active user registry when security is enabled.
Use FIPS	□	This will enable the use of FIPS (Federal Information Processing Standard) approved cryptographic algorithms. Note that setting this flag does not automatically change the existing JSSE provider in the Secure Socket Layer configuration. Also note that a FIPS approved JSSE provider only allows TLS as the protocol. Moreover, the FIPS approved LTPA authentication mechanism is not backward compatible

Figure 6

____ 10. For Active User Registry, select **Custom** from the list.

____ 11. Leave the default values for the remaining fields and press **OK**.

____ 12. Now that all necessary changes have been made, we need to save our configuration changes. Click on **Save** on the top menu, or on the **Save link** in the Message(s) dialog (Figure 7), if displayed.



Message(s)

⚠ Changes have been made to your local configuration. Click Save to apply changes to the master configuration.

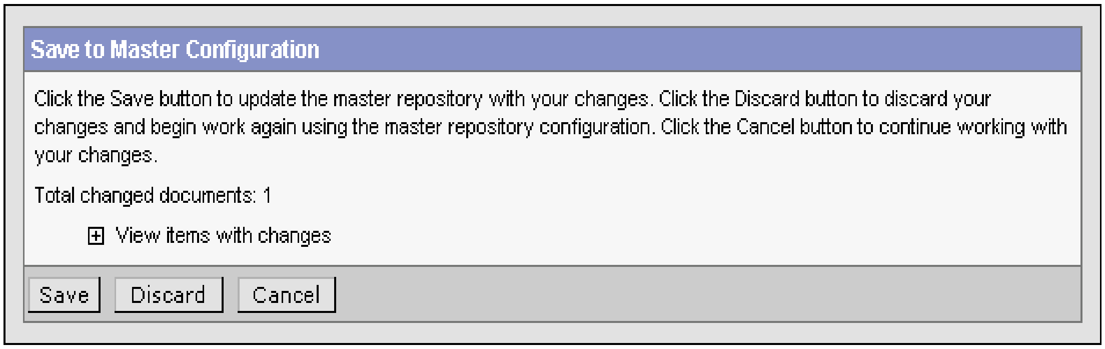
ℹ The server may need to be restarted for these changes to take effect.

⚠ If Java 2 Security is not enabled, the JVM system resources are not protected. For example, applications can read and write to files on file systems, listen to sockets, exit the Application Server process, etc.. However, by enabling Java 2 Security, applications may fail to run if the required permissions are not granted to the applications.

ℹ If any of the fields were changed, save the configuration, then stop and start the server.

Figure 7

____ 13. Click the **Save** button in the Save window (Figure 8) to make the configuration change final.



Save to Master Configuration

Click the Save button to update the master repository with your changes. Click the Discard button to discard your changes and begin work again using the master repository configuration. Click the Cancel button to continue working with your changes.

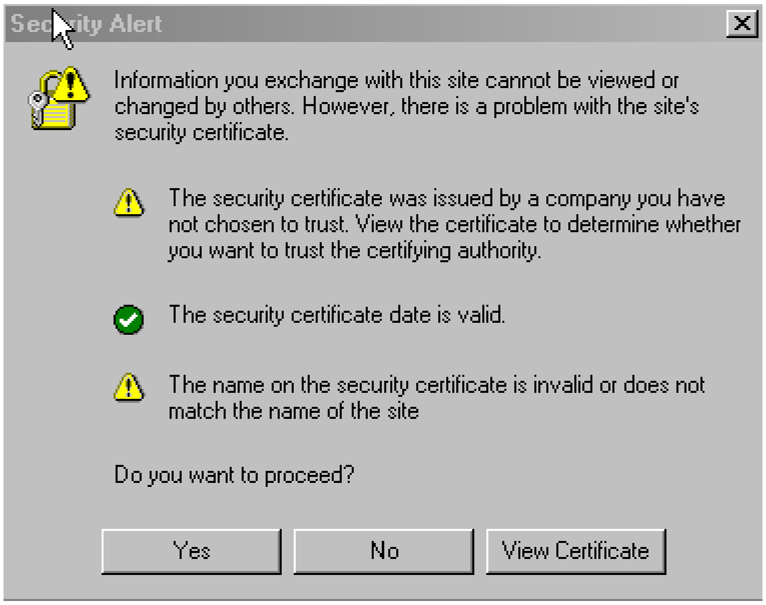
Total changed documents: 1

⊞ View items with changes

Figure 8

____ 14. For the User Registry configuration to take affect, we need to restart the Application Server. Logout of the Administration Console and restart the Application Server.

____ 15. After successful Server restart, open the Administration console from a web browser. Note the security alert window (Figure 9) that pops up before the console is displayed. This is due to the Global Security that we turned on earlier.



Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.

The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.

The security certificate date is valid.

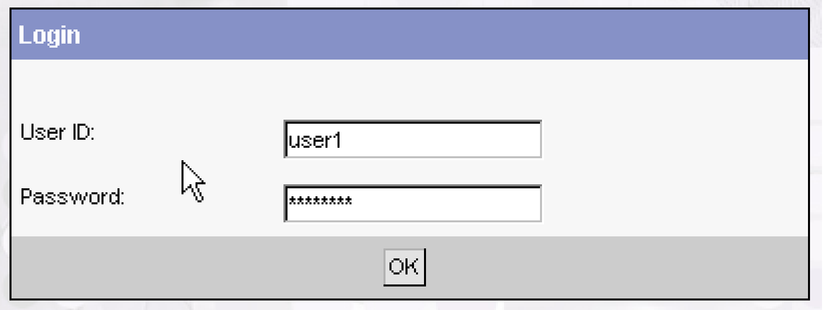
The name on the security certificate is invalid or does not match the name of the site

Do you want to proceed?

Figure 9

Click **Yes** on the security alert window.

____ 16. This time the Administration console Login screen prompts for a User ID and Password. Type in the Server user ID and password that was used when configuring the user registry.



User ID: user1

Password: ********

Figure 10

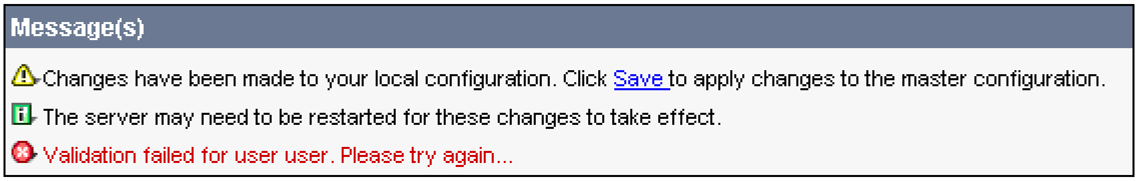
____ 17. Click **OK** to access the Administration Console.

It might happen that the security is not configured right and you need to debug to find the cause of the problem. WebSphere Application Server updates various log files with error messages, whenever there is a failure. The next section briefly discusses the problem areas and the log files to look for to track down the problem.

Security Problem Determination

➢ ***Check configuration of the Custom Registry***

In the Administration Console, when the Global Security is enabled (Figure 6 above) and the user Clicks '**OK**' to save the changes, WebSphere Application Server attempts to verify the Server User ID and password against the specified User Registry configuration. If the entered values (for Server User ID and password) are incorrect, you will get an error message (similar to Figure 11) indicating that the validation failed and the setting cannot be saved.



⚠ Changes have been made to your local configuration. Click Save to apply changes to the master configuration.

The server may need to be restarted for these changes to take effect.

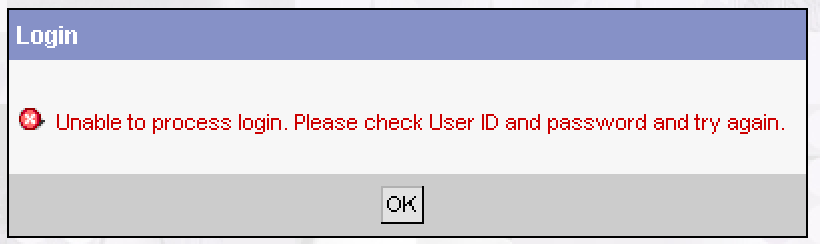
Validation failed for user user. Please try again...

Figure 11

Similar problem occurs if the specified Custom Registry implementation class is not valid or cannot be found in the classpath.

➢ ***Check the user ID and password used to access the Administration Console***

If the user ID and password entered in the login screen to access the Administration Console is not the same as the ones used to configure security, you will see the following screen when accessing the console:



Unable to process login. Please check User ID and password and try again.

Figure 12

Check your security settings to make sure you entered the correct user id/password.

➢ ***Checking JVM log files for security related messages***

The SystemOut.log for an Application Server, Node Agent, or the Deployment Manager will also indicate successful starting of the Security Server. There are no special requirements to view this log. It is located in the *installation_directory/logs/applicationServerName* directory, and by default is named SystemOut.log. There are two techniques that you can use to view the JVM log for an application server.

____ 1. View the JVM logs from the Administrative Console.

__ a. Start the Administrative Console.

__ b. Click **Troubleshooting > Logs and Trace** in the console navigation tree. To view the logs for a particular server, click on the server name to select it, and then click **JVM Logs**.

__ c. Select the **Runtime** tab.

__ d. Click **View** corresponding to the log you want to view.

____ 2. View the JVM logs from the machine where they are stored.

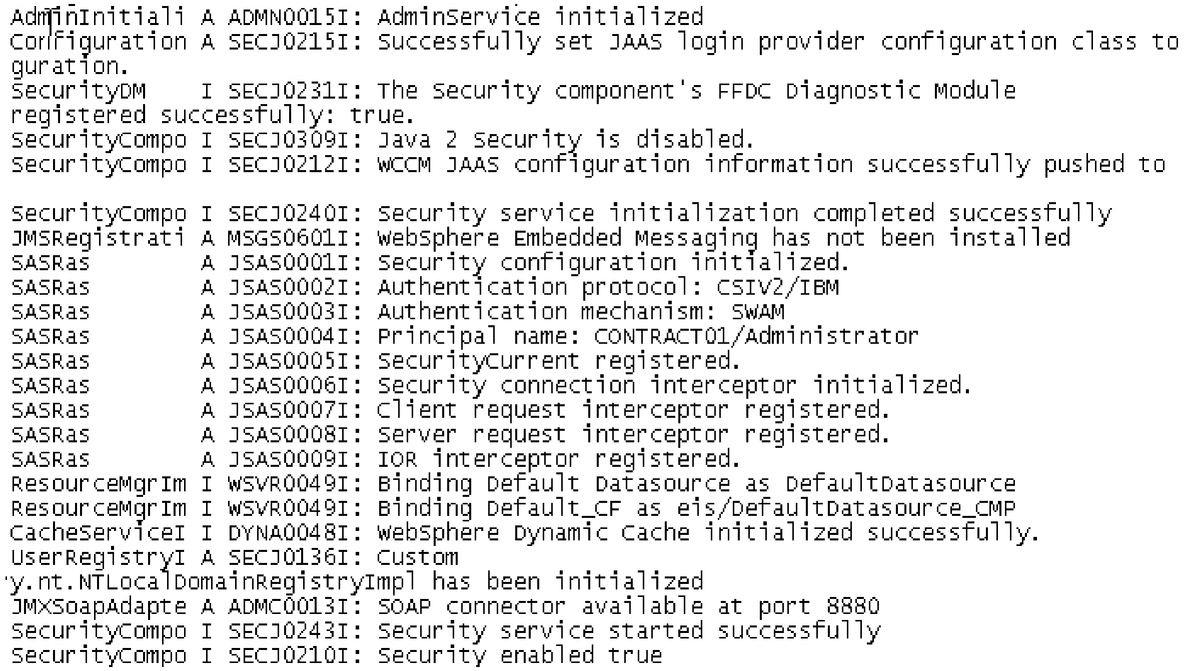
__ a. Go to the machine where the logs are stored.

__ b. Open the file in a text editor or drag and drop the file into an editing and viewing program.

➢ ***Did security appear to initialize properly?***

A lot of security code is visited during initialization. So you will likely see problems there first if the problem is configuration related. The following sequence of messages generated in the SystemOut.log indicates normal code initialization of an application server in which the security service has started successfully:

This sequence will vary based on the configuration, but the messages are similar:



```
 AdminInitiali A ADMN0015I: AdminService initialized
 Configuration A SECJ0215I: Successfully set JAAS login provider configuration class to
 guration.
 SecurityDM    I SECJ0231I: The Security component's FFDC Diagnostic Module
 registered successfully: true.
 SecurityCompo I SECJ0309I: Java 2 Security is disabled.
 SecurityCompo I SECJ0212I: WCCM JAAS configuration information successfully pushed to

 SecurityCompo I SECJ0240I: Security service initialization completed successfully
 JMSRegistrati A MSGS0601I: WebSphere Embedded Messaging has not been installed
 SASRas        A JSAS0001I: Security configuration initialized.
 SASRas        A JSAS0002I: Authentication protocol: CSIV2/IBM
 SASRas        A JSAS0003I: Authentication mechanism: SWAM
 SASRas        A JSAS0004I: Principal name: CONTRACT01/Administrator
 SASRas        A JSAS0005I: SecurityCurrent registered.
 SASRas        A JSAS0006I: Security connection interceptor initialized.
 SASRas        A JSAS0007I: Client request interceptor registered.
 SASRas        A JSAS0008I: Server request interceptor registered.
 SASRas        A JSAS0009I: IOR interceptor registered.
 ResourceMgrIm I WSVR0049I: Binding Default Datasource as DefaultDatasource
 ResourceMgrIm I WSVR0049I: Binding Default_CF as eis/DefaultDatasource_CMP
 CacheServiceI I DYNA0048I: WebSphere Dynamic Cache initialized successfully.
 UserRegistryI A SECJ0136I: Custom
y.nt.NTLocalDomainRegistryImpl has been initialized
 JMXSoapAdapte A ADMC0013I: SOAP connector available at port 8880
 SecurityCompo I SECJ0243I: Security service started successfully
 SecurityCompo I SECJ0210I: Security enabled true
```

If none of these steps solves the problem, check to see if the problem has been identified and documented using the links in:

1. **Diagnosing and fixing problems: Resources for learning**

   http://publib.boulder.ibm.com/infocenter/ws51help/index.jsp?topic=/com.ibm.websphere.base.doc/info/aes/ae/rtrb_allrfl.html

2. If you do not see a problem that resembles yours, or if the information provided does not solve your problem, contact **IBM support** for further assistance.

   http://www-1.ibm.com/support/docview.wss?rs=180&context=SSEQTP&uid=swg21145599

Reference:

- **Custom User Registries**

  http://publib.boulder.ibm.com/infocenter/ws51help/index.jsp?topic=/com.ibm.websphere.base.doc/info/aes/ae/rsec_customauth.html

- **Security Troubleshooting Tips**

  http://publib.boulder.ibm.com/infocenter/ws51help/index.jsp?topic=/com.ibm.websphere.base.doc/info/aes/ae/rtrb_securitycomp.html

- **IBM WebSphere V5.0 Security Handbook**

  http://www.redbooks.ibm.com/redbooks/SG246573.html

Trademarks and Disclaimers

The following terms are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both:

IBM
IBM(logo)
e(logo)business
Tivoli
iSeries
pSeries
xSeries
zSeries
OS/400
AIX
CICS
OS/390
Informix
Cloudscape
DB2 Universal Database
IMS
WebSphere
MQSeries
DB2
Lotus

Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both. Microsoft, Windows, Windows NT, and

the Windows logo are registered trademarks of Microsoft Corporation in the United States, other countries, or both. Intel, ActionMedia, LANDesk, MMX, Pentium and ProShare are

trademarks of Intel Corporation in the United States, other countries, or both. UNIX is a registered trademark of The Open Group in the United States and other countries. Linux is a registered trademark of Linus Torvalds. Other company, product and service names may be trademarks or service marks of others.

Product data has been reviewed for accuracy as of the date of initial publication. Product data is subject to change without notice. This document could include technical inaccuracies or typographical errors. IBM may make improvements and/or changes in the product(s) and/or program(s) described herein at any time without notice. Any statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only. References in this document to IBM products, programs, or services does not imply that IBM intends to make such products, programs or services available in all countries in which IBM operates or does business. Any reference to an IBM Program Product in this document is not intended to state or imply that only that program product may be used. Any functionally equivalent program, that does not infringe IBM's intellectual property rights, may be used instead.

Information is provided "AS IS" without warranty of any kind. THE INFORMATION PROVIDED IN THIS DOCUMENT IS DISTRIBUTED "AS IS" WITHOUT ANY WARRANTY, EITHER EXPRESS OR IMPLIED. IBM EXPRESSLY DISCLAIMS ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NONINFRINGEMENT. IBM shall have no responsibility to update this information. IBM products are warranted, if at all, according to the terms and conditions of the agreements (e.g., IBM Customer Agreement, Statement of Limited Warranty, International Program License Agreement, etc.) under which they are provided. Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products in connection with this publication and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. IBM makes no representations or warranties, express or implied, regarding non-IBM products and services.

The provision of the information contained herein is not intended to, and does not, grant any right or license under any IBM patents or copyrights. Inquiries regarding patent or copyright licenses should be made, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

Performance is based on measurements and projections using standard IBM benchmarks in a controlled environment. All customer examples described are presented as illustrations of how those customers have used IBM products and the results they may have achieved. The actual throughput or performance that any user will experience will vary depending upon considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve throughput or performance improvements equivalent to the ratios stated here.

Note to U.S. Government Users - Documentation related to restricted rights-Use, duplication or disclosure is subject to restrictions set forth in GSA ADP Schedule Contract and IBM Corp.