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*.

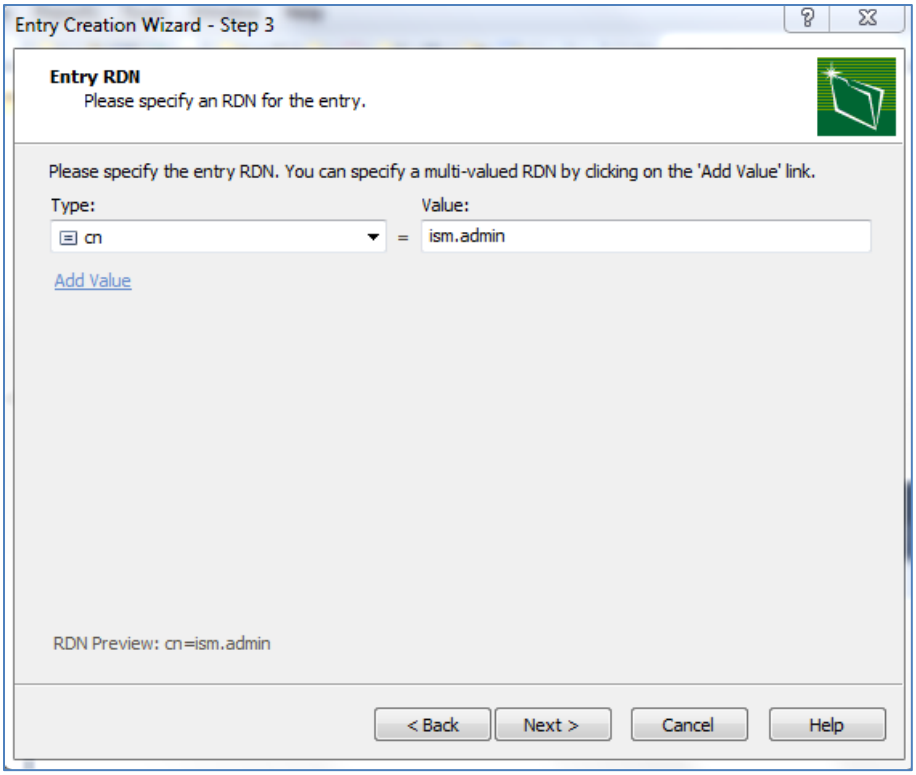
The built-in administrator role is *ism.admin*.

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.

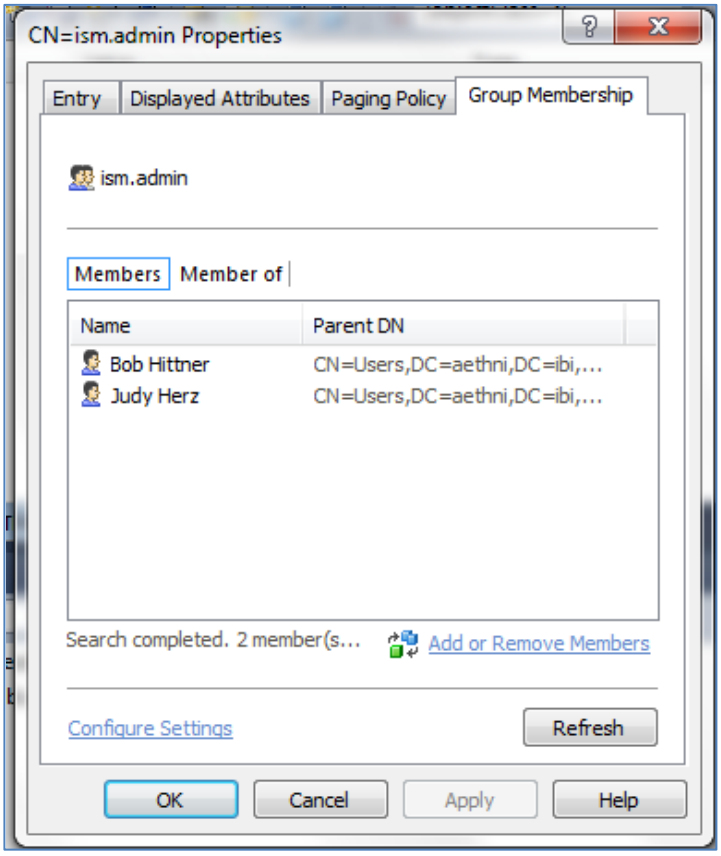
Configuring LDAP Groups

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*.

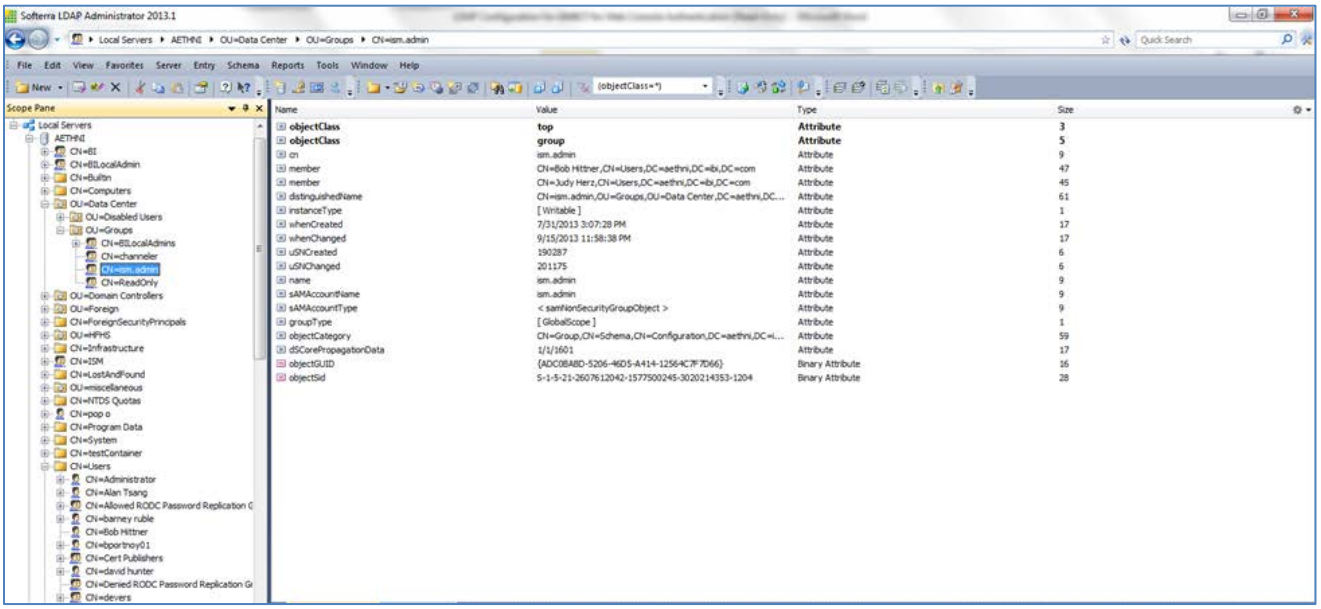
1. Create a new LDAP Group for *ism.admin* and then set *cn=ism.admin*, as shown in the following image.



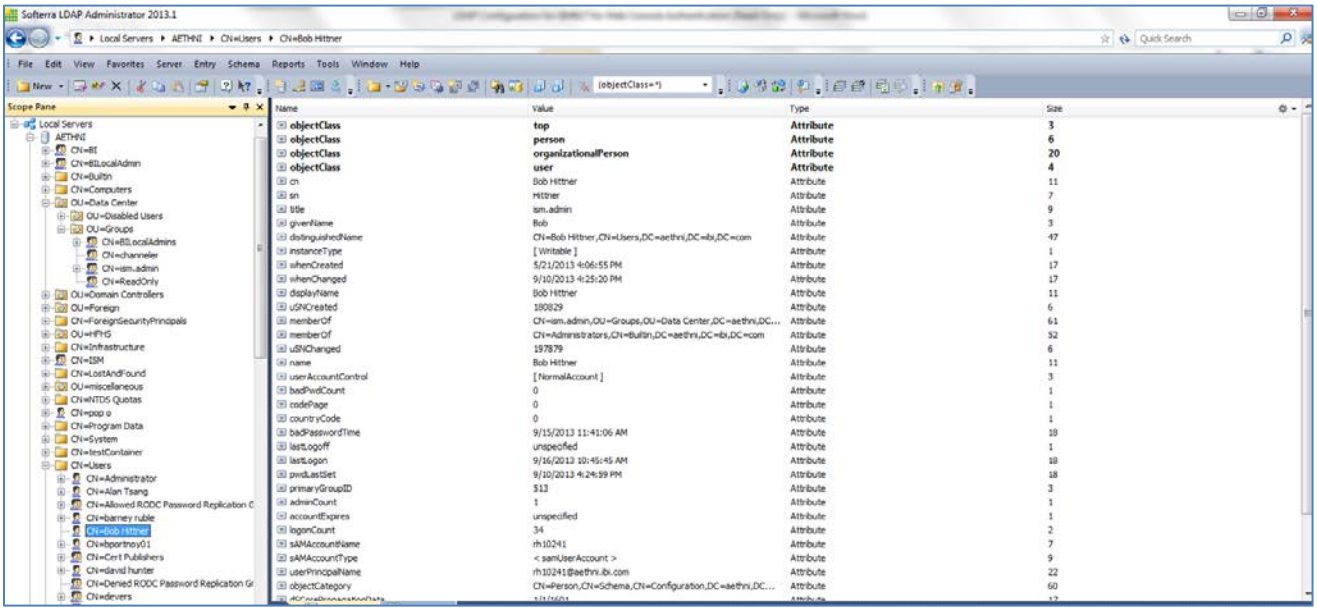
2. Add LDAP users as members to the LDAP group (*ism.admin*), as shown in the following image.



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.



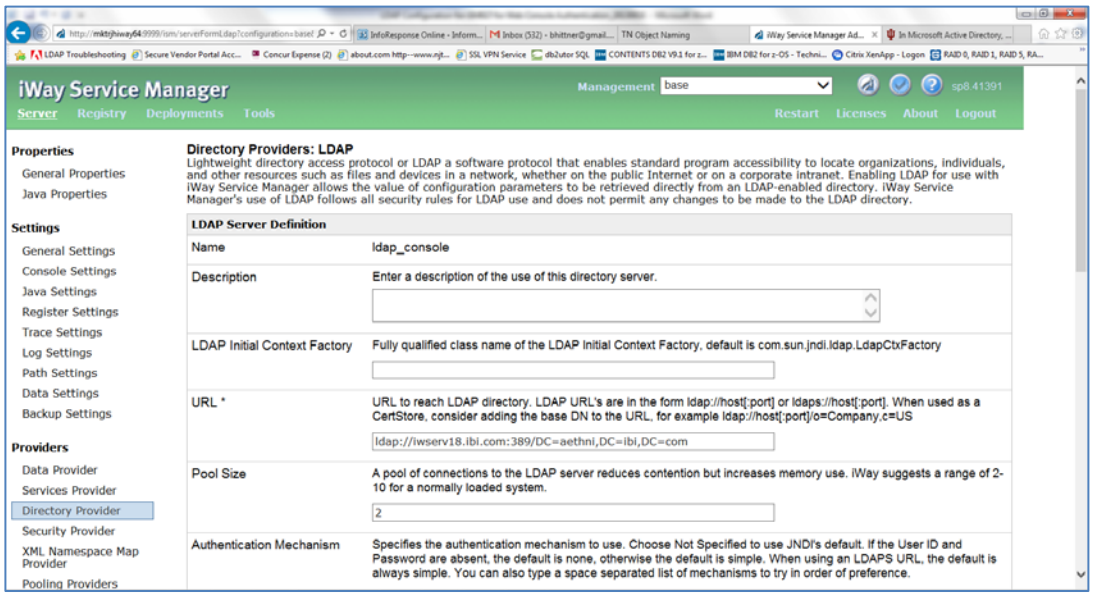
Configuring iWay Service Manager (iSM)

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.

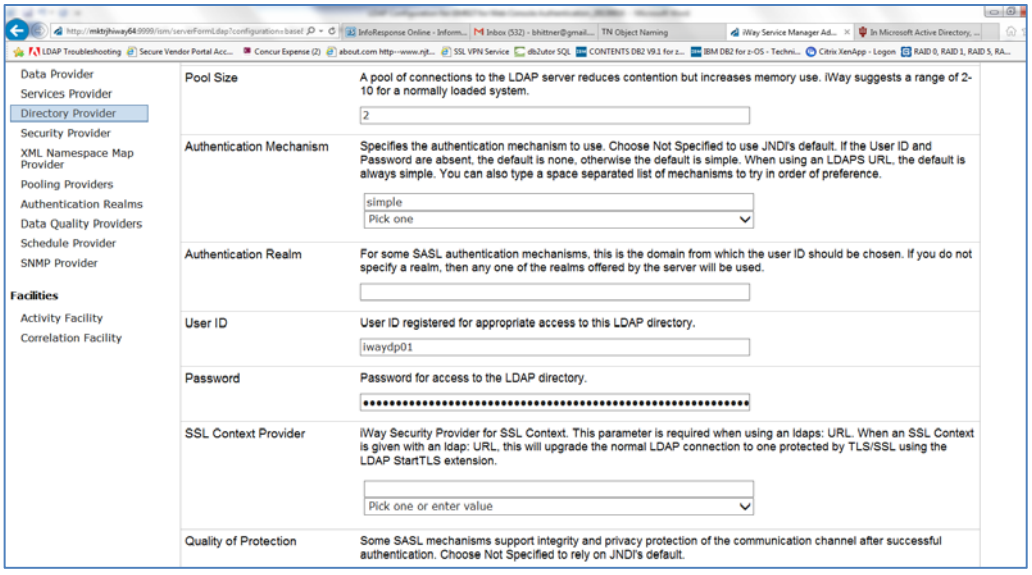
2. Logon to the iSM Administration Console, click *Server*, and then *Directory Provider* in the left pane.

3. Enter the LDAP URL and Base DSN.

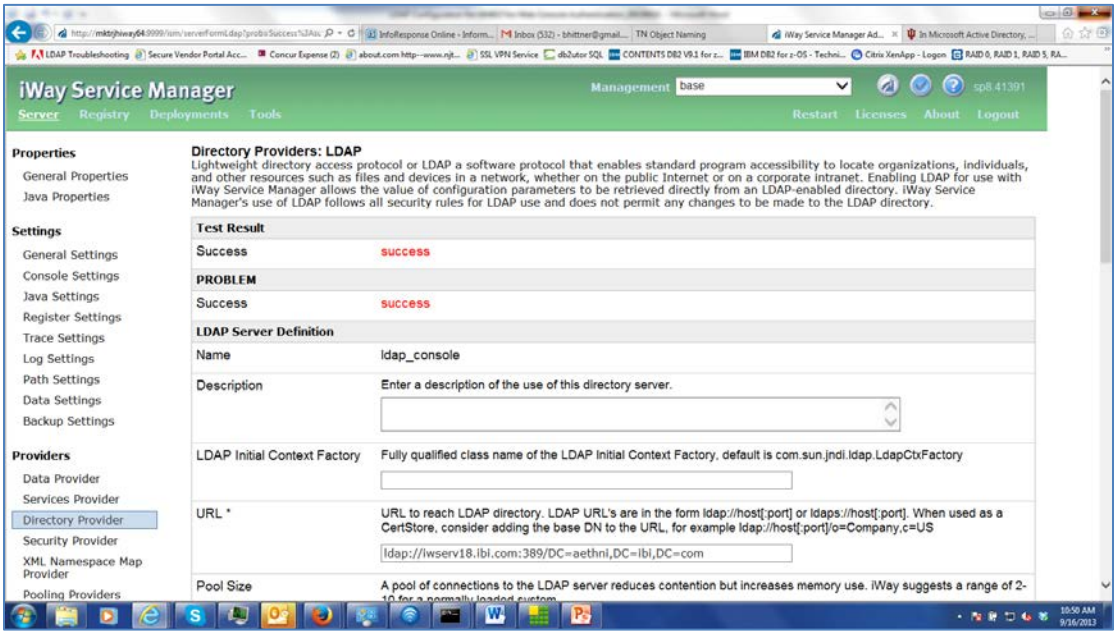


4. Update the required fields for the LDAP Directory Provider.

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



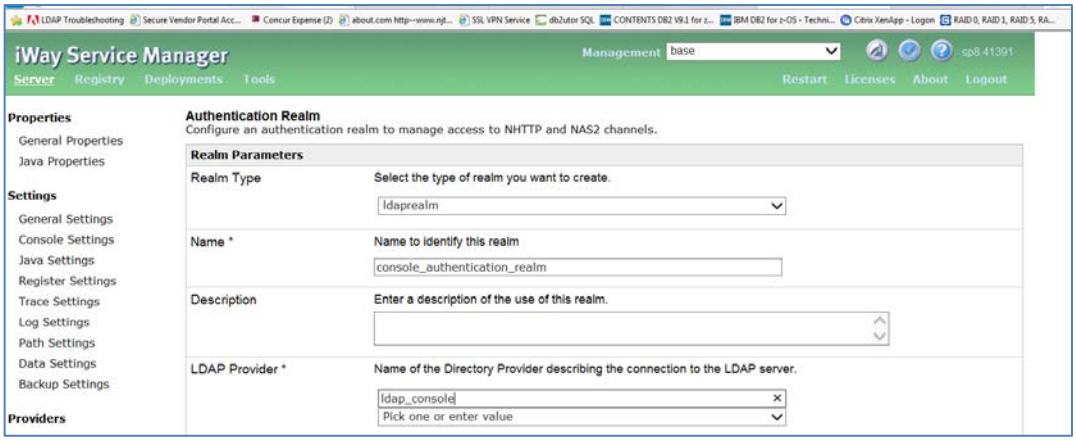
6. Click *Add* and then test the Directory Provider for successful connectivity.



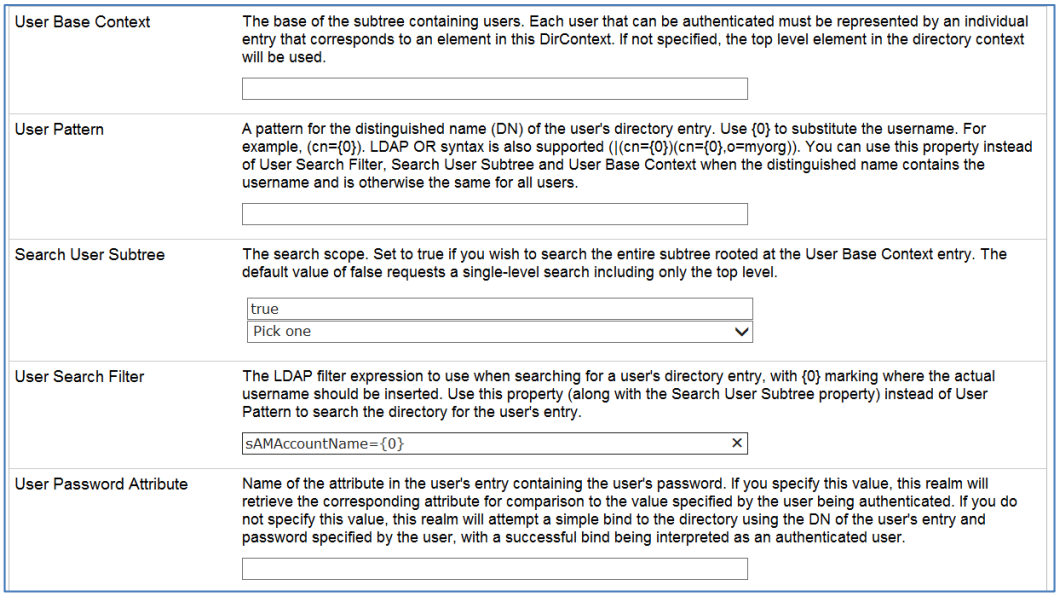
7. Add the Authentication Realm by clicking on *Authentication Realm* under Providers in the left pane.

8. Click *New*.

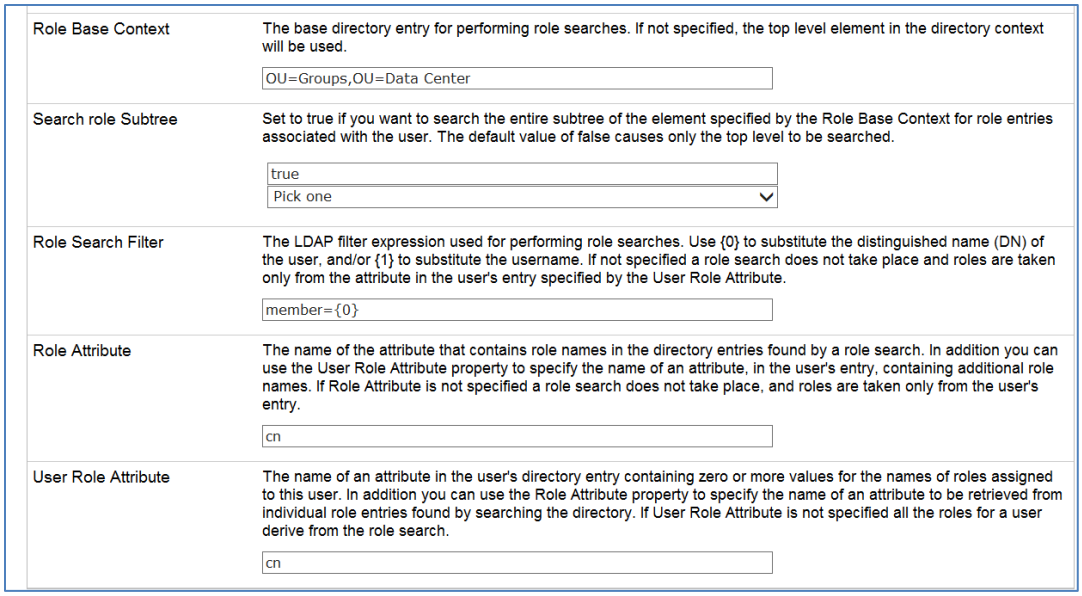
9. Select *ldaprealm* from the Realm Type drop-down list, enter a name in the Name field, and then select the configured directory provider for LDAP in the LDAP Provider field.



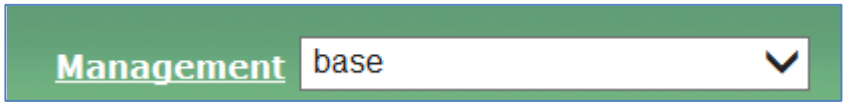
10. Enter the user-based LDAP information by selecting *true* from the Search User Subtree drop-down list, and then entering *sAMAccountName={0}* in the User Search Filter field.



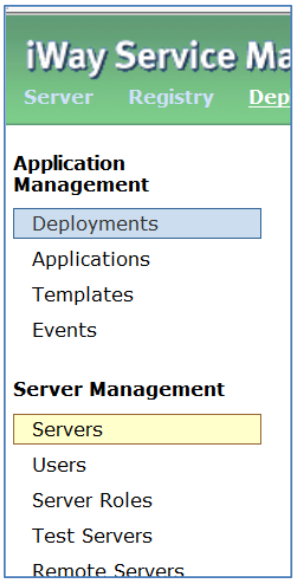
11. Enter the role-based information by adding the Role Base Context, selecting *true* from the Search role Subtree drop-down list, specifying values for the Role Search Filter and Role Attribute parameters. Click *Add* when finished.



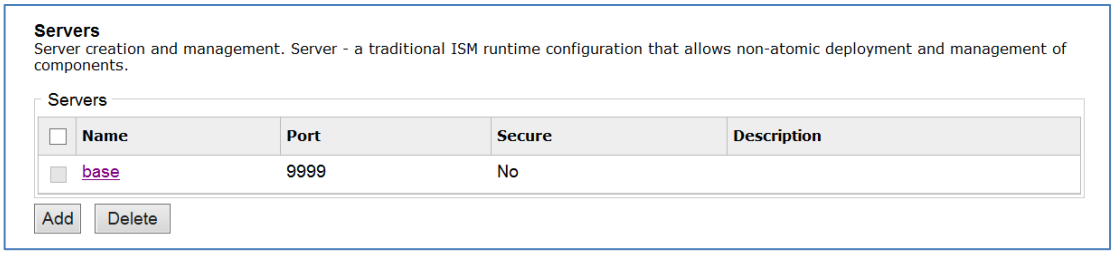
12. Click *Management*.



13. Click *Servers*.

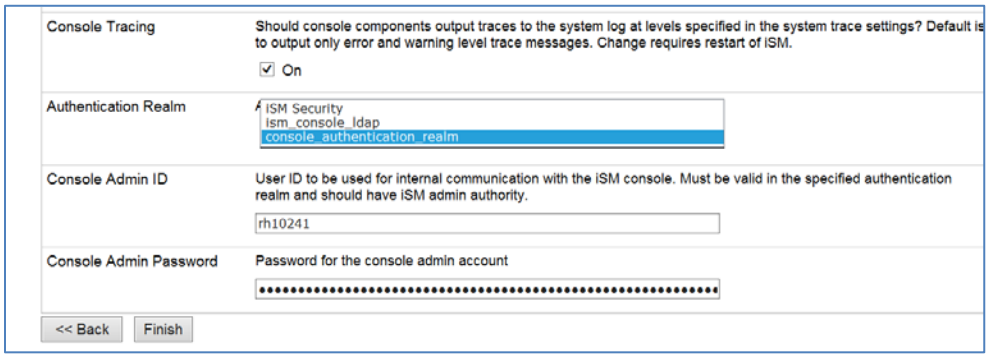


14. Click the configuration name that will be using the LDAP authentication (for example, *base*).



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:

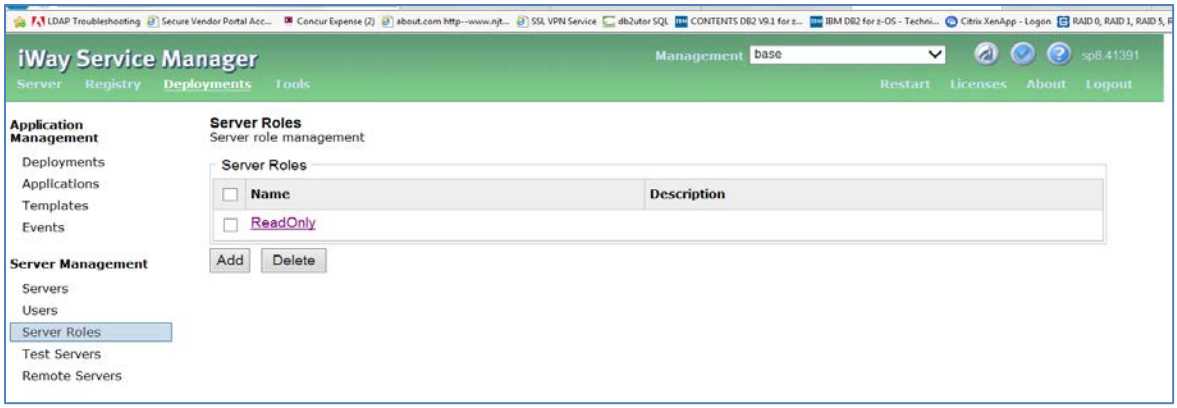
    ```
    c:\> iway61 base –u
    ```

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

Adding Additional Server Roles in iWay Service Manager (iSM)

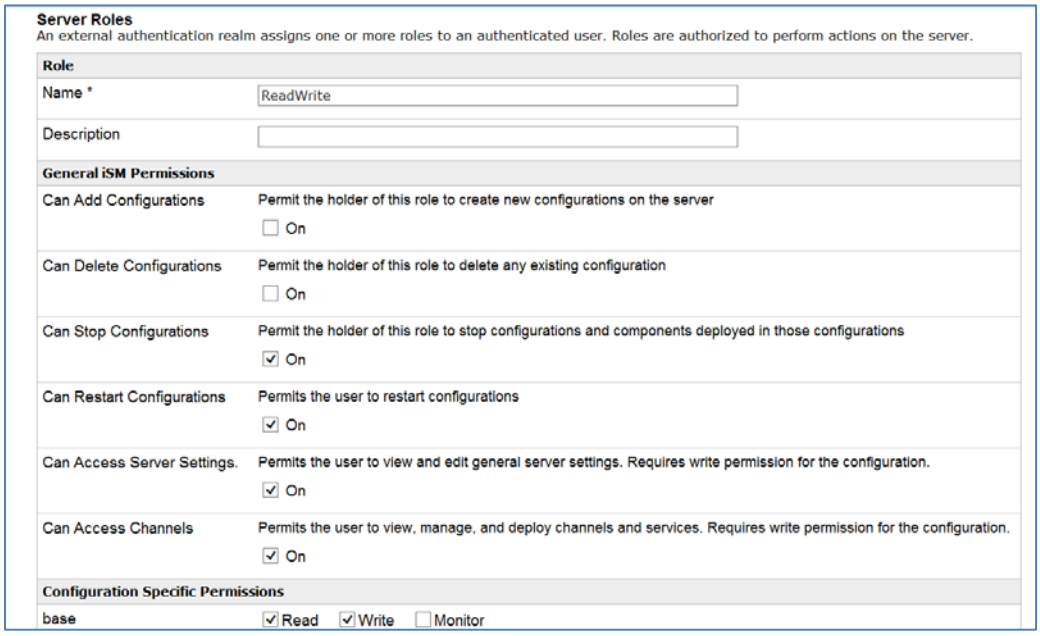
1. To add additional iSM roles, click *Management* and then click *Server Roles* in the left pane.

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.



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: CSSWXZ**ism.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.