

User Permissions

SharePath user permissions are based on roles. Three application-based roles are defined automatically every time a new application domain is created. Two of these roles, if assigned to a user, allow that user to manage or view the application. The third role, “revoke”, is used to provide for exceptions when a user has been assigned the role of MANAGE or VIEW for all applications. Assigning the user xxx_Revoke and CRM_Revoke, for example, will exclude xxx and CRM from the applications the user is allowed to view or manage. If the user has been assigned the All_Manage role, the user will be able to manage all applications except those for which a view role has been assigned (i.e. CRM_view) or a revoke role has been assigned. So a user assigned All_Manage, app1_revoke, app2_View and app3_View will be able to manage all applications except app1, app2 and app3 and will not be able to view app1 at all.

While the roles all_applications_VIEW and all_applications_MANAGE and the application-based Manage, View and Revoke roles are provided automatically by SharePath, the SharePath Administrator can create complex roles that include any combination of these automatically created roles. Complex roles can be assigned to members of a group sharing responsibilities for the same applications. Complex views are easy to create, easy to modify and can be easily assigned to additional users.

The following sections discuss:

- [Accessing the User Permissions Tabs](#)
- [Manual and Automatic Role Creation](#)
- [Accessing the User Permissions Tabs](#)

To access the *Users*, *Roles*, and *LDAP* tabs, a SharePath administrator can:

1. Click on *Settings*
2. Click on *User Permissions*

Manual and Automatic Role Creation

SharePath roles can be defined manually via the Roles tab, based on application name and allowed action (view, manage). When defining the SharePath role, select the LDAP role that should be associated with the SharePath role from the LDAP roles list, when relevant.

Since a set of simple application-based roles (view, manage and revoke) are created automatically each time a new application is established, manually defined roles are usually a combination of simple application-roles. By associating LDAP roles with the SharePath roles, external users will automatically gain the correct access to monitored application data.

- [SharePath Role Types](#)
- [Roles Tab](#)
- [Creating a new Role](#)
- [Role Properties](#)
- [Users tab](#)
- [Assigning Roles to Users](#)

- [SharePath LDAP Integration](#)
- [LDAP tab](#)

Accessing the User Permissions Tabs

To access the *Users*, *Roles*, and *LDAP* tabs, a SharePath administrator can:

3. Click on *Settings*
4. Click on *User Permissions*

Manual and Automatic Role Creation

SharePath roles can be defined manually via the Roles tab, based on application name and allowed action (view, manage). When defining the SharePath role, select the LDAP role that should be associated with the SharePath role from the LDAP roles list, when relevant.

Since a set of simple application-based roles (view, manage and revoke) are created automatically each time a new application is established, manually defined roles are usually a combination of simple application-roles. By associating LDAP roles with the SharePath roles, external users will automatically gain the correct access to monitored application data.

SharePath Role Types

The three SharePath Role Types are Administrator, Application Manager and Application Viewer.

Administrator

Administrator permissions enable full (read/write) access to all *Settings* tabs including Host Managers, Tier Types, Nodes, Parameters, SMPT, User Permissions, Alerts, Application Domains, Transformation Rules, Areas/Locations and System Health.

Application Manager (role)

Application Managers can manage their applications by:

- Managing Application SLA (See [Chapter 5: SLA Management](#))
- Managing Transaction SLA (See [Chapter 5: SLA Management](#))
- Determining *Transaction Description* in the Transaction Properties dialog
- Assigning transactions to the Application (only if application owner has SharePath Administrator privileges)
- Defining *Transaction Naming* rules for the application

Application Viewer (role)

Application Viewers can view monitored data for all or some monitored applications, according to their permissions as configured by the Administrator.

Roles Tab

The roles tab lists all the roles currently defined for SharePath, including Role Name, a free-text Description and the SharePath Applications to which the role applies. The free-text description is

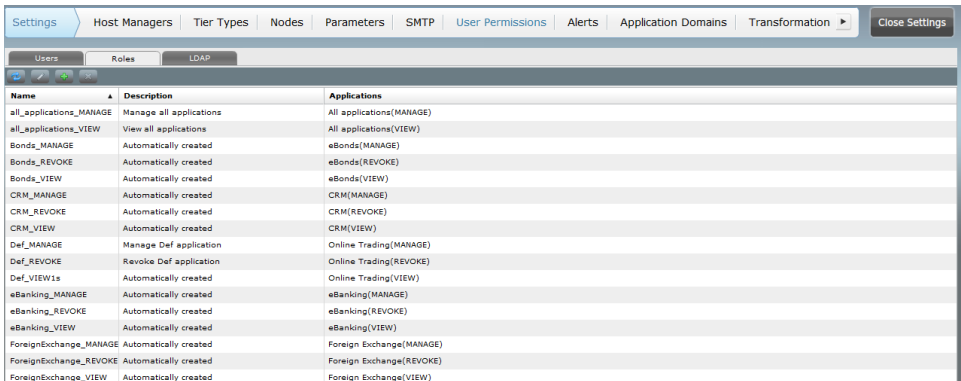
especially important because it is the field that is visible when adding roles to individual users via the *Users* tab..

The roles are defined in terms of application access (View, Manage and Revoke where Revoke is used only in cases that All, all_applications_MANAGE or all_applications_VIEW is one of the user's roles). The application-based roles View, Manage and Revoke are created automatically each time a new application domain is established. The SharePath administrator can access the Roles tab and use its toolbar buttons and the Role Properties dialog to add, modify and delete roles.

Roles, once created, can be assigned to any individual user via the *Users* tab and the *User Properties* dialog. The roles description text in the Roles Tab is forms the selectable text visible from the user tab when assigning a role to a user. This should be kept in mind when defining a new role. Meaningful text in the description field will help you recognize this role later.

Three roles are automatically created and available for every application. The SharePath Administrator can define additional complex roles that refer to more than one application.

Complex roles are convenient. Use complex roles to save time and to assign a combination of application permissions to a number of people without making errors and without the need for excessive checking. Complex roles can be updated after they have been assigned. They are helpful when assigning roles to a group of people who need the same permissions, such as members of a team.






Name	Description	Applications
all_applications_MANAGE	Manage all applications	All applications(MANAGE)
all_applications_VIEW	View all applications	All applications(VIEW)
Bonds_MANAGE	Automatically created	eBonds(MANAGE)
Bonds_REVOKE	Automatically created	eBonds(REVOKE)
Bonds_VIEW	Automatically created	eBonds(VIEW)
CRN_MANAGE	Automatically created	CRN(MANAGE)
CRN_REVOKE	Automatically created	CRN(REVOKE)
CRN_VIEW	Automatically created	CRN(VIEW)
Def_MANAGE	Manage Def application	Online Trading(MANAGE)
Def_REVOKE	Revoke Def application	Online Trading(REVOKE)
Def_VIEW1s	Automatically created	Online Trading(VIEW)
eBanking_MANAGE	Automatically created	eBanking(MANAGE)
eBanking_REVOKE	Automatically created	eBanking(REVOKE)
eBanking_VIEW	Automatically created	eBanking(VIEW)
ForeignExchange_MANAGE	Automatically created	Foreign Exchange(MANAGE)
ForeignExchange_REVOKE	Automatically created	Foreign Exchange(REVOKE)
ForeignExchange_VIEW	Automatically created	Foreign Exchange(VIEW)

Figure 1: Roles tab

This *Roles* tab displays the list of all currently defined SharePath Roles, including Role name, a free-text Description and the SharePath Application(s) to which the role applies. The description is especially important because it is the field that is visible when adding roles to individual users via the *Users* tab.

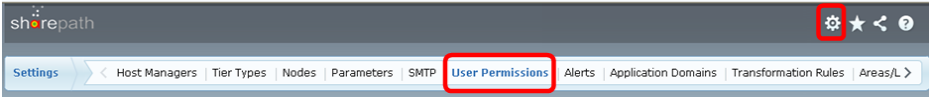
Creating a new Role

The roles tab enables you to create new roles, edit roles and delete roles.

- Select a specific Role from the list and click on Edit  icon (or double click on user line) to edit the Roles' properties dialog. See "Role Properties" below.
- Select a specific Role from the list and click the Delete  icon to remove the selected role from SharePath. Do this only if there is no user associated with the role.
- Click the create  icon to open the *new Role* properties dialog.

To create a new role:

1. Click *Settings* and select the *User Permissions* tab



2. Select the *Roles* tab

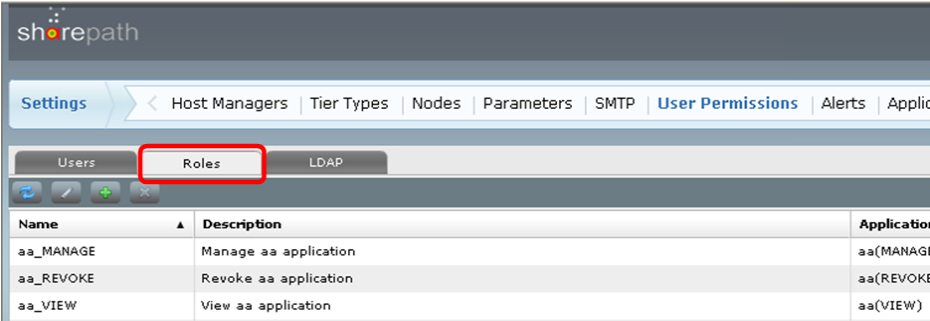

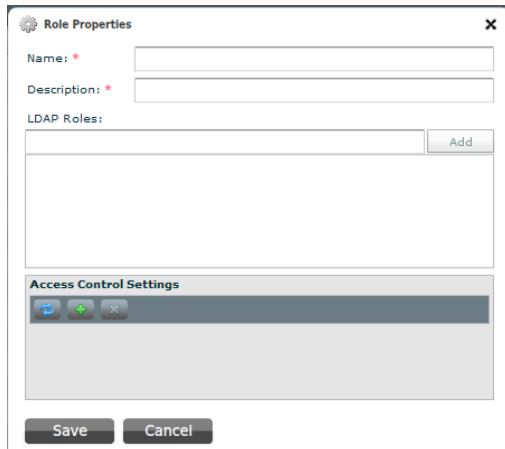


Figure 2: Select the Roles tab

3. Click Create  in the Roles tab toolbar.
The *Create Role* dialog is displayed.

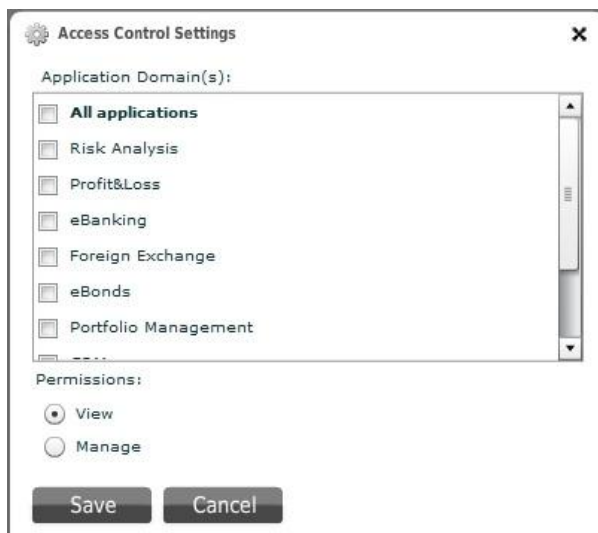


The **Role Properties** dialog box contains the following fields and controls:

- Name:** A text input field with a red asterisk indicating it is required.
- Description:** A text input field with a red asterisk indicating it is required.
- LDAP Roles:** A list box with an **Add** button to its right.
- Access Control Settings:** A section containing three icons (a blue gear, a green plus, and a red minus) and a large empty rectangular area below them.
- Buttons:** **Save** and **Cancel** buttons at the bottom.

Figure 3: Role Properties dialog

4. Fill in text fields according to the Role properties table below.
5. Add new Access Control Setting opens a dialog to select a SharePath Application for Manage or View.



The **Access Control Settings** dialog box contains the following fields and controls:

- Application Domain(s):** A list box with a scroll bar containing the following items:
 - ☒ **All applications**
 - ☐ Risk Analysis
 - ☐ Profit&Loss
 - ☐ eBanking
 - ☐ Foreign Exchange
 - ☐ eBonds
 - ☐ Portfolio Management
 - ☐ ...
- Permissions:** Two radio buttons:
 - ☒ **View**
 - ☐ **Manage**
- Buttons:** **Save** and **Cancel** buttons at the bottom.

Figure 4: Permissions for Viewing or Managing Applications

6. Add LDAP roles as relevant, clicking the *Add* button each time.

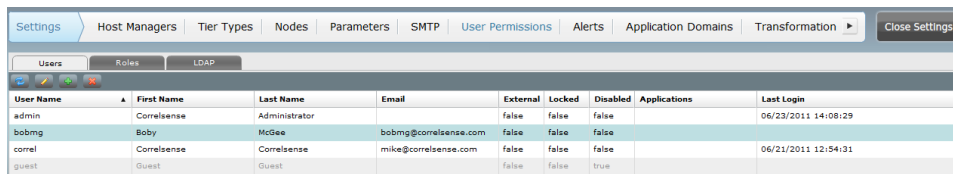
7. To save the Role, do one of the following:

- Click *Save* to save the new Role configuration, or
- Click *Save and New* to save the new Role and continue adding Roles. A new Create Role dialog is displayed.

Role Properties

Property Name	Description
Name	Role Name (unique key)
Description	Role Description
LDAP Roles	<p>Mapping of current SharePath Role to one or many existing LDAP Roles.</p> <p>Can be “None” if no mapping is required for this Role, or no LDAP integration.</p> <p>LDAP Role Names must be entered manually (since they are not maintained by SharePath but externally by the organization’s LDAP). Separated by comma.</p>
Access Control Settings	Define which Applications this Role can Manage or View. Add new Access Control Setting opens a dialog to select a SharePath Application for Manage or View.

Users tab






User Name	First Name	Last Name	Email	External	Locked	Disabled	Applications	Last Login
admin	Correlensense	Administrator		false	false	false		06/23/2011 14:08:29
bobmg	Bobby	McGee	bobmg@correlensense.com	false	false	false		
correl	Correlensense	Correlensense	mike@correlensense.com	false	false	false		06/21/2011 12:54:31
guest	Guest	Guest		false	false	true		

Figure 5: User Permissions tab

The *Users* tab presents the list of SharePath Users, including their main User properties, SharePath Applications association and date of last login.

From the *Users* tab SharePath Administrators can:

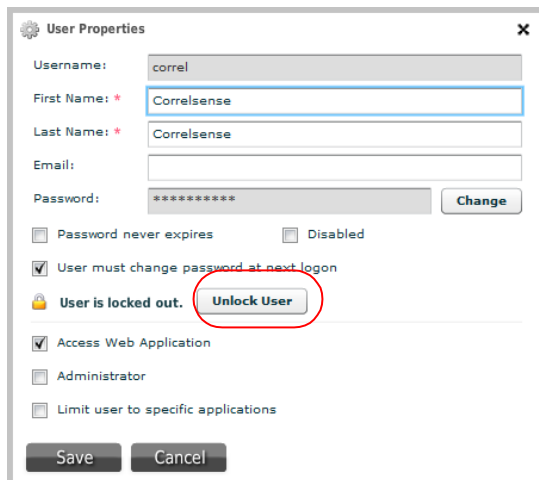
- Unlock locked users
- Create new users
Click on the *Create*  button in the User Permissions toolbar.
Use the dialog that opens to create a new user. For details, see [Creating a New User](#).
- Modify existing users
Select a specific user from the list.
Click on the *Edit*  button in the User Permissions toolbar (or double click on user line) to open the *User Properties* dialog. For descriptions of the fields, see [Fields of the Create User and User Properties dialogs](#)
- Delete users
Click on the *Delete*  button in the User Permissions toolbar to remove this user from SharePath.

Unlocking locked Users

A user may be locked out by the system for exceeding the maximum of consecutive unsuccessful password entry attempts. When a user is locked out, the administrator can unlock the user.

To unlock a user:

1. Go to Settings > Users Permissions > Users
2. Click on the locked out user.
3. Click the *Unlock User* button on the *User Properties* dialog that is displayed.
4. Click *Save*



The image shows a 'User Properties' dialog box with the following fields and options:

- Username: correl
- First Name: * Correlsense
- Last Name: * Correlsense
- Email:
- Password: ***** (with a 'Change' button)
- ☐ Password never expires ☐ Disabled
- ☒ User must change password at next logon
- ☒ User is locked out. (with an 'Unlock User' button circled in red)
- ☒ Access Web Application
- ☐ Administrator
- ☐ Limit user to specific applications

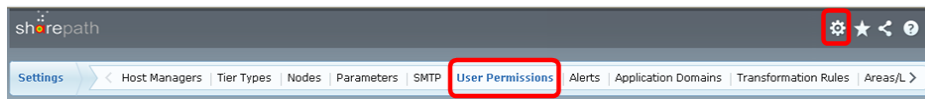
At the bottom are 'Save' and 'Cancel' buttons.

Figure 6: User Properties Dialog When a User Is Locked Out.

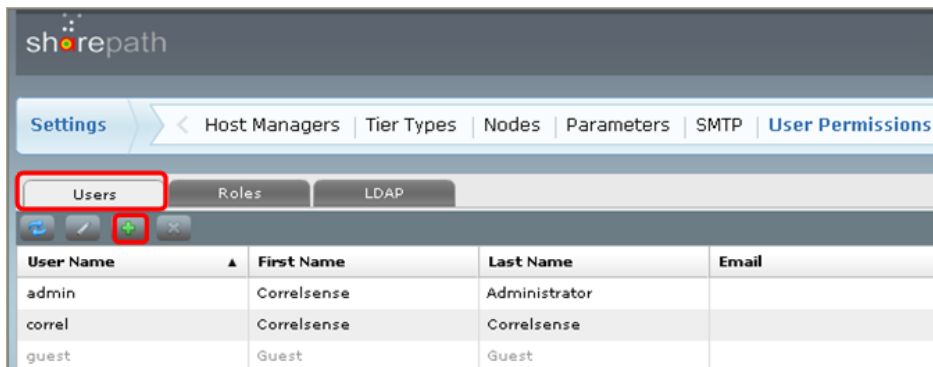
Creating a New User

To Create a New User:

1. Click *Settings* and select the *User Permissions* tab.



2. Select the *Users* tab and click the *Create* button  on the Users tab toolbar.



3. Click Create in the Users tab toolbar.

The *Create user* dialog is displayed.

Create user

Username: *

First Name: *

Last Name: *

Email:

Password: *

☐ Password never expires ☐ Disabled

☐ User must change password at next login

☐ Administrator

Application Role(s):

Figure 7: Create User dialog

4. Fill in text fields of the *Create User* dialog according to the field descriptions in the [Fields of the Create User](#) table below.

5. From the *Application Role(s)* drop down list, select one or more available roles to assign the User:

Create user

Username: * admin

First Name: * Correlense

Last Name: * Administrator

Email: Administrator1@xxx.com

Password: * *****

☐ Password never expires ☐ Disabled

☐ User must change password at next login

☒ Administrator

Application Roles: (0 selected)

- ☐ View Def application
- ☐ Manage Def application
- ☐ Revoke Def application
- ☐ View all applications
- ☒ Manage all applications
- ☐ View RiskAnalysis application
- ☐ Manage RiskAnalysis application
- ☐ Revoke RiskAnalysis application

Save Save & Add New Cancel

6. To save the user, do one of the following:

- Click *Save* to save the new user configuration
- or
- Click *Save and New* to save the new user and continue adding users (in which case a new Create User dialog is displayed).

Fields of the Create User and User Properties dialogs

Property Name	Description
Username	ID in the SharePath system
First Name	User's First Name
Last Name	User's Last Name
Email	Email address for use by system
Password	Current Password is not displayed. Administrator can change a user's password.
Password never expires	When checked, periodic requests for changing the password will be avoided for this user.
User must change password at next logon	The administrator can force a user to change his own password the next time he logs on.
Disabled	When this check box is selected, a user is not able to enter SharePath.
Administrator	<p>When value is true, the user has Administrator permissions, which means this user can change SharePath Settings.</p> <p>Administrator does not reflect any Application permissions. I.e. User might be an Admin but see no Applications.</p>
Application Roles	User can have one or more Application Roles. These Roles define access control permissions for Manage/View of specific SharePath Applications.
Applications	Select the check boxes of the applications the user can access from the displayed list. Available when the <i>Limit user to specific applications</i> check box is selected.

Property Name	Description
External (Available from Settings>Users Permissions >Users)	True indicates that user is managed by LDAP. In this case its properties are managed in LDAP so these fields will be disabled for editing.
Locked (Available from Settings>Users Permissions >Users)	True indicates that user is locked out of SharePath because wrong password entries exceeded the maximum permitted attempts. Administrator can unlock the user through the <i>Unlock</i> button on the <i>User Properties</i> dialog. NOTE: You will only see LOCKED when it is true. You will not see it when creating a new user.
Last Login (Available from Settings>Users Permissions >Users)	Shows when user last logged in. NOTE: This field is not displayed when creating a new user.

Assigning Roles to Users

Roles can be assigned to SharePath users manually via the *Users* tab or can be automatically assigned to external users through LDAP Integration and the association of LDAP roles with SharePath roles..

Comment [yg1]: Are these the same roles?

For Assigning roles manually, see [Creating a New User](#) and (Modifying a User TBD). For LDAP role integration, see [SharePath LDAP Integration](#).

Comment [yg2]: Make sure there is a cross reference to go to

Three roles are automatically created by SharePath every time a new application domain is established. These are the applicationx_view, applicationx_manage and applicationx_revoke roles.

The _view role allows the user assigned this role to view the data regarding this application.

The _manage role allows the user assigned this role to

- Managing Application and Transaction SLAs
- Determine *Transaction Descriptions* for the Application
- Assigning transactions to the Application (requires SharePath Administrator privileges)
- Define *Transaction Naming* rules for the application

The `_revoke` role bars a user assigned privileges to all applications from a particular application. This role is only relevant in situations where an ALL role has been applied to a user.

The `_view` role limits a user assigned manage privileges to all applications to view to a view role on the targeted application.

To associate an LDAP role with a SharePath role:

1. Click on *Settings > User Permission >> Roles* tab
2. Click the required SharePath role or create a new role.
3. In the LDAP Roles text box, add the LDAP Role to be associated with the SharePath role.
4. Click on the Add button.
5. Repeat steps 3 and 4 as required.
6. Click the *Save* button.

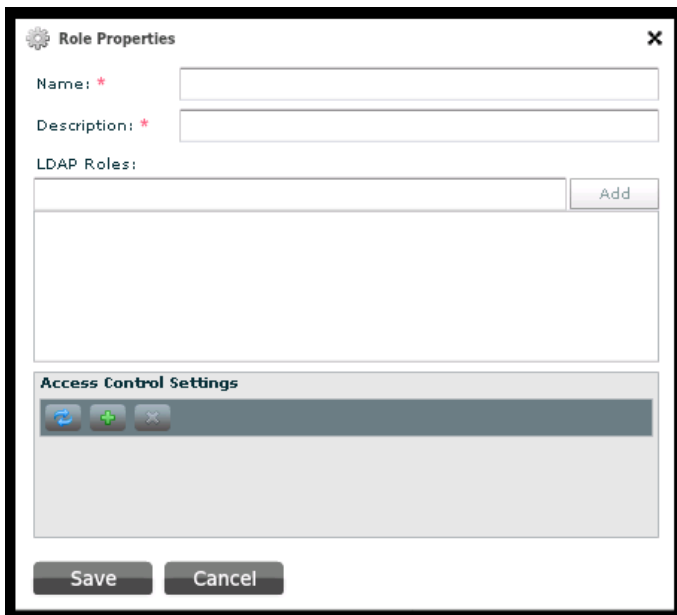


Figure 8: SharePath Role Properties tab

SharePath LDAP Integration

SharePath enables integration with your organization's LDAP for authentication and authorization.

LDAP integration enables user authentication based on LDAP user policy settings, and authorization based on LDAP user-group association. Mapping between LDAP users and SharePath users, and between

LDAP “Roles” (groups) and SharePath Roles facilitates efficient management of SharePath registration and SharePath user privileges for all members of your organization.

Users who are SharePath Users before LDAP integration or were added to your organization’s LDAP system after being previously registered through SharePath, remain internally defined SharePath users; All their role definitions remain as defined in the SharePath system. To change the status of one of these users, their *local* status must be changed via the SharePath database to *external*.

External Users (users on basis of LDAP credentials) have all the privileges of the SharePath roles that their LDAP roles are linked to. For example, if CRM_Manager role in SharePath is associated with CRM_Level1 in the LDAP system, all users with CRM_Level1 role in the LDAP system will receive the privileges associated with the CRM_Manager in SharePath

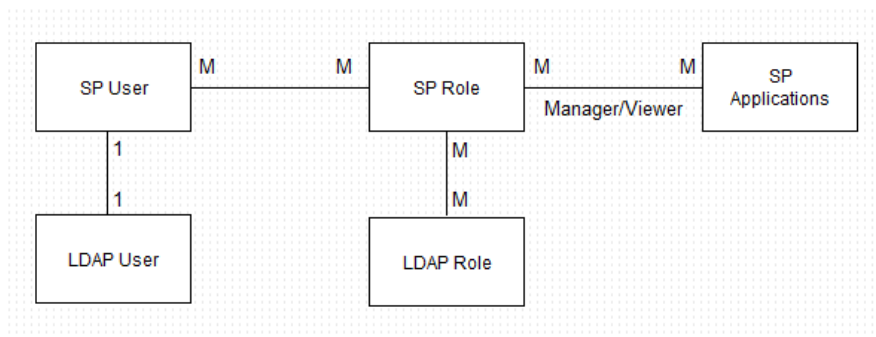


Figure 9: SharePath Permissions model.

A SharePath (SP) User can be attached to one or more Roles. Each Role can be attached to one or more Applications, as a Manager or Viewer per Application. When a User is attached through two (or more) Roles to the same Application, the higher permission (Manager) overrides lower permission (Viewer) defined by another Role.

Here are some principles for working with SharePath and LDAP roles and users:

- One LDAP User is associated with one SharePath User.
- A SharePath Role can be associated with several corresponding LDAP Roles and vice versa.

LDAP tab

Use this tab to define LDAP integration.

The screenshot shows the 'LDAP' tab in a configuration window. At the top, there are three tabs: 'Users', 'Roles', and 'LDAP', with 'LDAP' being the active tab. Below the tabs, there is a checkbox labeled 'Enable user authentication via LDAP'. Under this, there are two sections: 'LDAP Connection' and 'LDAP Authentication & Authorization'. The 'LDAP Connection' section contains fields for 'LDAP Host' (value: yanive7w), 'LDAP Port' (value: 389), a checkbox for 'Use SSL Connection' (unchecked), 'Admin DN' (value: uid=user.4,ou=People,dc=another,dc=com), and 'Admin Password' (masked with asterisks). A 'Test Connection' button is located to the right of the 'Admin Password' field. The 'LDAP Authentication & Authorization' section contains several fields with red asterisks indicating they are required: 'Search Base' (value: dc=another,dc=com), 'User Name Attribute' (value: uid), 'First Name Attribute' (value: givenName3), 'Last Name Attribute' (value: sn), 'Email Attribute' (value: mail), 'Role Name Attribute' (value: cn), 'Role Membership Attribute' (value: member), and 'Role Object Class' (empty). A 'Save' button is located at the bottom left of the form.

Figure 10: SharePath Permissions model.

LDAP integration is both configured and enabled from the LDAP tab.

- To enable the LDAP connection, define *LDAP Host* and *Port* and click the *Test Connection* button.
- To enable LDAP SSL connection, select the *Use SSL Connection* text box, define *Admin DN* and enter the *Admin* password before clicking the *Test Connection* button
- To enable LDAP integration, define the following parameters on the LDAP tab and select the *Enable user authentication via LDAP* checkbox at the top of the LDAP tab. Note that when *Enable user authentication via LDAP* checkbox is selected and the setting is saved, the value of the parameter *usersPolicy* is "Multiple". When the *Enable user authentication via LDAP* checkbox is deselected and the setting is saved, the value of *usersPolicy* is "Local". (To verify this, see *Settings > Parameters* tab and search all parameters whose name contains the string "usersPolicy".)

Field / Checkbox	Description / Instructions	Purpose
LDAP Host	Name of LDAP connection Host Enter name of Host	Connection to LDAP server
LDAP Port	LDAP server port number Default: 389	
Use SSL Connection (checkbox)	Select this checkbox for SSL connection to LDAP database	
Admin Dn	Define Administrator allowed to view all LDAP data. The Admin DN is a fully qualified name that uniquely identifies the Admin in the directory	
Admin Password	Password for Admin DN	Attributes for LDAP integration
Search Base	Location from which the LDAP search begins - The DN (Distinguished Name) of the entry at which to start a lookup search	
User Name Attribute	The name of the DN's attribute that stores the user's name (user-id).	
First Name Attribute	The name of the DN's attribute that stores the user's first name.	
Last Name Attribute	The name of the DN's attribute that stores the user's last name.	
User Email Attribute	The name of the DN's attribute that stores the user's email.	
Role Name Attribute	The name of the Role Object Class attribute that stores the Role name.	
Role Membership Attribute	The name of the Role Object Class attribute that stores the list of Users associated with this Role.	
Role Object Class	- The name of the LDAP Class that is used for Role association (usually LDAP Group Class).	

- Selection of the Enable LDAP authentication checkbox affects the setting of the parameter usersPolicy. Values for this parameter include Local, External, Multiple:
 - Local - Only local users are allowed (LDAP is not enabled).
 - External - Only external users are allowed (This is not in use).
 - Multiple - Both local users and external users are allowed. (This is the setting when the Enable LDAP user authentication is enabled. It means that both SharePath user registrations and LDAP user definitions are used for user authentication in by the SharePath server.

