IBM WEBSPHERE APPLICATION SERVER v5.x – EDUCATION ON DEMAND

Configuring WebSphere to use SSL for LDAP(LDAPS)

Introduction

This paper will discuss how to establish a Secure Sockets Layer (SSL) connection between WebSphere Application Server and a Lightweight Directory Access Protocol (LDAP) server for WebSphere Application Server V5.

We assume that the user registry we use was created with a sample user (wsadmin) and a sample group entry in the directory by using IBM Directory Server. We did not import a schema, but set up a user following the process described below:

For our example, we use the X.500 methodology that will set the root of the directory to a specific organization.

-Set the following suffix: **o=ibm**.

- Set the administrator DN: **cn=root**.

- Create a new server: **ldap://<supertiger.austin.ibm.com>:389**

- Adding an organization to the new server created previously: **o=ibm** as the Entry RDN (Relative Distinguished Name)

- Adding a new user (a new administrative user in order to set a Security Server ID in the WebSphere Global Security settings, for use as the user ID under which the server runs for security purposes.) to the new organization created previously: **cn=wsadmin** as the Entry RDN, **o=ibm** as the Parent DN.

- Adding a new group: **cn=admingrp** as the Entry RDN and assign the following group member to the group: **cn=wasadmin**, **o=ibm**.

Note: It is possible to add users and groups using an LDIF file, a standard format for representing LDAP entries in text form. This will be useful when the number of entries to add is very large.

We will then provide an example of how to configure WebSphere to use the given LDAP server over a normal LDAP connection, and then use SSL for LDAP (LDAPS).

Setting up an SSL connection between WebSphere Application Server and an LDAP server requires the following scenarios. There are two scenarios; the second built upon the first one:

- The first scenario covers the basic LDAP configuration with WebSphere Application Server.
- The second scenario covers how to enable the connection to use SSL for LDAP (LDAPS), providing security to WebSphere LDAP communication.

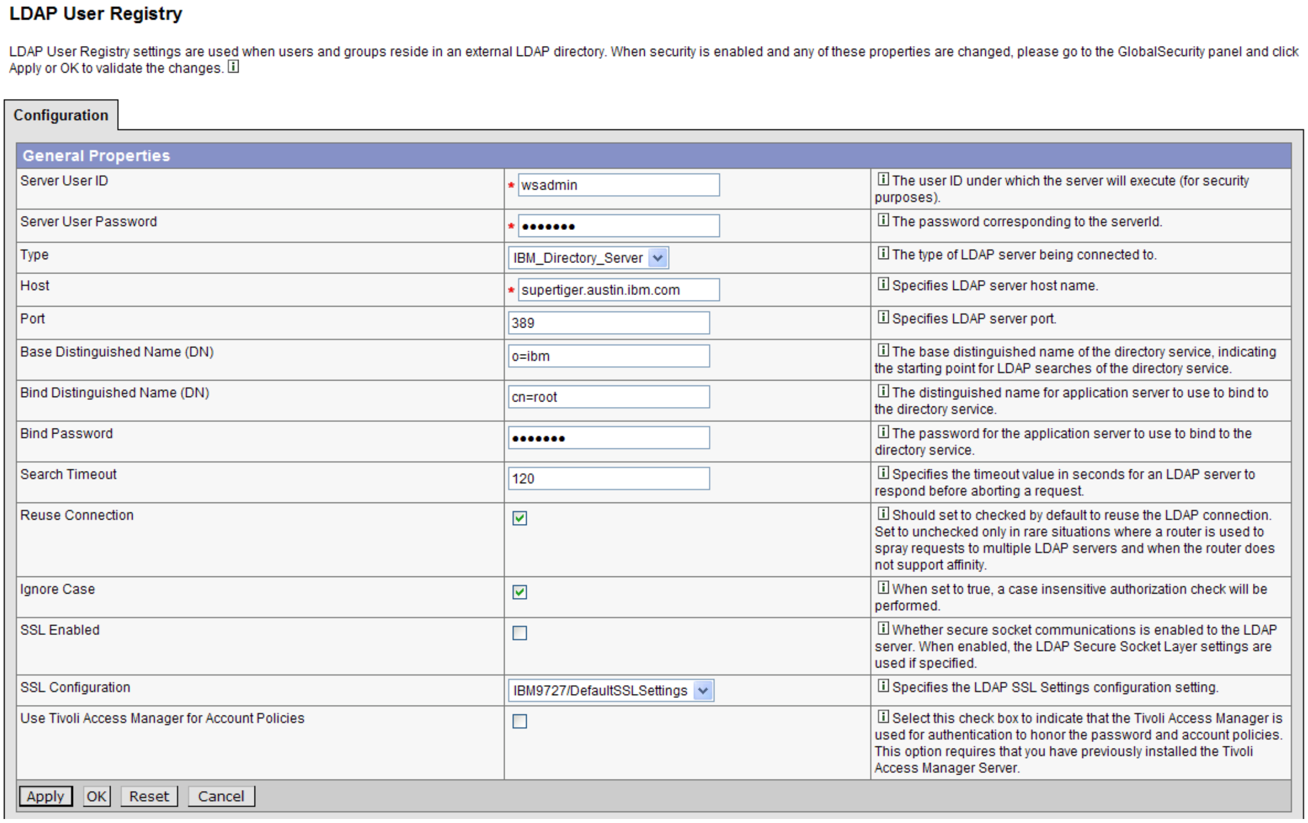
Part 1: Configuring WebSphere to use the LDAP user registry

In order to use the LDAP directory of your choice as the user registry, WebSphere has to be configured properly.

____ 1. Launch the Administrative Console for WebSphere.

____ 2. Select **Security -> User Registries -> LDAP**; this page will provide the settings for the LDAP configuration.

____ 3. Provide all the information shown in the picture below according to your system settings.



LDAP User Registry

LDAP User Registry settings are used when users and groups reside in an external LDAP directory. When security is enabled and any of these properties are changed, please go to the GlobalSecurity panel and click Apply or OK to validate the changes.

Configuration

General Properties		
Server User ID	* wsadmin	The user ID under which the server will execute (for security purposes).
Server User Password	* •••••••	The password corresponding to the serverId.
Type	IBM_Directory_Server	The type of LDAP server being connected to.
Host	* supertiger.austin.ibm.com	Specifies LDAP server host name.
Port	389	Specifies LDAP server port.
Base Distinguished Name (DN)	o=ibm	The base distinguished name of the directory service, indicating the starting point for LDAP searches of the directory service.
Bind Distinguished Name (DN)	cn=root	The distinguished name for application server to use to bind to the directory service.
Bind Password	•••••••	The password for the application server to use to bind to the directory service.
Search Timeout	120	Specifies the timeout value in seconds for an LDAP server to respond before aborting a request.
Reuse Connection	☑	Should set to checked by default to reuse the LDAP connection. Set to unchecked only in rare situations where a router is used to spray requests to multiple LDAP servers and when the router does not support affinity.
Ignore Case	☑	When set to true, a case insensitive authorization check will be performed.
SSL Enabled	☐	Whether secure socket communications is enabled to the LDAP server. When enabled, the LDAP Secure Socket Layer settings are used if specified.
SSL Configuration	IBM9727/DefaultSSLSettings	Specifies the LDAP SSL Settings configuration setting.
Use Tivoli Access Manager for Account Policies	☐	Select this check box to indicate that the Tivoli Access Manager is used for authentication to honor the password and account policies. This option requires that you have previously installed the Tivoli Access Manager Server.

Server User ID: Enter a valid user name in the **Server User ID** field. You can either enter the complete distinguished name (DN) of the user or the short name of the user as defined by the **User Filter** in the **Advanced LDAP** settings panel. In our example, this is set to `wsadmin`.

Server User Password: Enter the password of the user in the **Server User Password** field.

Host: Specifies the host ID (IP address or domain name system (DNS) name) of the LDAP server: In our example, this is set to `supertiger.austin.ibm.com.`

Port: Specifies the host port of the LDAP server. Take the default value: 389

Note: If the port, including the default port number, is specified explicitly in one server configuration, then verify that it is specified explicitly in all server configurations.

Base Distinguished Name: Specifies the base distinguished name of the directory service, indicating the starting point for LDAP searches of the directory service, In our example, this is set to **o=ibm.**

Bind Distinguished Name: Specifies the distinguished name for the application server to use when binding to the directory service. If no name is specified, the application server binds anonymously. See the Base Distinguished Name field description for examples of distinguished names. In our example, this is set to **cn=root**.

Bind password: Enter the password corresponding to the Bind DN in the **Bind password** field, if necessary.

Search Time Out: Modify the **Search Time Out** value if required. This timeout value is the maximum amount of time the LDAP server waits to send a response to the product client before aborting the request. The default is 120 seconds.

Reuse Connection: Disable the **Reuse Connection** field only if you use routers to spray requests to multiple LDAP servers, and if the routers do not support affinity. Leave this field enabled for all other situations.

Ignore Case: Enable the **Ignore Case** flag. When this is enabled, the authorization check is case insensitive. Normally, an authorization check involves checking the complete DN of a user, which is unique in the LDAP server and is case sensitive.

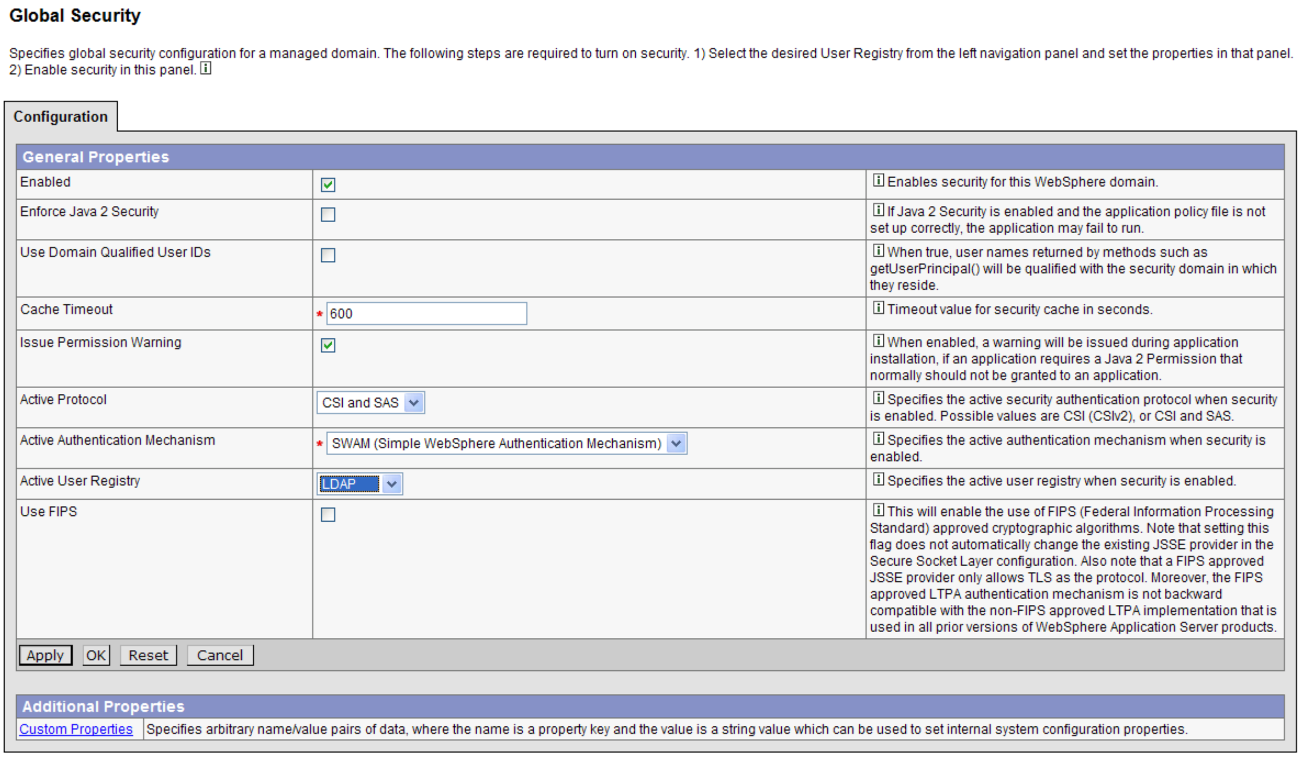
Note: When using either the IBM Directory Server or the iPlanet Directory Server LDAP servers, this flag needs enabling because the group information obtained from the LDAP servers is not consistent in case. This inconsistency only affects the authorization check.

SSL Configuration: If SSL is enabled, select the appropriate SSL alias configuration from the list in the **SSL configuration** field. We will do this later.

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

____ 5. Once finished with the LDAP configuration, save the settings to make it available for WebSphere.

____ 6. The validation of the user, password, and the setup does not take place in LDAP panel. Validation is only done when you click **OK** or **Apply** in the **Global Security** panel.



Global Security

Specifies global security configuration for a managed domain. The following steps are required to turn on security. 1) Select the desired User Registry from the left navigation panel and set the properties in that panel. 2) Enable security in this panel. ⓘ

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	LDAP	ⓘ 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 with the non-FIPS approved LTPA implementation that is used in all prior versions of WebSphere Application Server products.

Additional Properties

Custom Properties	Specifies arbitrary name/value pairs of data, where the name is a property key and the value is a string value which can be used to set internal system configuration properties.

__ a. Click **Security -> Global Security**. Select the **Enabled** check box.

__ b. Select **LDAP** as the active user registry.

__ c. As a final step, validate the user and password by clicking **OK** and **Save**.

If you receive an error message displayed in the Administrative Console when selecting **OK** or after saving global security settings:

```
"Validation failed for user userid. Please try again..."
```

Things to check:

- Any of the settings that enable WebSphere Application Server to communicate with LDAP might be invalid, such as the LDAP server's user ID, password, host, port, or LDAP filter. When you select **Apply** or **OK** on the Global Security panel, a validation routine connects to the registry just as it would during runtime when security is enabled. This is done in order to verify any configuration problems immediately, instead of waiting until the server restarts.

- Verify whether your LDAP server requires the Bind Distinguished Name (DN) to find the user in the LDAP directory. If the bind distinguished name is required, you must specify a DN instead of a short name. You can specify the bind distinguished name by clicking **Security > User Registries > LDAP** in the administrative console. For example, you might add cn=root.

- Sometimes the LDAP server might be down during configuration. Verifying your LDAP server is running. From the Control panel and in the Service panel, check that the IBM Directory Server is started.

Note: If you are enabling security for the first time, complete the remaining steps and go to the **Global Security** panel. Select **LDAP** as the Active User Registry. If security is already enabled, but information on this panel changes, go to the **Global Security** panel and click **OK** or **Apply** to validate your changes. If your changes are not validated, the server might not come up.

____ 7. You will need to restart the application server in order to make the changes effective.

Testing the connection

When the server starts, go to the Administrative Console; it should ask you for the user name and password for authentication. This is because Global Security is enabled. Give the user name as **wasadmin** (or **cn=wasadmin, o=ibm, c=us**) and password as *password*. If you are able to log in successfully, it means your configuration is working properly.

Things to check if there is a problem with the configuration

____ 1. Check that your user registry is running normally. For instance, if you have an LDAP user registry, check that the machine is available and that LDAP is running.

____ 2. Review your security related settings: user registry (LDAP, global security).

____ 3. Be sure that you are using the correct user name and password that goes with the user registry enabled in the Administrative Console. Verify that your username exists in the registry and that you are using the correct format for your ID.

Part 2: Configuring the secure LDAP (LDAPS) connection

Here, the assumption is that you have previously configured WebSphere to successfully authenticate users against the IBM LDAP Directory Server without using SSL for securing the WebSphere-to-LDAP connection. This section allows you to configure the LDAP connection for WebSphere Application Server V5 to use SSL by following the previous steps from **Configuring WebSphere to use the LDAP user registry.**

Creating the certificate for SSL

This section provides information for the keyring settings needed for the secure LDAP connection over SSL.

➢ ***Creating a self-signed certificate for the IBM Directory LDAP peer***

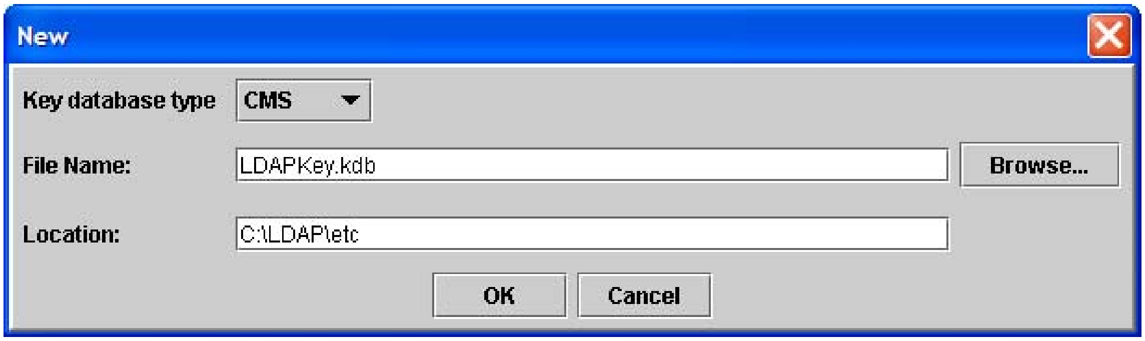
To create a self-signed certificate for the IBM Directory LDAP peer, follow the steps:

On the **LDAP machine,** where the LDAP server is installed, that has Windows system, the process is as follows.

____ 1. From the Start menu, select **Programs -> IBM HTTP Server 1.3.28 -> Start Key Management Utility**.

> **Note:** This is a different version of the ikeyman utility. It works with different types of key stores. Not all key management utilities are created equal. It is important that you use the IHS Key Management utility when dealing with keyfiles on the Web server side, and the WebSphere iKeyMan tool when dealing with keyfiles on the WebSphere application server side.

____ 2. From the menu bar, select **Key Database File -> New**



Key database type: CMS

File Name: LDAPKey.kdb

Location: C:\LDAP\etc

____ 3. Select **CMS key database file** from the Key database type drop-down menu.

____ 4. Enter a file name for the new key store, `LDAPKey.kdb` in this example

____ 5. Enter a path in the Location text area, `c:\LDAP\etc` in this example.

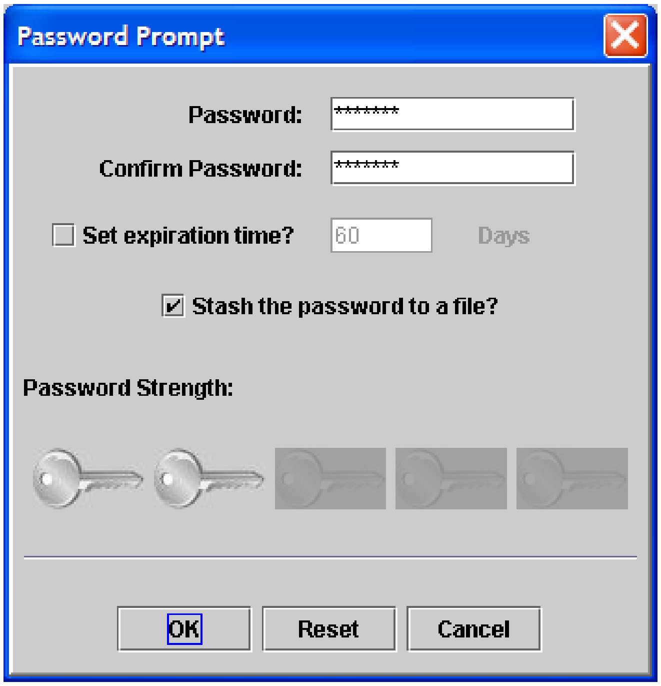
____ 6. Click **OK.**

____ 7. Enter a password in the Password text area and again in the Confirm Password area.

____ 8. Enable the *Stash the password to a file* option, which will allow WebSphere Application Server to make use of the password to gain access to the certificates contained in the key store.

____ 9. Click **OK.**

____ 10. Click **OK** to confirm that the password has been stashed.



Password Prompt

Password: ********

Confirm Password: ********

□ Set expiration time? 60 Days

☑ Stash the password to a file?

Password Strength:

____ **11.** Now a self-signed certificate can be generated. From the menu bar, select **Create -> New Self-Signed Certificate.**

____ 12. A window will appear requesting information in order to generate the certificate. Enter `LDAP SSL` as the Key Label. Ideally, spaces should not be used in the key label.

____ 13. Select **X509 V3** as the Version and **1024** as the Key Size.

____ 14. The first field of the Common Name is mandatory. The LDAP server name might be entered as the Common Name, for example: `supertiger.austin.ibm.com`. While Organization Unit, Locality and State/Province are optional fields, it is recommended that appropriate values be entered; for example: IBM, Austin, TX.

____ 15. Select the appropriate Country, in our case: **US**.

____ 16. Enter 365 as the Validity Period.

____ **17.** Click **OK**.

____ 18. The new self-signed certificate should be added to the Personal Certificates list.

____ **19.** It is necessary to extract this certificate so it can be added to the client's trust file later. Click **Extract Certificate** at the lower hand right corner**.**

____ 20. Select **Base64-encoded ASCII data** as the Data type.

____ 21. Enter `IBMDirectoryCert.arm` as the Certificate file name.

____ 22. Enter the directory that will hold the extracted certificate as the Location, in our case: `C:\LDAP\etc`.

____ 23. Click **OK.**

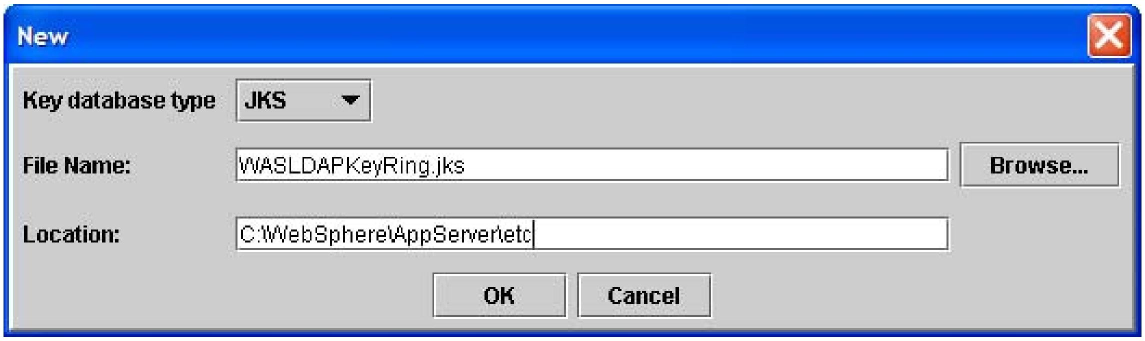
____ 24. From the menu bar, select **Key Database File -> Close**. This will close the current key store.

➢ ***Creating a keystore for the WebSphere server***

To create a key database for the WebSphere LDAP SSL peer, follow the steps:

On the WebSphere server machine, launch the ikeyman tool.

____ 1. Launch the ikeyman tool. It may be started from the command line in the bin directory as **ikeyman.bat** (on Windows platforms) or **ikeyman.sh** (on UNIX platforms).



Key database type: JKS

File Name: WASLDAPKeyRing.jks

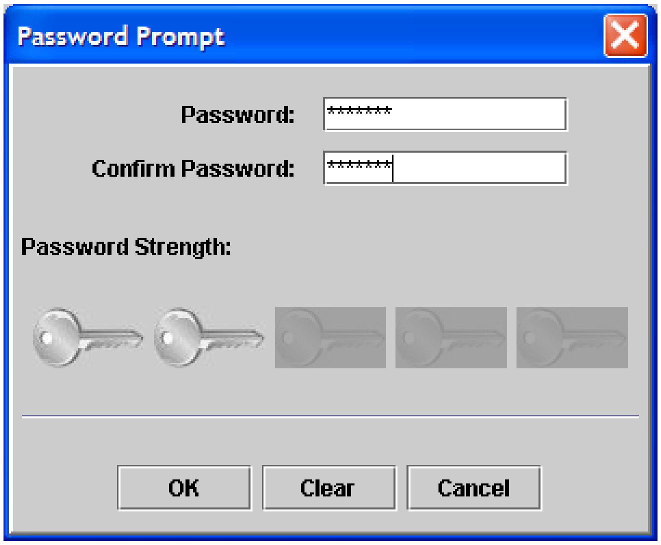
Location: C:\WebSphere\AppServer\etc

____ 2. From the menu bar, select **Key Database File -> New**.

____ 3. Ensure that the Key database type is set to JKS. Enter `WASLDAPKeyRing.jks` as the file name

____ 4. Enter the directory that will hold the key file as the location, in this case: `c:\Websphere\AppServer\etc`.

____ 5. 6. Click **OK.**



Password: *******

Confirm Password: *******

____ 6. A password prompt will appear. Enter a password and repeat to confirm. This password will be required to read from or write to this file in the future, so do not forget it. The password strength is determined by the variety of the characters used in the password.

____ 7. Click **OK**.

____ **8.** From the menu bar, select **Key Database File -> Close.** This will close the current key store.

Importing the certificate into the WebSphere server keystore

____ 1. In order to import the certificate into the keystore, you will have to copy over the certificate and the extracted .arm file to the WebSphere machine. Copy LDAP certificate file created previously on the LDAP machine `C:\LDAP\etc\IBMDirectoryCert.arm` to the WebSphere server machine. The source directory in our case is `C:\LDAP\etc` while the destination is: `C:\WebSphere\AppServer\etc`

____ 2. On the WebSphere machine, launch the IBM JKS capable ikeyman version that ships under the WebSphere bin directory.

____ 3. From the ikeyman menu, select **Key Database File -> Open** and select the previously created **WebSphereLDAPKeyring.jks** file.

____ 4. At the password prompt, enter the password for the keyfile, and then click **OK**.

____ 5. Select **Signer Certificates** in the drop-down list and click the **Add** button. This will allow you to import the public certificate previously extracted from the LDAP server keyfile.

```
Data type: Base64-encoded ASCII data


Certificate file name: IBMDirectoryCert.arm

Location: c:\WebSphere\Appserver\etc\
```

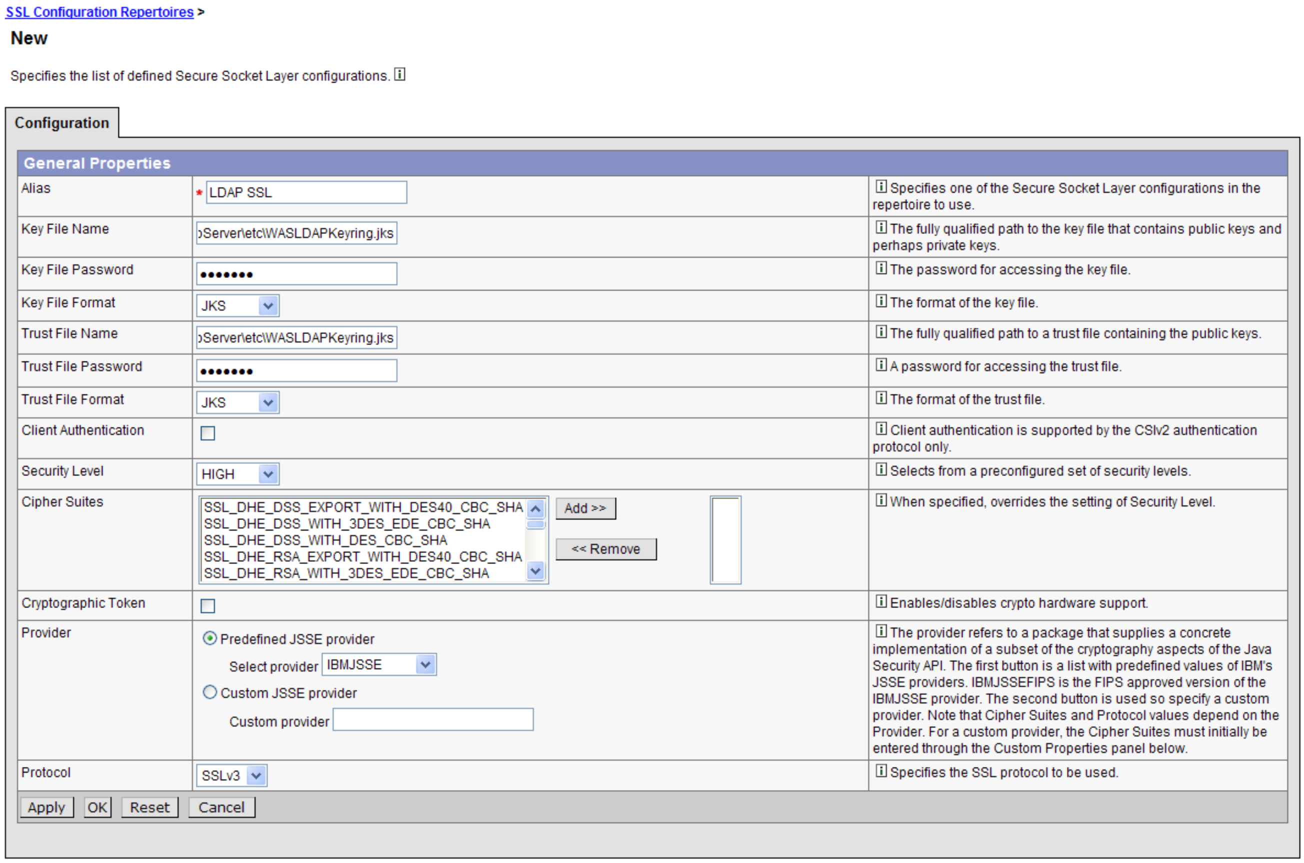
____ 6. Click **OK** when you are finished.

____ 7. You will be prompted for a label name by which the trusted signer public certificate will be known. Enter a label for the certificate: `WASserver_cert`.

____ 8. Close the key database and quit ikeyman when you are finished.

Configuring secure sockets layer (SSL) for the lightweight directory access protocol (LDAP) client

We need to configure the keyring for SSL we previously created in “Creating the certificate for SSL” using the Administrative Console for WebSphere Application Server V5.



SSL Configuration Repertoires >

New

Specifies the list of defined Secure Socket Layer configurations.

General Properties

Alias	* LDAP SSL	Specifies one of the Secure Socket Layer configurations in the repertoire to use.
Key File Name	)Server\etc\WASLDAPKeyring.jks	The fully qualified path to the key file that contains public keys and perhaps private keys.
Key File Password	•••••••	The password for accessing the key file.
Key File Format	JKS	The format of the key file.
Trust File Name	)Server\etc\WASLDAPKeyring.jks	The fully qualified path to a trust file containing the public keys.
Trust File Password	•••••••	A password for accessing the trust file.
Trust File Format	JKS	The format of the trust file.
Client Authentication	□	Client authentication is supported by the CSIv2 authentication protocol only.
Security Level	HIGH	Selects from a preconfigured set of security levels.
Cipher Suites	SSL_DHE_DSS_EXPORT_WITH_DES40_CBC_SHA SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA SSL_DHE_DSS_WITH_DES_CBC_SHA SSL_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA Add >> << Remove	When specified, overrides the setting of Security Level.
Cryptographic Token	□	Enables/disables crypto hardware support.
Provider	● Predefined JSSE provider Select provider IBMJSSE ○ Custom JSSE provider Custom provider	The provider refers to a package that supplies a concrete implementation of a subset of the cryptography aspects of the Java Security API. The first button is a list with predefined values of IBM's JSSE providers. IBMJSSEFIPS is the FIPS approved version of the IBMJSSE provider. The second button is used so specify a custom provider. Note that Cipher Suites and Protocol values depend on the Provider. For a custom provider, the Cipher Suites must initially be entered through the Custom Properties panel below.
Protocol	SSLv3	Specifies the SSL protocol to be used.

____ 1. From the Administrative Console, click **Security -> SSL**.

____ 2. Fill in the configuration values as follows:

- **Key File Name:** specify the fully qualified file name of the Java Key Store (JKS) key database previously created. In our example, this is set to `C:\WebSphere\AppServer\etc\WASLDAPKeyRing.jks`.

- **Key File Password:** state the password used to protect the Java Key Store (JKS) certificate key database above.

- **Key file format:** ensure that **JKS** is selected.

- **Trust file name:** potentially, you can set this to point to a second Java Key Store (JKS) used for holding trusted certificate keys. However, if you choose not to differentiate between personal keys and trusted keys, and opt to use a single key database for both tasks, this field should be set to the same value as the Key file name. In our example, this is set to `C:\WebSphere\AppServer\etc\WASLDAPKeyRing.jks`.

- **Trust file password:** state the password used to protect the Java Key Store (JKS) certificate key database above.

- **Trust file format:** ensure that **JKS** is selected.

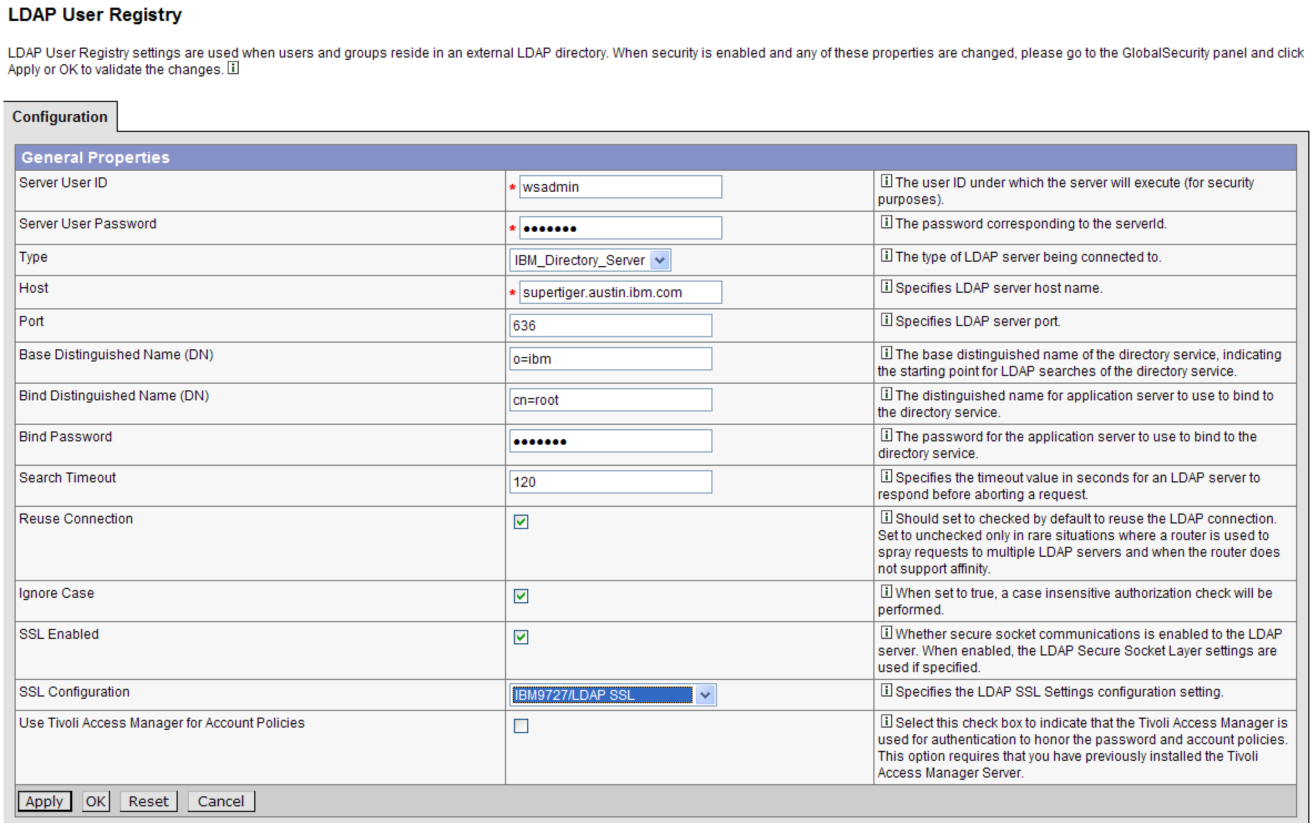
- **Security level:** setting this to High will ensure that the strongest SSL encryption algorithms are used for secure communication. The setting must be compatible with algorithms supported by the SSL peer.

____ 3. Click **OK** when you are done.

Note: If you are using the Default SSL settings to secure the LDAP connection, you have to restart the server before you can enable SSL for the LDAP User Registry for WebSphere Application Server V5.

Configuring LDAP User Registry to use SSL

Here, the assumption is again that you have previously configured WebSphere to successfully authenticate users against the IBM LDAP Directory Server without using SSL for securing the WebSphere-to-LDAP connection. The LDAP Distinguished Name (DN) and LDAP topology structure do not need to be modified in any way to support SSL.



LDAP User Registry

LDAP User Registry settings are used when users and groups reside in an external LDAP directory. When security is enabled and any of these properties are changed, please go to the GlobalSecurity panel and click Apply or OK to validate the changes.

Configuration

General Properties

Server User ID	* wsadmin	The user ID under which the server will execute (for security purposes).
Server User Password	* •••••••	The password corresponding to the serverId.
Type	IBM_Directory_Server	The type of LDAP server being connected to.
Host	* supertiger.austin.ibm.com	Specifies LDAP server host name.
Port	636	Specifies LDAP server port.
Base Distinguished Name (DN)	o=ibm	The base distinguished name of the directory service, indicating the starting point for LDAP searches of the directory service.
Bind Distinguished Name (DN)	cn=root	The distinguished name for application server to use to bind to the directory service.
Bind Password	•••••••	The password for the application server to use to bind to the directory service.
Search Timeout	120	Specifies the timeout value in seconds for an LDAP server to respond before aborting a request.
Reuse Connection	☑	Should set to checked by default to reuse the LDAP connection. Set to unchecked only in rare situations where a router is used to spray requests to multiple LDAP servers and when the router does not support affinity.
Ignore Case	☑	When set to true, a case insensitive authorization check will be performed.
SSL Enabled	☑	Whether secure socket communications is enabled to the LDAP server. When enabled, the LDAP Secure Socket Layer settings are used if specified.
SSL Configuration	IBM9727/LDAP SSL	Specifies the LDAP SSL Settings configuration setting.
Use Tivoli Access Manager for Account Policies	□	Select this check box to indicate that the Tivoli Access Manager is used for authentication to honor the password and account policies. This option requires that you have previously installed the Tivoli Access Manager Server.

____ 1. Launch the Administrative Console http://<serverName>:9090/admin. Click **Security -> User Registries -> LDAP**.

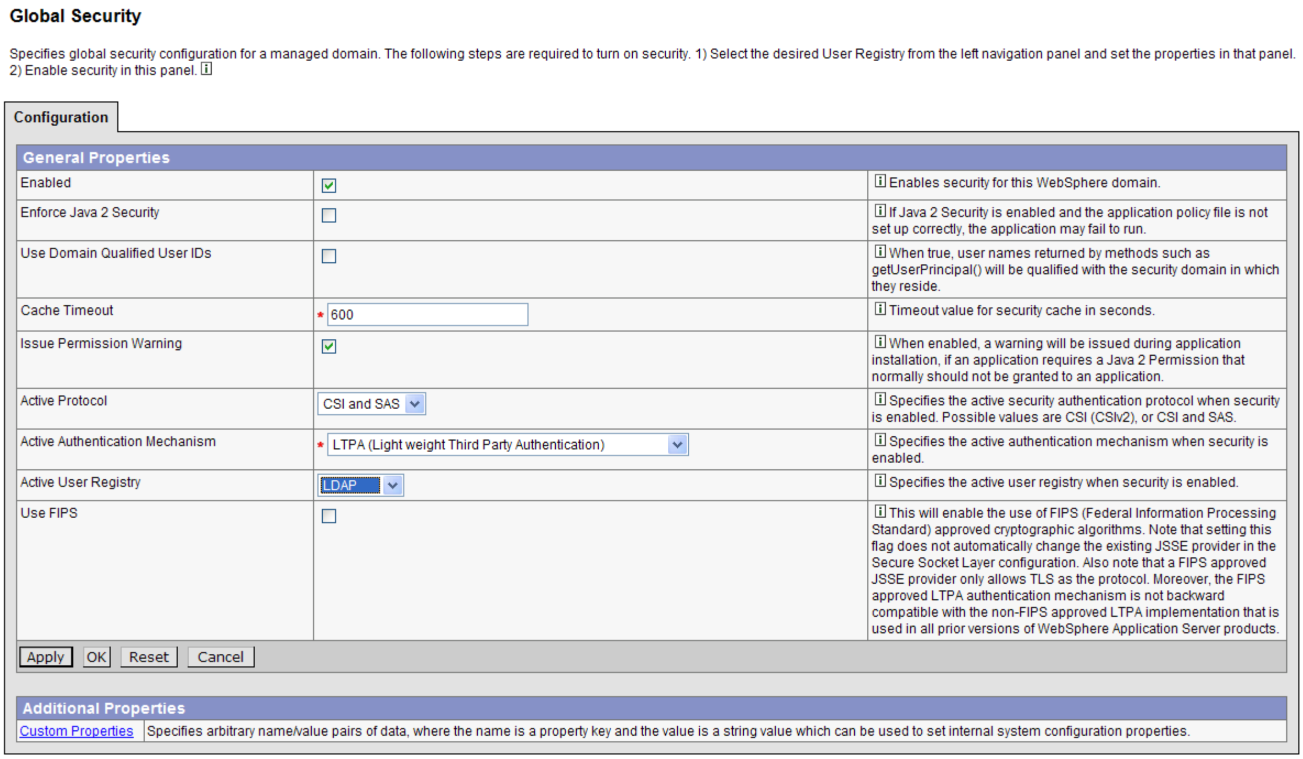
____ 2. In the right hand frame, fill out the Configuration fields as follows:

- **Port:** specify 636 which correspond to the TCP/IP port listening for SSL enabled LDAP queries on the remote IBM Directory Server LDAP Directory.
- **SSL Enabled:** select this check box to enable SSL.
- **SSL Configuration:** in the drop-down list, you should see the LDAP SSL entry we created previously; select it.

____ 3. Click **Apply**.

____ 4. Save the configuration.

____ 5. Next, we will verify that the Active User Registry in the **Global Security** panel is set to the appropriate registry which is supposed to be LDAP Click **Security > Global Security**. Make sure that the **Enabled** check box is checked.



Global Security

Specifies global security configuration for a managed domain. The following steps are required to turn on security. 1) Select the desired User Registry from the left navigation panel and set the properties in that panel. 2) Enable security in this panel. ⓘ

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	* LTPA (Light weight Third Party Authentication)	ⓘ Specifies the active authentication mechanism when security is enabled.
Active User Registry	LDAP	ⓘ 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 with the non-FIPS approved LTPA implementation that is used in all prior versions of WebSphere Application Server products.

Additional Properties

Custom Properties	Specifies arbitrary name/value pairs of data, where the name is a property key and the value is a string value which can be used to set internal system configuration properties.

____ 6. Make sure that **LDAP** is selected as the active user registry.

____ 7. As a final step, validate the user and password by clicking **OK** and **Save**.

Note: If you receive an error message when selecting OK:

-Checking your username and password again.

-Verifying your LDAP server is running. From the Control panel and in the Service panel, check that the IBM Directory Server is started.

____ 8. Re-start WebSphere so that changes can be included next time.

Note: For **WebSphere Network Deployment** environment: save, stop and start all the WebSphere Application Servers (cells, nodes and all the application servers). To avoid inconsistencies between the WebSphere Application Server processes, make sure any changes to the registry are done when all the processes are running. If any of the processes are down, force synchronization to make sure that process can come up later. If the server or servers start without any problems, the set up is correct.

➢ ***Testing the connection***

❖ *Test form login by bringing up the administrative console:*

`http://hostname.domain:9090/admin`. A form-based login page appears. Type in the administrative user ID and password that was used for configuring your user registry when configuring security. it should ask you for the user name and password for authentication. This is because Global Security is enabled. Give the user name and password as wasadmin (or cn=wasadmin,o=ibm,c=us) and password as password. If you are able to log in successfully, it means your configuration is working properly. In addition, when security is enabled in the product, this server ID and password are authenticated with the registry during the product startup. If authentication fails, the server does not start.

❖ *Test basic authentication with snoop by accessing the following URL:*

`https://<fully_qualified_host_name>:9443/snoop`. You are presented with a login challenge. Type in the valid user ID and password in your configured user registry. If the login panel fails to appear, there is a problem.

➢ ***Things to check***

Like WebSphere Application Server security, SSL can be difficult to configure correctly between components. Once it is working, there are a few things that can still interfere during run-time.

____ 1. Your certificate could expire. When this happens you will see SSL errors and the components talking to each other over SSL will no longer work correctly. To fix this, issue new certificates.

____ 2. A false indication of expired certificates could happen if the date or time changes on the machines involved in SSL communication. Check that the times and dates between systems are synchronized.

Security Problem Determination

➢ ***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:

```
SASRas        A JSAS0001I: Security configuration initialized.
SASRas        A JSAS0002I: Authentication protocol: CSIV2/IBM
SASRas        A JSAS0003I: Authentication mechanism: SWAM
SASRas        A JSAS0004I: Principal name: MYHOSTNAME/aServerID
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.
NameServerImp I NMSV0720I: Do Security service listener registration.
SecurityCompo A SECJ0242A: Security service is starting
UserRegistryI A SECJ0136I: Custom Registry:com.ibm.ws.security.registry.nt.
NTLocalDomainRegistryImpl has been initialized
SecurityCompo A SECJ0202A: Admin application initialized successfully
SecurityCompo A SECJ0203A: Naming application initialized successfully
SecurityCompo A SECJ0204A: Rolebased authorizer initialized successfully
SecurityCompo A SECJ0205A: Security Admin mBean registered successfully
SecurityCompo A SECJ0243A: Security service started successfully
SecurityCompo A SECJ0210A: Security enabled true
```

➢ *Errors after enabling LDAP*

The following is an example of messages from a server for which LDAP has been specified as the security mechanism, but the LDAP keys have not been properly configured:

```
SASRas        A JSAS0001I: Security configuration initialized.
SASRas        A JSAS0002I: Authentication protocol: CSIV2/IBM
SASRas        A JSAS0003I: Authentication mechanism: LTPA
SASRas        A JSAS0004I: Principal name: MYHOSTNAME/anID
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.
NameServerImp I NMSV0720I: Do Security service listener registration.
SecurityCompo A SECJ0242A: Security service is starting
UserRegistryI A SECJ0136I: Custom Registry:com.ibm.ws.security.registry.nt.
NTLocalDomainRegistryImpl has been initialized
SecurityServe E SECJ0237E: One or more vital LTPAServerObject configuration
attributes are null or not available. The attributes and values are password :
LTPA password does exist, expiration time 30, private key <null>, public key <null>,
and shared key <null>.
```

➢ *Errors after enabling Secure Sockets Layer, or Secure Sockets Layer-related error messages*

A problem with the SSL configuration might lead to the following message. You should ensure that the keystore location and keystore passwords are valid. Also, ensure the keystore has a valid personal certificate and that the personal certificate public key or CA root has been extracted on put into the truststore.

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

If you do not see a problem that resembles yours, or if the information provided does not solve your problem, contact **IBM support** (http://www-1.ibm.com/support/docview.wss?rs=180&context=SSEQTP&uid=swg21145599) for further assistance.

Reference:

- **WebSphere Application Server Information Center Version 5**

http://www-306.ibm.com/software/webservers/appserv/infocenter.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.