



Configuring LDAP Authentication in iWay Service Manager

LDAP authentication in iWay Service Manager (iSM) allows iSM to authenticate against LDAP and associate an LDAP iSM role to the user.

iSM includes a built-in role for an administrator that allows for complete management and control of iSM from the iSM Administration Console. Other roles may be added using the iSM Administration Console to limit access and management of iSM.

To implement LDAP authentication for the iSM Administration Console, each of these roles must be added to an LDAP/Active Directory configuration as Groups and then associated to users. Optionally, an LDAP attribute like *title*, can be associated to a role like *ism.admin*.

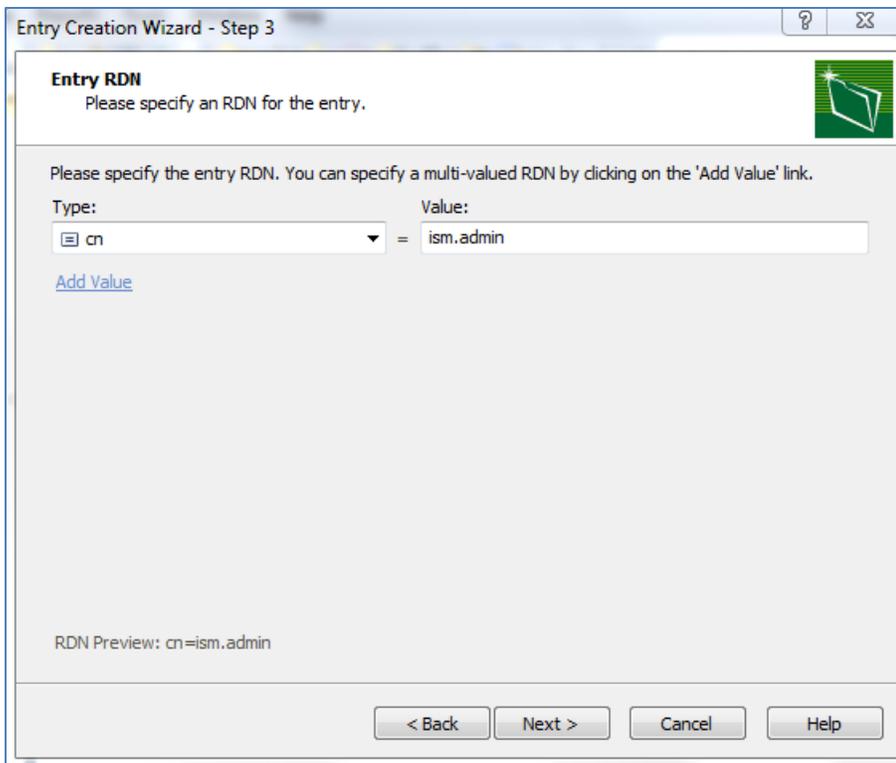
The built-in administrator role is *ism.admin*.

Additional roles must be defined in the iSM Administration Console and also in LDAP. This how-to describes the required configuration for LDAP and iSM.

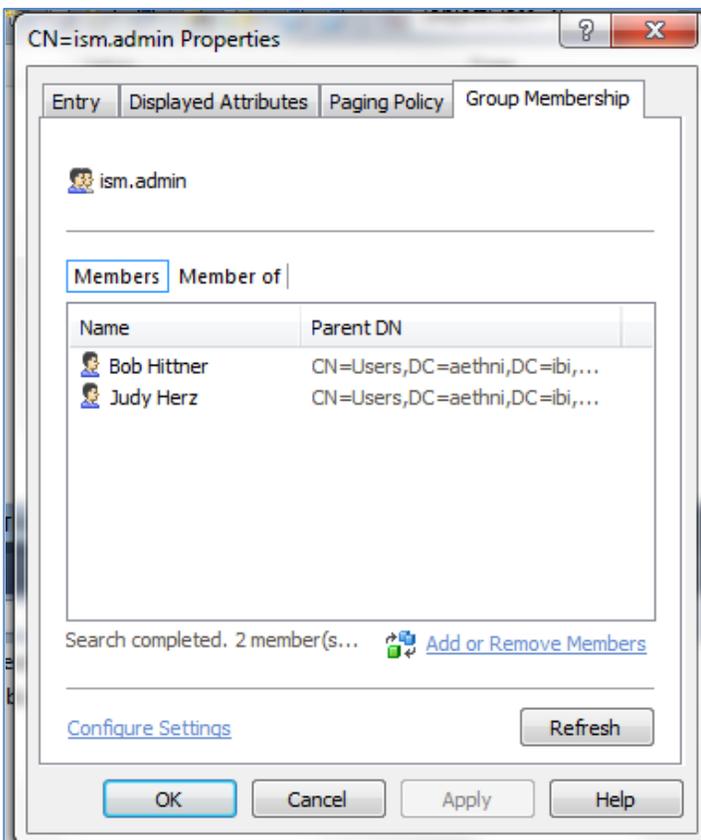
Configuring LDAP Groups

This section describes how to configure LDAP groups for iSM roles. The following steps describe how to create an LDAP group based on the iSM role and a Common Name (CN), which is the iSM role, then adding LDAP members to the group. For example, in the LDAP group for the built-in iSM administrator, *ism.admin* will have *CN=ism.admin*.

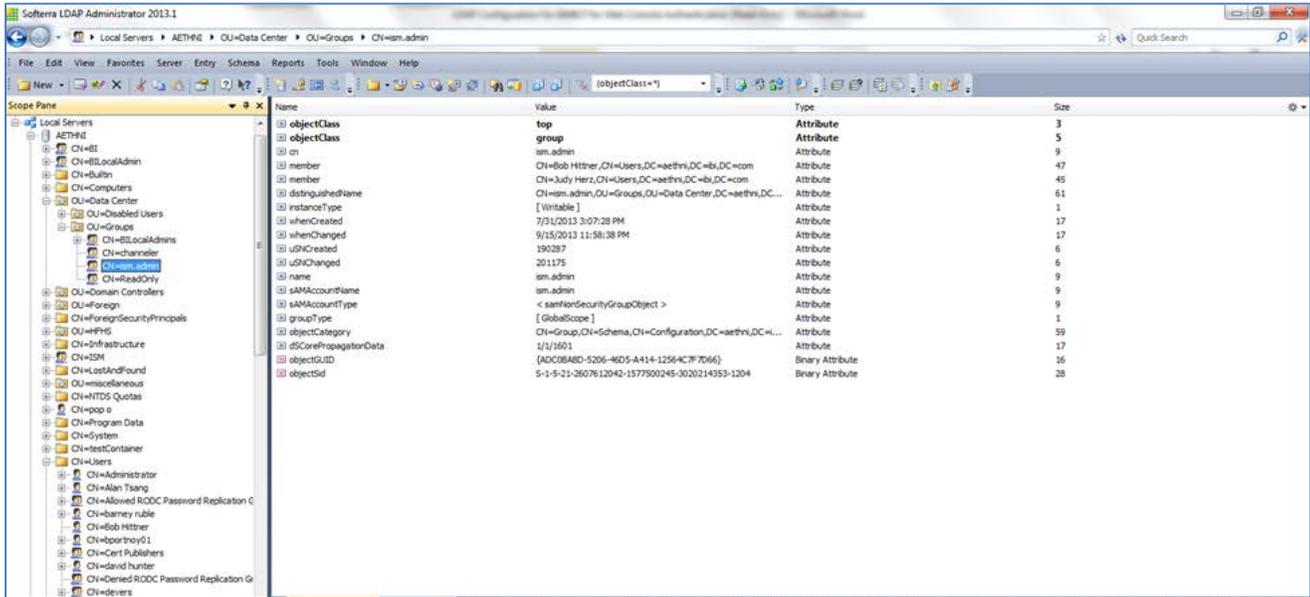
1. Create a new LDAP Group for *ism.admin* and then set *cn=ism.admin*, as shown in the following image.



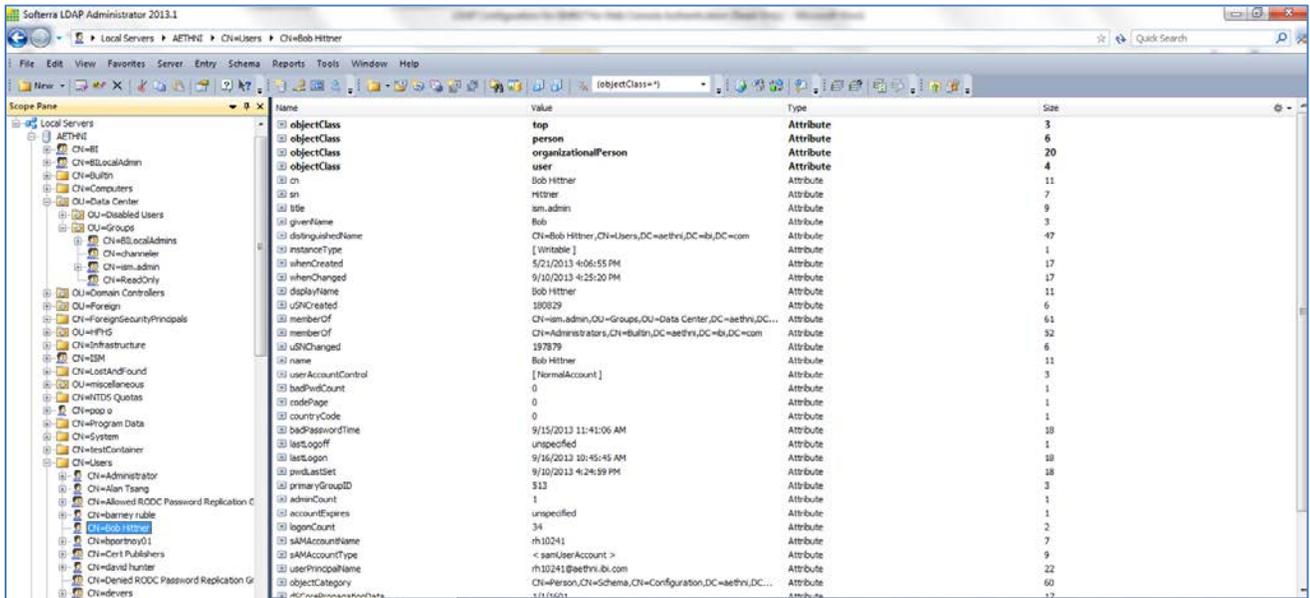
2. Add LDAP users as members to the LDAP group (*ism.admin*), as shown in the following image.



The LDAP group (*ism.admin*) and the associated members of this group are shown in the following image.



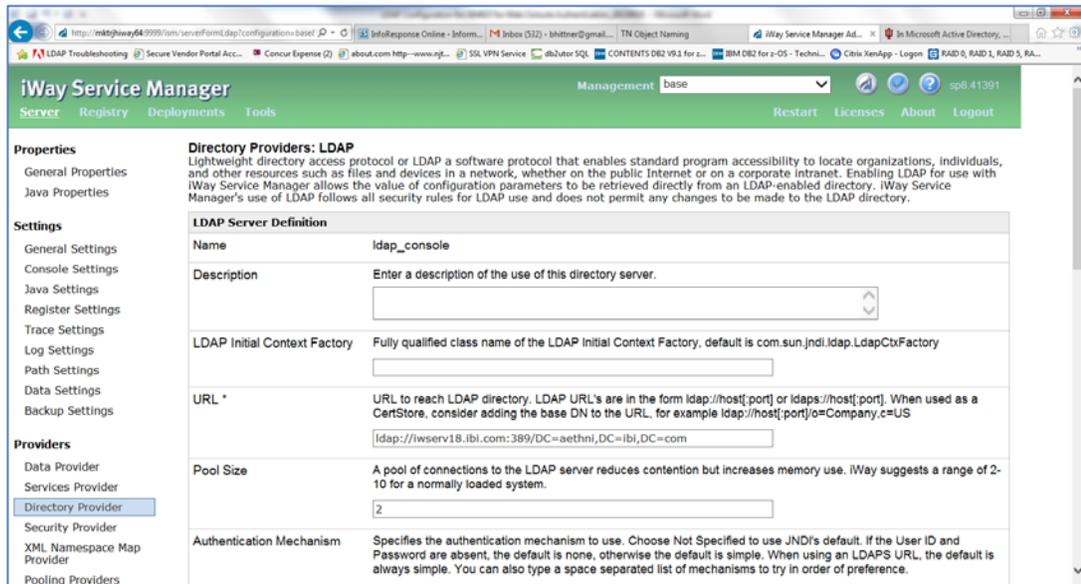
The following image shows LDAP user *Bob Hittner* as a member of the *ism.admin* LDAP group.



Configuring iWay Service Manager (iSM)

This section describes how to configure iSM to access and authenticate against LDAP. The following steps will create an iSM Directory Provider, an Authentication Realm, and define additional iSM roles.

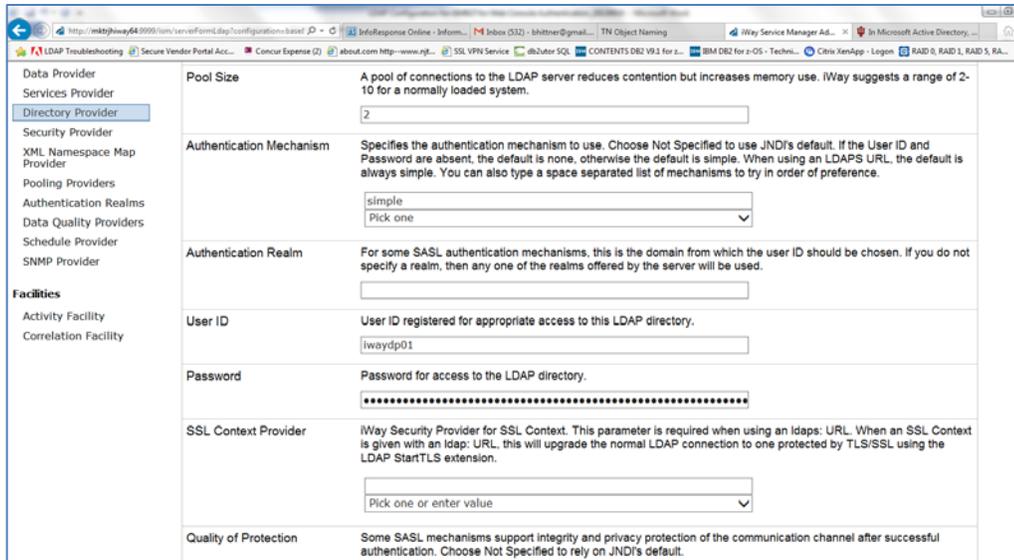
1. Create an iSM Directory Provider to access the LDAP directory.
2. Logon to the iSM Administration Console, click *Server*, and then *Directory Provider* in the left pane.
3. Enter the LDAP URL and Base DSN.



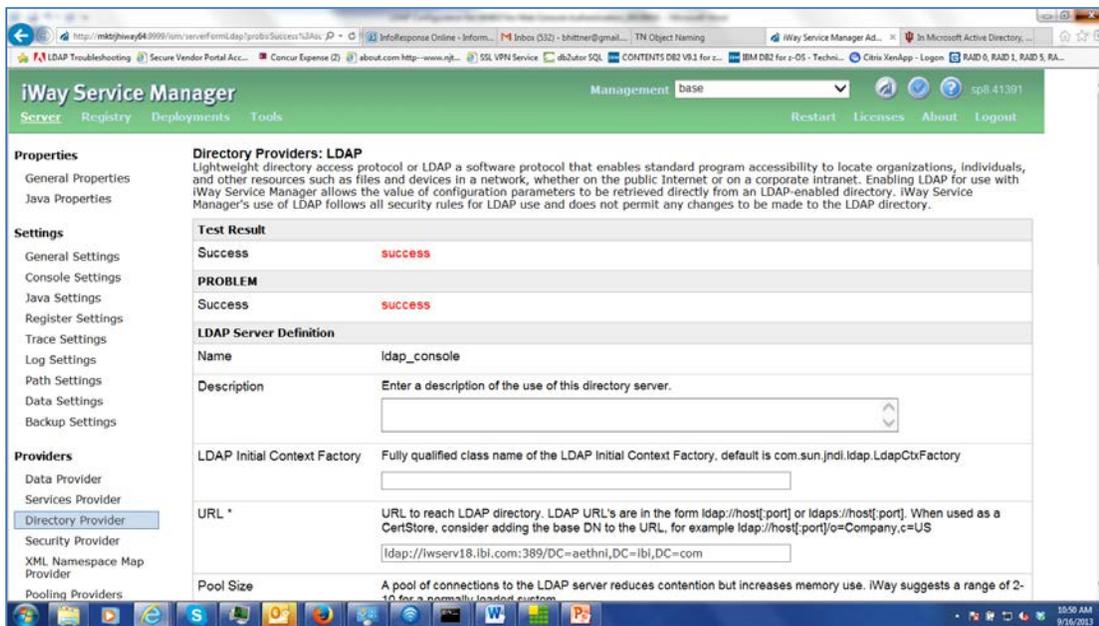
The screenshot shows the iWay Service Manager Administration Console. The left sidebar contains a navigation menu with sections: Properties (General Properties, Java Properties), Settings (General Settings, Console Settings, Java Settings, Register Settings, Trace Settings, Log Settings, Path Settings, Data Settings, Backup Settings), and Providers (Data Provider, Services Provider, Directory Provider, Security Provider, XML Namespace Map Provider, Pooling Providers). The 'Directory Provider' is selected. The main content area is titled 'Directory Providers: LDAP' and includes a description of LDAP. Below this is the 'LDAP Server Definition' form with the following fields:

LDAP Server Definition	
Name	ldap_console
Description	Enter a description of the use of this directory server. <input type="text"/>
LDAP Initial Context Factory	Fully qualified class name of the LDAP Initial Context Factory, default is com.sun.jndi.ldap.LdapCtxFactory <input type="text"/>
URL *	URL to reach LDAP directory. LDAP URL's are in the form ldap://host[:port] or ldaps://host[:port]. When used as a CertStore, consider adding the base DN to the URL, for example ldap://host[:port]o=Company.c=US <input type="text" value="ldap://wsserv18.ibi.com:389/DC=aethni,DC=ibi,DC=com"/>
Pool Size	A pool of connections to the LDAP server reduces contention but increases memory use. iWay suggests a range of 2-10 for a normally loaded system. <input type="text" value="2"/>
Authentication Mechanism	Specifies the authentication mechanism to use. Choose Not Specified to use JNDI's default. If the User ID and Password are absent, the default is none, otherwise the default is simple. When using an LDAPS URL, the default is always simple. You can also type a space separated list of mechanisms to try in order of preference.

4. Update the required fields for the LDAP Directory Provider.
5. Select *simple* from the Authentication Mechanism drop-down list. Enter the user ID and password for LDAP in the corresponding fields.



6. Click **Add** and then test the Directory Provider for successful connectivity.



7. Add the Authentication Realm by clicking on *Authentication Realm* under Providers in the left pane.

8. Click **New**.

- Select *ldaprealm* from the Realm Type drop-down list, enter a name in the Name field, and then select the configured directory provider for LDAP in the LDAP Provider field.

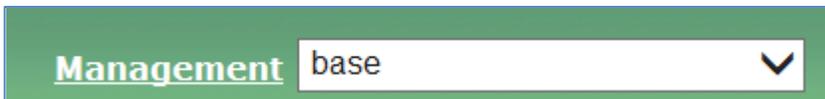
- Enter the user-based LDAP information by selecting *true* from the Search User Subtree drop-down list, and then entering *sAMAccountName={0}* in the User Search Filter field.

User Base Context	The base of the subtree containing users. Each user that can be authenticated must be represented by an individual entry that corresponds to an element in this DirContext. If not specified, the top level element in the directory context will be used.
User Pattern	A pattern for the distinguished name (DN) of the user's directory entry. Use {0} to substitute the username. For example, (cn={0}). LDAP OR syntax is also supported ((cn={0})(cn={0},o=myorg)). You can use this property instead of User Search Filter, Search User Subtree and User Base Context when the distinguished name contains the username and is otherwise the same for all users.
Search User Subtree	The search scope. Set to true if you wish to search the entire subtree rooted at the User Base Context entry. The default value of false requests a single-level search including only the top level.
User Search Filter	The LDAP filter expression to use when searching for a user's directory entry, with {0} marking where the actual username should be inserted. Use this property (along with the Search User Subtree property) instead of User Pattern to search the directory for the user's entry.
User Password Attribute	Name of the attribute in the user's entry containing the user's password. If you specify this value, this realm will retrieve the corresponding attribute for comparison to the value specified by the user being authenticated. If you do not specify this value, this realm will attempt a simple bind to the directory using the DN of the user's entry and password specified by the user, with a successful bind being interpreted as an authenticated user.

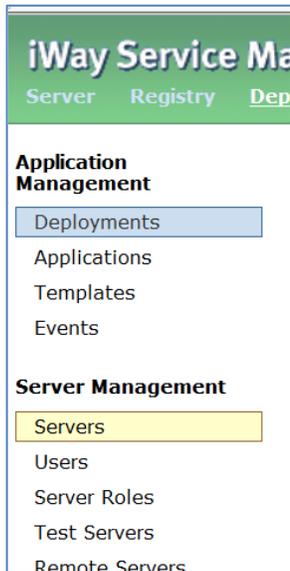
- Enter the role-based information by adding the Role Base Context, selecting *true* from the Search role Subtree drop-down list, specifying values for the Role Search Filter and Role Attribute parameters. Click *Add* when finished.

Role Base Context	The base directory entry for performing role searches. If not specified, the top level element in the directory context will be used. <input type="text" value="OU=Groups,OU=Data Center"/>
Search role Subtree	Set to true if you want to search the entire subtree of the element specified by the Role Base Context for role entries associated with the user. The default value of false causes only the top level to be searched. <input type="text" value="true"/> <input type="button" value="Pick one"/>
Role Search Filter	The LDAP filter expression used for performing role searches. Use {0} to substitute the distinguished name (DN) of the user, and/or {1} to substitute the username. If not specified a role search does not take place and roles are taken only from the attribute in the user's entry specified by the User Role Attribute. <input type="text" value="member={0}"/>
Role Attribute	The name of the attribute that contains role names in the directory entries found by a role search. In addition you can use the User Role Attribute property to specify the name of an attribute, in the user's entry, containing additional role names. If Role Attribute is not specified a role search does not take place, and roles are taken only from the user's entry. <input type="text" value="cn"/>
User Role Attribute	The name of an attribute in the user's directory entry containing zero or more values for the names of roles assigned to this user. In addition you can use the Role Attribute property to specify the name of an attribute to be retrieved from individual role entries found by searching the directory. If User Role Attribute is not specified all the roles for a user derive from the role search. <input type="text" value="cn"/>

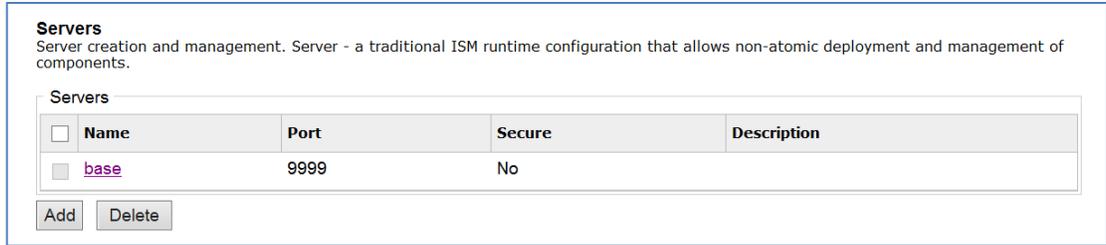
12. Click *Management*.



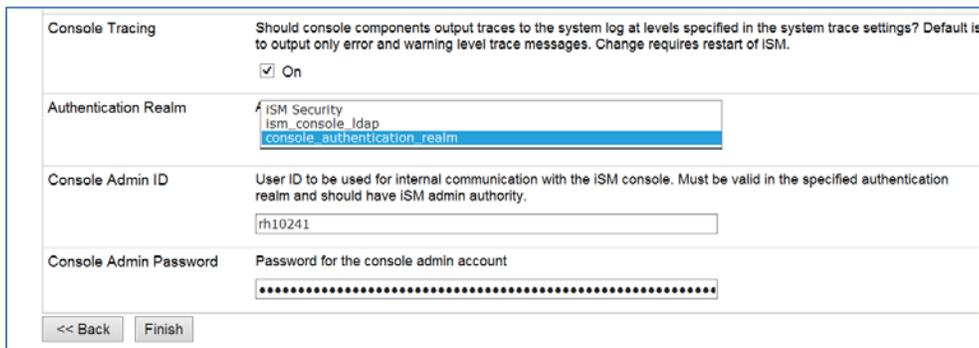
13. Click *Servers*.



14. Click the configuration name that will be using the LDAP authentication (for example, *base*).



15. Under Console Attributes, update the Authentication Realm parameter to use the Authentication Realm that you configured earlier.
16. Enter the LDAP user ID and password that was associated to the LDAP group (*ism.admin*). Optionally, enable the Console Tracing option for debugging LDAP authentication issues, as shown in the following image.



17. Restart iSM and logon to the iSM Administration Console.

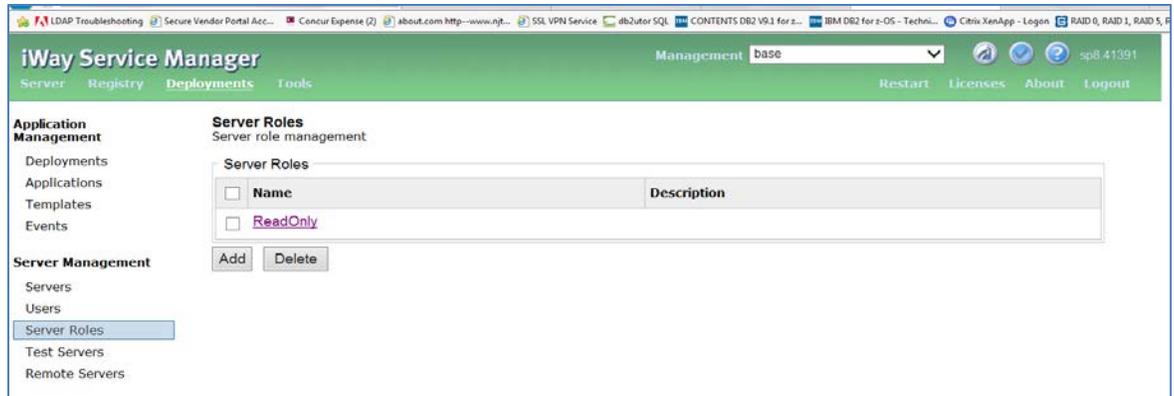
To debug any potential LDAP authentication issues, start iSM from a Windows Command Prompt using the following command:

```
c:\> iway61 base -u
```

Configuration of an LDAP connection and authentication for iSM is complete.

Adding Additional Server Roles in iWay Service Manager (iSM)

1. To add additional iSM roles, click *Management* and then click *Server Roles* in the left pane.
2. Click *Add*, provide a name for the role, and assign permissions.



3. Click *Add*.
4. In the Server Roles section, enter *ReadWrite* in the Name field, and then select the allowable permissions, as shown in the following image.

The screenshot shows the 'Server Roles' configuration form. The 'Role' section has 'Name *' set to 'ReadWrite'. The 'General iSM Permissions' section includes the following checked options: 'Can Stop Configurations', 'Can Restart Configurations', 'Can Access Server Settings', and 'Can Access Channels'. The 'Configuration Specific Permissions' section has 'Read' and 'Write' checked for the 'base' role.

5. Perform the steps in *Configuring LDAP Groups* to add the LDAP group for the *ReadWrite* role.
6. Restart iSM and verify the new role.

The name of the iSM role must match the name of the LDAP group. For example:

- iSM role = ReadWrite
- LDAP group = ReadWrite

They are mapped by using the same name.

Troubleshooting LDAP Authentication Using the iWay Service Manager Configuration Log (Tracing)

1. Enable Console Tracing. For more information, see step 16 in *Configuring iWay Service Manager (iSM)*.
2. Click *Server*, navigate to *Trace Settings*, and then enable *Deep and Debug*.
3. Log on to the iSM Administration Console (configuration).
4. Examine the log file from the iSM log directory (*iway_home\config\base\log*) and look for the most recent log file. For example:

DEEP (console) LDAP Realm, entry found for csswxz with dn
CN=CSSWXZ,CN=Users,DC=eda,DC=csseda,DC=com

DEEP (console) LDAP User role name cn search

DEEP (console) LDAP Realm, retrieving values for attribute cn

DEBUG (console) LDAP Realm, csswxz authenticated successfully

DEEP (console) LDAP Realm, getRoles(CN=CSSWXZ,CN=Users,DC=eda,DC=csseda,DC=com)

DEEP (console) LDAP Realm, retrieving values for attribute cn

DEEP (console) LDAP Realm, Returning roles: CSSWXZism.admin

DEEP (console) LDAP Realm, Closing directory contex

The *ism.admin* role may seem joined to another role (CSSWXZism.admin), which is the expected behavior. It is important to ensure that the *ism.admin* role (or any other role you assign) exists within the *Returning roles* entry in the log file.