# pure::variants Model Server Administration Manual

pure-systems GmbH

Version 6.0.5.685 for pure::variants 6.0

Copyright © 2003-2024 pure-systems GmbH

2024

## Table of Contents



## 1. Introduction

The pure::variants Model Server Administration allows the administration of the users and roles for a pure::variants model server. It provides an editor to create, delete, modify, import, and synchronize users and roles, and to assign users to roles and vice versa. These operations require administrative access rights. The user and role data of a pure::variants model server is managed in the special administration project “ADMIN”.

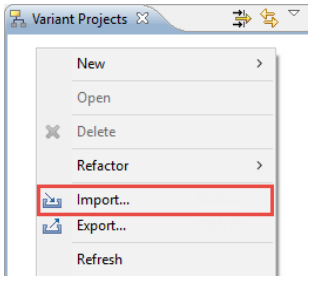
A printable version of this document is available.

## 2. Administration Project

The special administration project “ADMIN” exists on each pure::variants model server. It is used to define access rights for all projects, and to manage users and roles. In order to do this, you have to import the “ADMIN” project from the model server into your workspace first. This may require administrative rights.

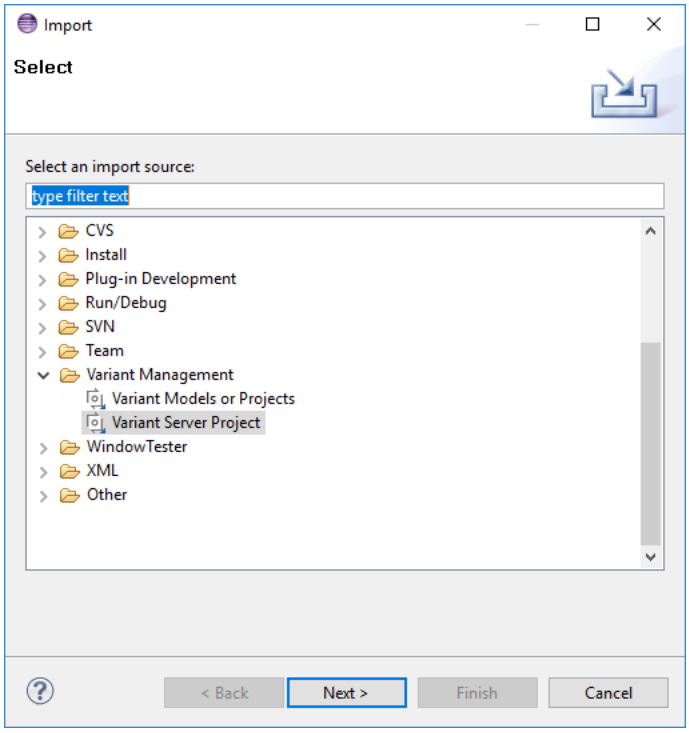
To import the “ADMIN” project, right-click in the “Variant Projects” view and select “Import...” from the context menu.

**Figure 1. Import from Context Menu**



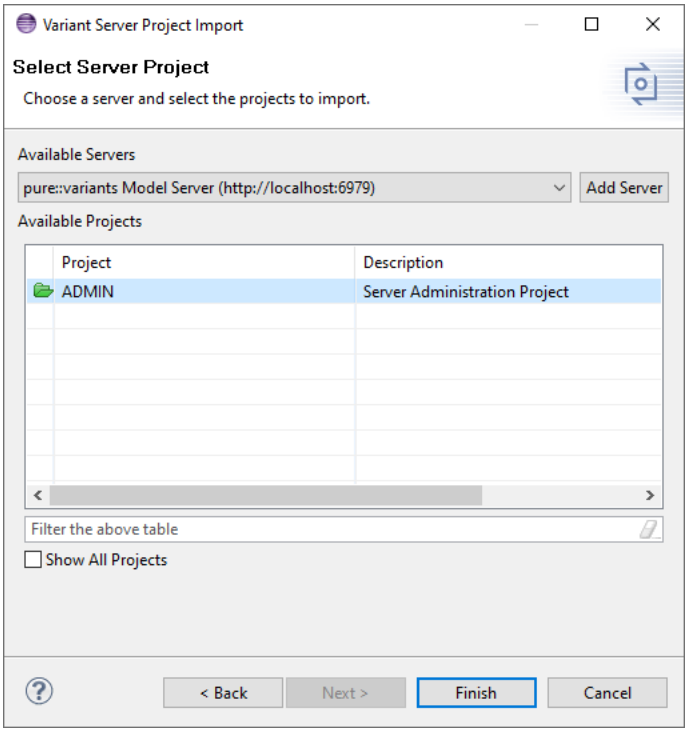

Select “Variant Server Project” from the list and click “Next”.

**Figure 2. Import Variant Server Project**



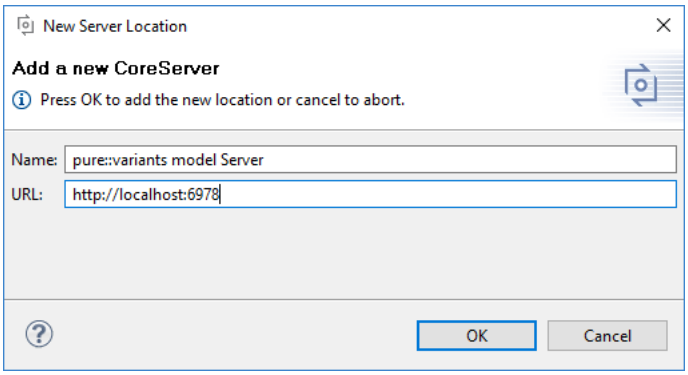

On the next page you can choose from the list of known pure::variants model servers, or add a new server if the server you want to connect to is not in the list.

**Figure 3. pure::variants Model Server and Project Selection**




To add a new server click “Add server”. A dialog pops up which allows you to enter a short description of the server, and its URL in the form “http://servername:port” or “https://servername:port”.

**Figure 4. Add a new pure::variants Model Server**



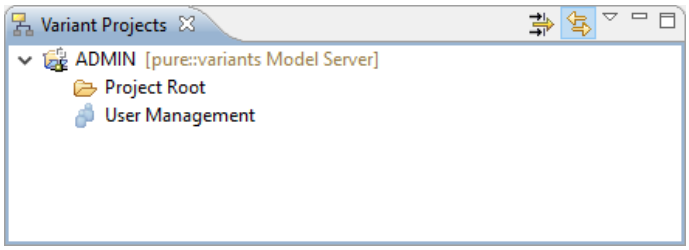

Click “OK” to add the new server to the list of pure::variants model servers.

You can manage the pure::variants model servers also in the pure::variants preferences by opening menu “Window” -> “Preferences” -> “Variant Management” -> “Known Servers”. Please consult the “pure::variants Server Support Plug-In Manual” for details.

After you have chosen or added a server, you are asked by the server to login. If you successfully authenticated at the server, the projects are shown that exist on this server and that you are permitted to see.

If you don't see the “ADMIN” project in the list of available projects, or it is marked with a red lock, then you don't have the appropriate permissions to import it. If the “ADMIN” project is listed with a green icon, then please select it and click “Finish” to import it into the workspace.

**Figure 5. Imported ADMIN Project**




The “ADMIN” project contains two entries.

| | |
|---|---|
| Project Root | This is a virtual folder for all the projects on the model server. It is used to define access rights for all projects, including the right to create new projects. |
| User Management | This is the user management model containing all the users and roles of the model server. It is used to manage the users and roles. All users should have “Read” access to this model. |

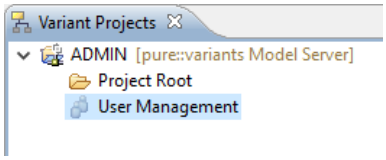
# 3. Users and Roles

Users and roles are managed in the “User Management” of a pure::variants model server.

## 3.1. Open User Management

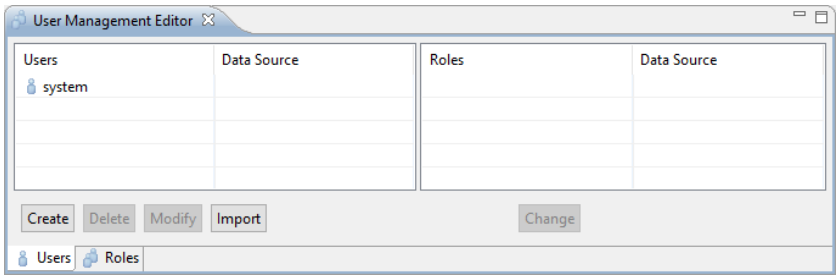
To manage users and roles, double-click the “User Management” item in the “ADMIN” project.

**Figure 6. Open User Management**




The “User Management” editor opens and shows all available users in the left table. Initially after installation of a pure::variants model server, there is only one user, i.e. the build-in user “system”.

**Figure 7. User Management Editor**

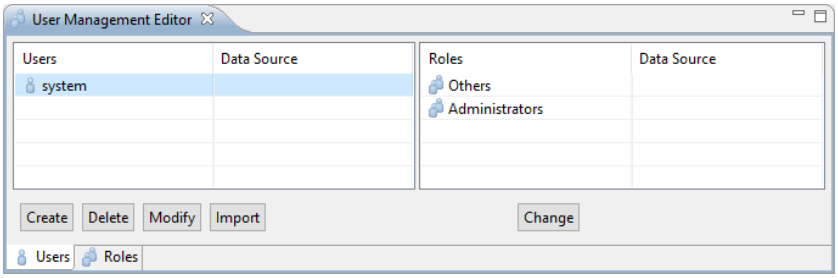



### Note

The build-in user “system” has a predefined password that MUST BE CHANGED immediately after starting the first time a model server that supports local authentication. Since all pure::variants server installations share this initial password, keeping this password unchanged renders the server insecure. Please consult the "pure::variants Server Quick Installation Guide" for the password. Please see Section 3.4, “Change User Password” on how to change the password.

If you select a user in the table, the right table shows all roles assigned to this user. Initially there are two roles named “Administrators” and “Others”.

**Figure 8. Selected User**




Users and roles can be sorted alphabetically ascending and descending by clicking the “Users” or “Roles” table column titles.

Users and roles can be imported from and synchronized with data sources, in which case they have a data source assigned. To sort the users or roles by their data source, click the “Data Source” table column title.

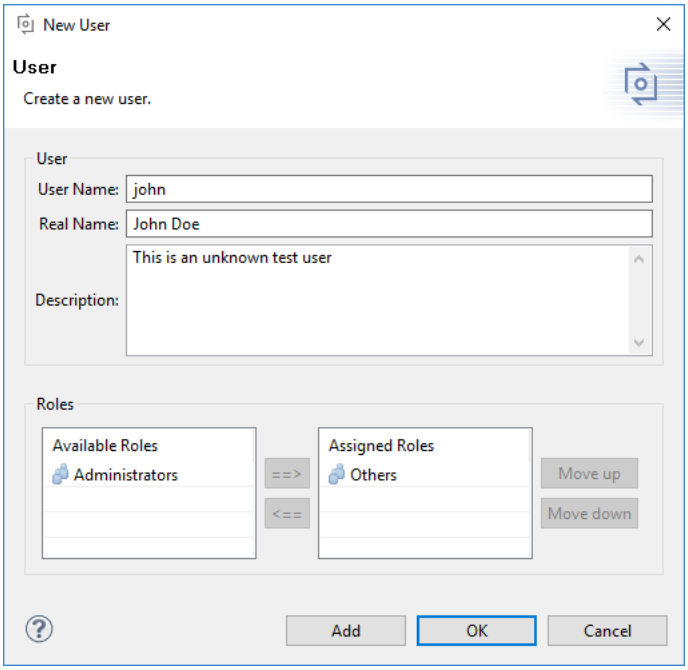
## 3.2. Create Users and Roles

To create a new user click the “Create” button on the lower left of the editor. A dialog opens (see Figure 9, “Create a new User”) where you can enter the unique name (i.e. username), real name, and description of the user.

The bottom of the dialog shows two lists where you can assign the user to existing roles. The left side of the list shows all available roles. The right side shows all roles which are already assigned. You can assign a user to a role by selecting the role on the left side and click the “==>” button, or simply double-click the role on the left side. To remove a user from a role you need to select the role on the right side and click the ”<==” button, or double-click the role on the right side.

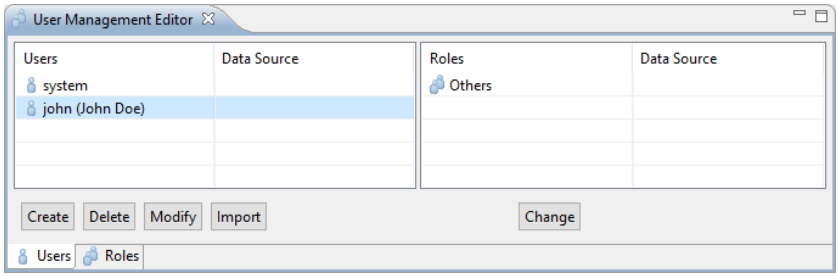
To create more than one user click the “Add” button after entering the user data of the first user. This creates the first user with the given data and clears the dialog values. You are now able to create another user.

**Figure 9. Create a new User**



Clicking the “OK” button creates the user and closes the dialog. The newly created user is shown in the left table of the “User Management” editor.

**Figure 10. New User**




Creating a role works just the same. You only need to select the “Roles” tab on the lower left part of the editor and then click “Create”.

Roles can have one of the following functions:

- Reader

  User having the Reader role do have read access to the models in the server only.

  For read only access to the model server no license is needed in the web client.

  In the desktop client still a license is necessary but user does have read only access to the models from the model server. Local projects are not affected.

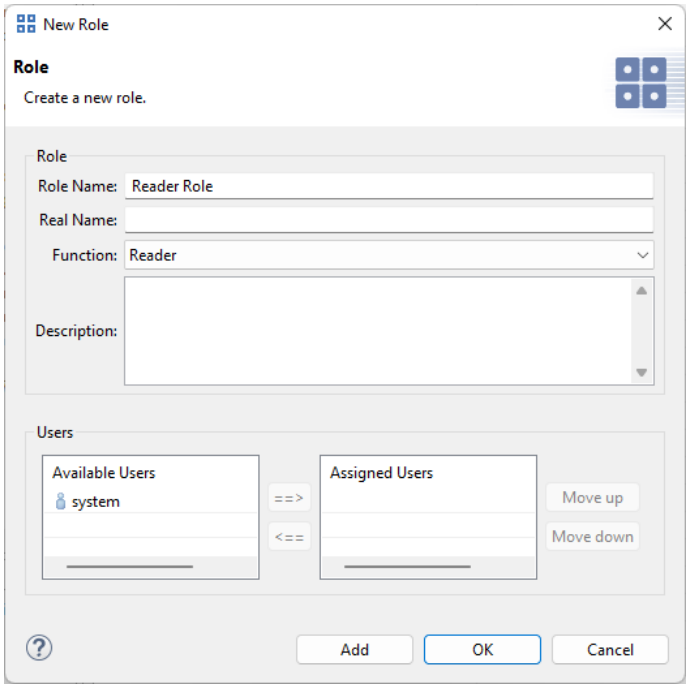
- Transformation Administrator

  Users having this role are allowed to administer transformation configurations in the web client. This role has no affect to the desktop client.

- Permission

  Roles which define access rigths to the model server models.

**Figure 11. Create a new Role**



## 3.3. Modify Users and Roles

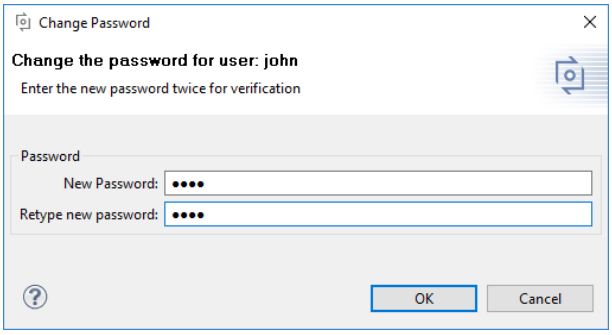
To modify a user, select the user in the left table of the editor and click the “Modify” button, or simply double-click the user. The modification dialog opens which is the same dialog as for creating users and roles. Click the “OK” button to apply the modifications for the selected user or role.

## 3.4. Change User Password

If a pure::variants model server supports local authentication, then the passwords needed for local authentication are managed by the server itself (instead of maybe an LDAP server) and can be changed. Otherwise, changing passwords from within pure::variants is not supported.

To change a user's password, right-click the user in the “User Management” editor and choose “Change Password” from the context menu. A dialog opens where you have to enter the new password twice, and then apply it by clicking “OK”.

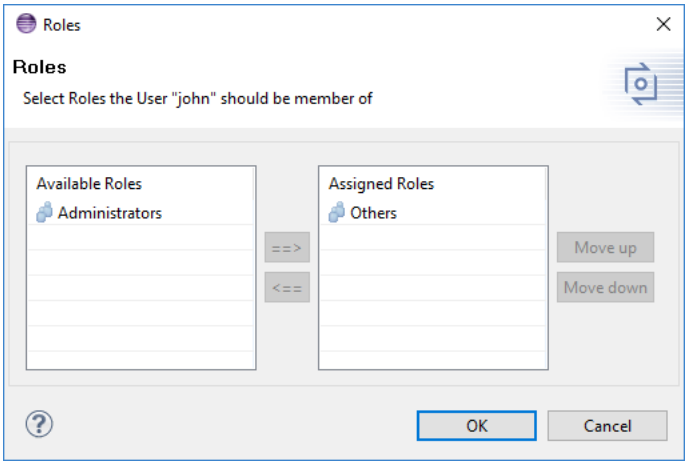
**Figure 12. Change User Password**




## 3.5. Change Roles assigned to a User

To change the roles assigned to a user, select the user in the left table of the “User Management” editor and click the “Change” button below the role list, or simply double-click the user. A dialog opens showing the available and already assigned roles. To assign a role, double-click it in the “Available roles” list or select it and use the “==>” button. Apply the changes by clicking “OK”. The changes take effect after the next login of the user.

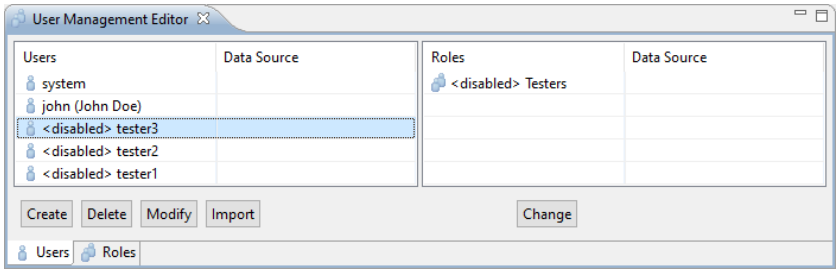
**Figure 13. Role Assignment Dialog**




## 3.6. Enable and Disable Users and Roles

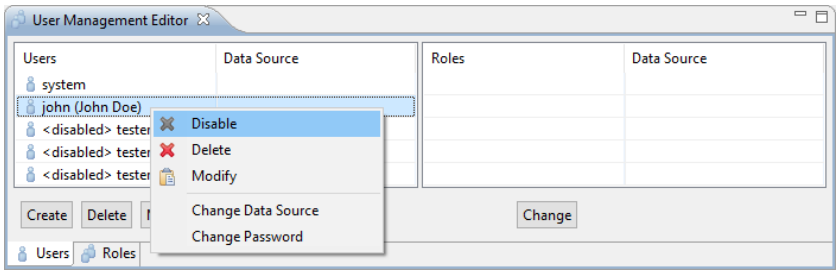
Users and roles can be disabled. If a user is disabled, then this user cannot login to the server anymore. If a role is disabled, then the permissions granted to this role do not apply. The name of disabled users and roles is automatically prefixed with “<disabled>” in the “User Management” editor.

**Figure 14. Visualization of disabled Users and Roles**



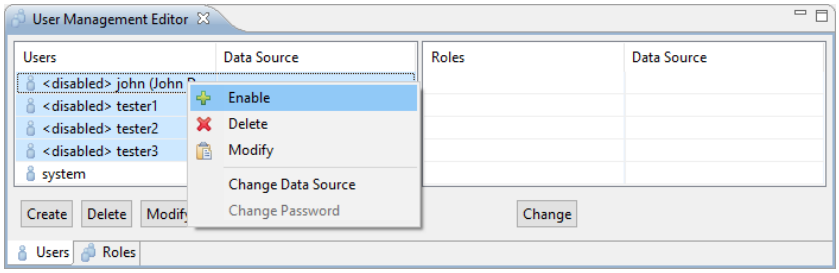

To disable an existing user or role, select it in the “User Management” editor, right-click to open the context menu, and choose the “Disable” action.

**Figure 15. Disable a User**




To enable a disabled user or role, select it in the “User Management” editor, right-click to open the context menu, and choose the “Enable” action.

**Figure 16. Enable Users**

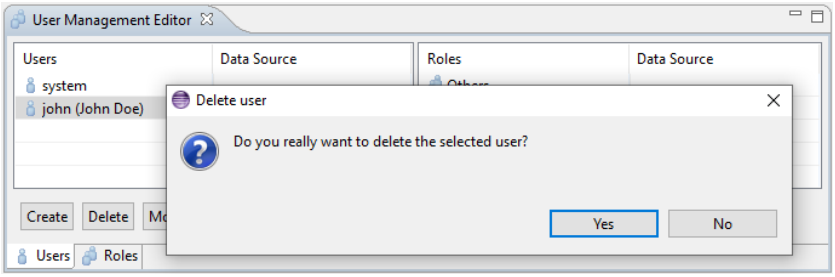



You can enable or disable multiple users and roles at once. Just left-click the users or roles while pressing the “Ctrl” or “Shift” key, or press the keys “Ctrl” + “A” to select all, and then right-click to open the context menu and choose the “Enable” or “Disable” action.

## 3.7. Delete Users and Roles

To delete an existing user or role, select the user or role in the “User Management” editor and either click the “Delete” button or press the “Del” key on the keyboard. After clicking “Yes” in the confirmation dialog the selected user or role is deleted and removed from its assigned roles.

**Figure 17. Delete User or Role**




You can delete multiple users and roles at once. Just left-click the users or roles while pressing the “Ctrl” or “Shift” key, or press the keys “Ctrl” + “A” to select all, and then right-click to open the context menu and choose the “Delete” action, or press the “Del” key.

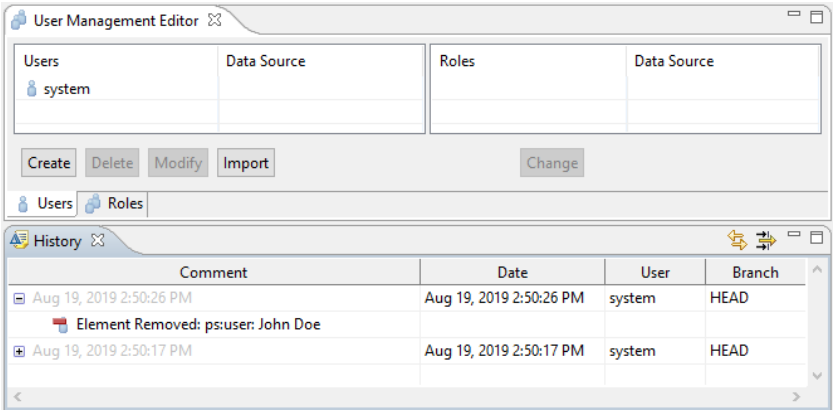
### Note

If a user or role is deleted, then this does not automatically delete the access rights granted to that user or role for any resource on the pure::variants model server. If you recreate a user or role with the same name, then this user or role will have the same rights again.

## 3.8. Restore Users and Roles

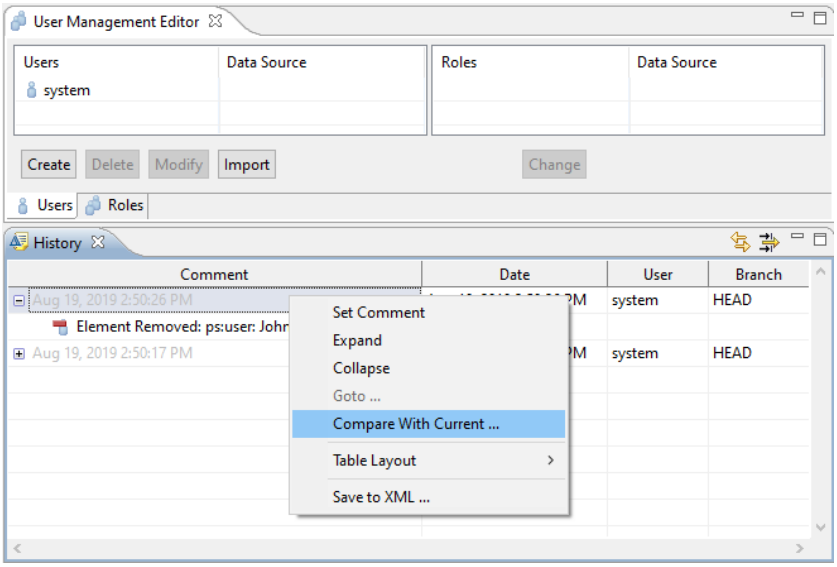
If users or roles have been changed or deleted, then you can restore them using the pure::variants change history. To do this, open the “User Management” editor. Then open the “History” view by clicking “Window” -> “Show View” -> “Other...”, scroll down to and expand “Variant Management”, and double-click “History”.

**Figure 18. Change History**



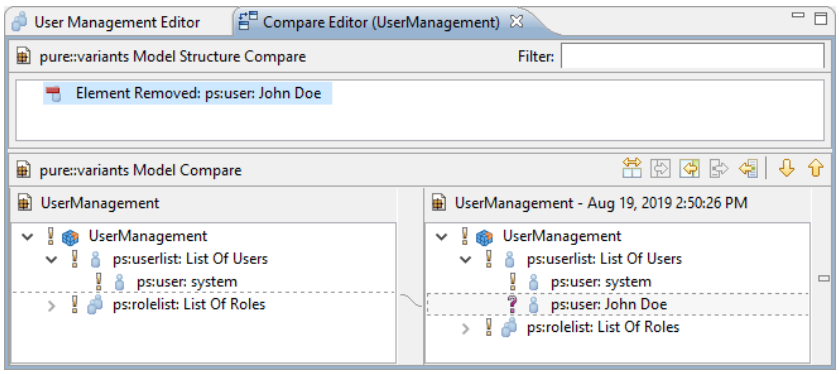

The “History” view shows the changes on the “User Management” in chronological order, beginning with the newest change. If for instance the user “John Doe” shall be restored, select the change that removed the user, right-click to open the context menu, and select “Compare With Current ...”.

**Figure 19. Compare With Current State**



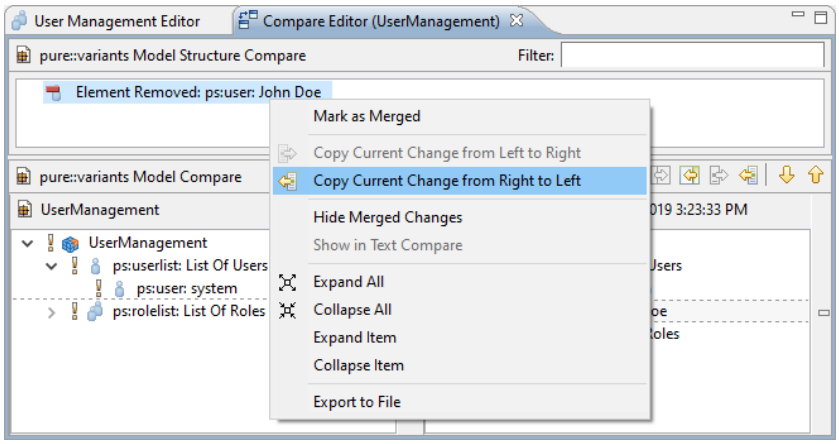

All the changes occurred between the selected change and the current state of the “User Management” are presented in a compare editor.

**Figure 20. Compare Editor**



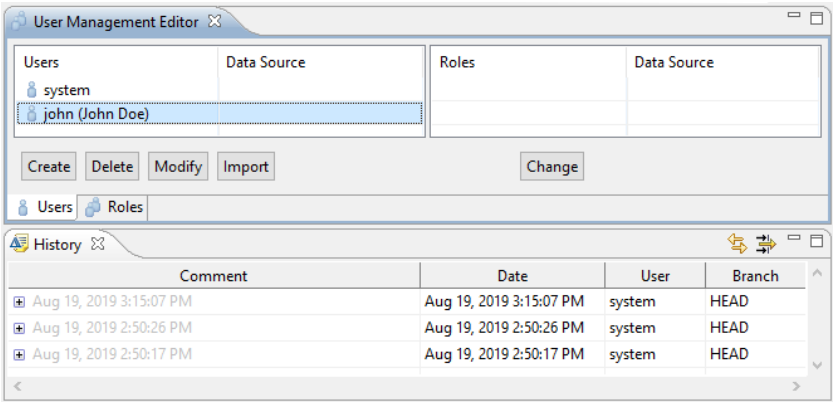

You can select changes in the upper part of the editor which then shows the details in the lower part. To restore a change, right-click a change and select “Copy Current Change from Right to Left”.

**Figure 21. Revert a Change**




The change is reverted immediately.

**Figure 22. Restored User**




### Note

This is a low level comparison of “User Management” versions. Changes may be more complex as shown in the example above. Please revert changes carefully.

## 3.9. Import Users and Roles

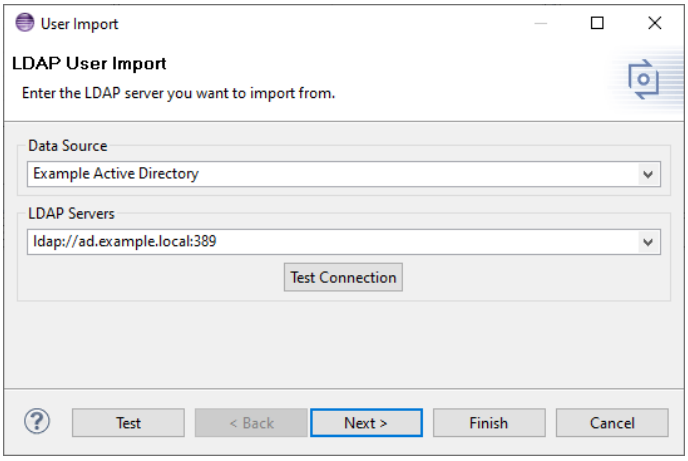
pure::variants supports the import of users and roles from external data sources. To import users or roles, click “Import” below the left table of the “User Management” editor.

If you do this on the “Users” tab of the “User Management” editor, then you can import users and optionally the roles that the imported users are member of.

If you do this on the “Roles” tab, then you can import roles and optionally the users that are member of the imported role.

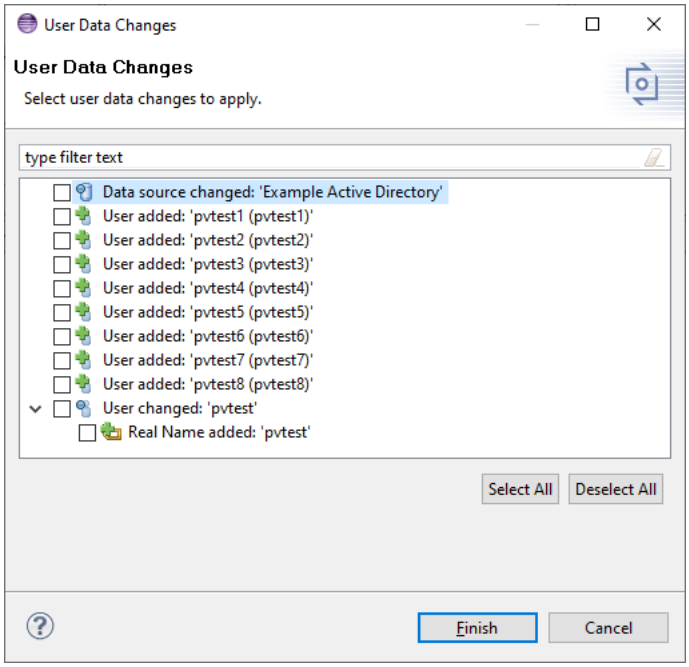
In both cases an import dialog opens allowing you to select the data source from which to import the users or roles, make changes on the import settings, test the import, and eventually perform the import. As for now, LDAP directory servers are the only supported data source. See Section 4.2, “LDAP Directories”.

**Figure 23. User Import from an LDAP directory**




After finishing the import dialog, the import from the data source is performed and the imported users and roles are presented to you. If the data source settings have been changed, then this is also marked as a change.

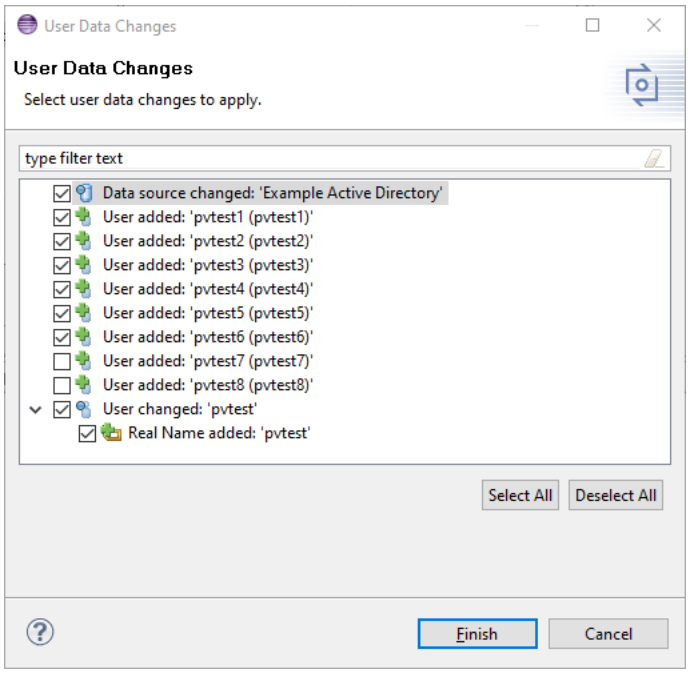
**Figure 24. Import Result**




As a result of the import, new users or roles may be added, and existing users and roles may be disabled or updated according to the existence and state of the users and roles in the data source.

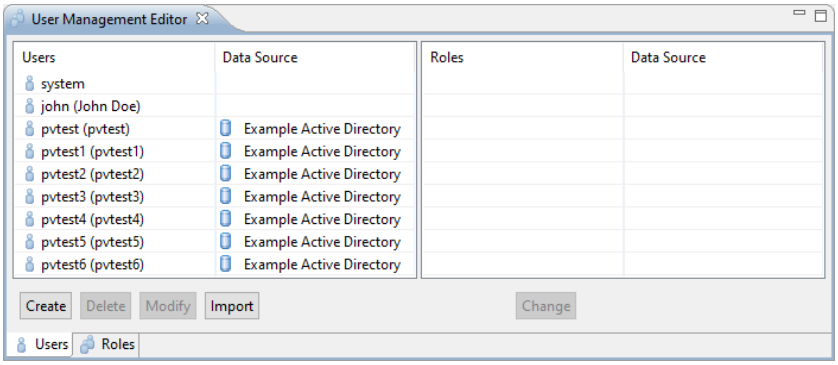
As long as no listed change is selected, nothing will changed. To select all the changes, click “Select All”. You can deselect all selected changes by clicking “Deselect All”. In the following screenshot all changes have been selected, except the changes that add the users “pvtest7” and “pvtest8”.

**Figure 25. Selective Import**




Click “Finish” to apply the selected changes, and “Cancel” to abort the import. The imported users and roles are now shown in the “User Management” editor.

**Figure 26. Imported Users**



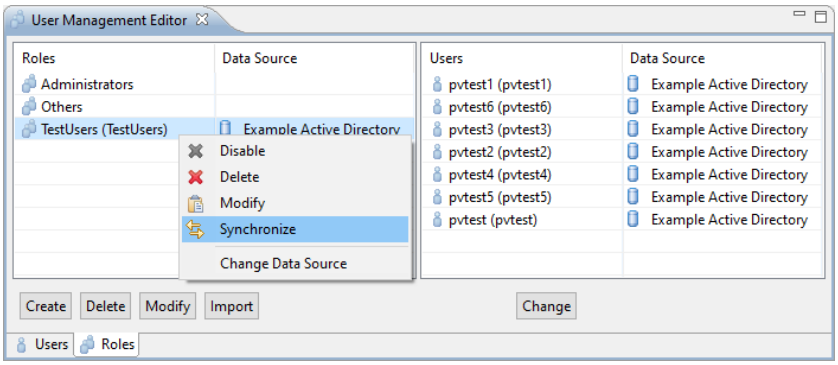

## 3.10. Synchronize Users and Roles

Users and roles with a data source assigned can be synchronized with that data source. This means that user and role data of the model server is compared to the data of the data source. If changes are found, then these changes can be applied to the model server's user and role data.

To synchronize a user or role, right-click the user or role in the “User Management” editor and choose “Synchronize” from the context menu.

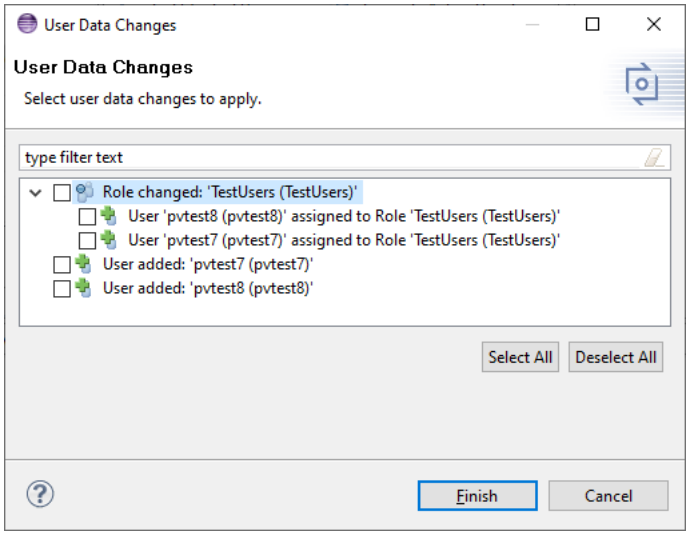
You can also synchronize at once multiple users and roles with the same data source assigned. Just left-click the users or roles while pressing the “Ctrl” or “Shift” key, or press the keys “Ctrl” + “A” to select all, and then right-click to open the context menu and select “Synchronize”.

**Figure 27. Synchronize Role “TestUsers”**




You may be asked to login to the data source, e.g. an LDAP directory server. Then the selected users or roles are compared with the data source. If changes are found, a dialog is opened to let you select the changes to apply.

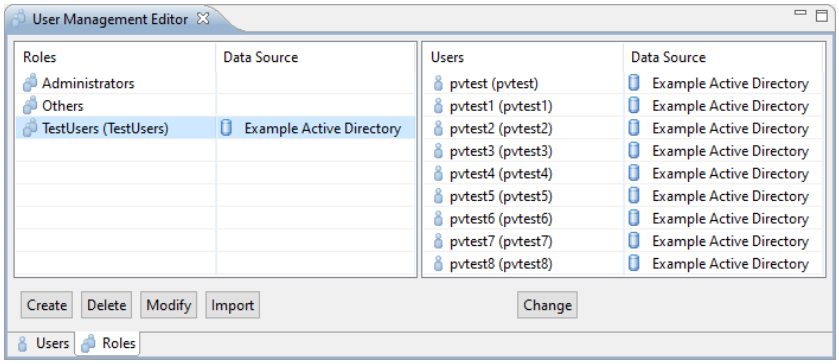
**Figure 28. Changes Found**




Please see Section 3.9, “Import Users and Roles” for details on how to use this dialog.

After applying all changes, the users and roles in the “User Management” have been updated. In this example, the two users “pvtest7” and “pvtest8” have been added and assigned to role “TestUsers” according to the data source.

**Figure 29. Synchronized Users and Roles**




If a synchronized user or role does not exist in the data source, then it may be disabled in the model server. Users and roles are updated if they also exist in the data source. If a role is synchronized, then new role members (i.e. users) may be imported from the data source. If a user is a member of a role in the model server but not anymore in the data source, then the role assignment of the user may also be removed in the model server. Former role members may be disabled if they are not member of any group anymore after synchronization with the data source. This all depends on the data source.

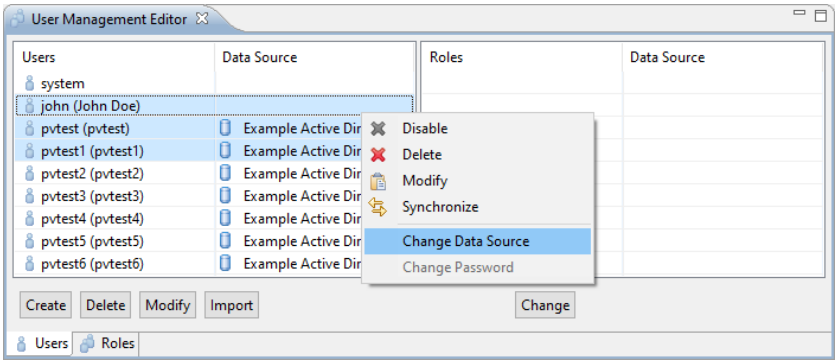
## 3.11. Change Data Source of Users and Roles

Users and roles are assigned a data source implicitly by importing them from that data source. But you can also explicitly assign a data source to users and roles, or change the assigned data source, or even remove the data source from a user or role at all.

To change the data source of a user or role, right-click the user or role in the “User Management” editor and choose “Change Data Source” from the context menu.

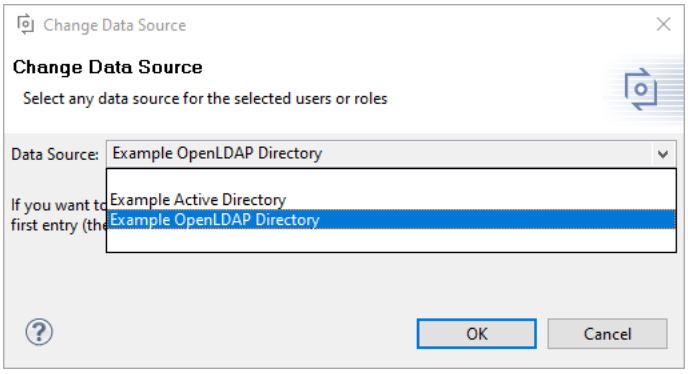
You can also change the data source of multiple users and roles at once. Just left-click the users or roles while pressing the “Ctrl” or “Shift” key, or press the keys “Ctrl” + “A” to select all, and then right-click to open the context menu and select “Change Data Source”.

**Figure 30. Change Data Source**



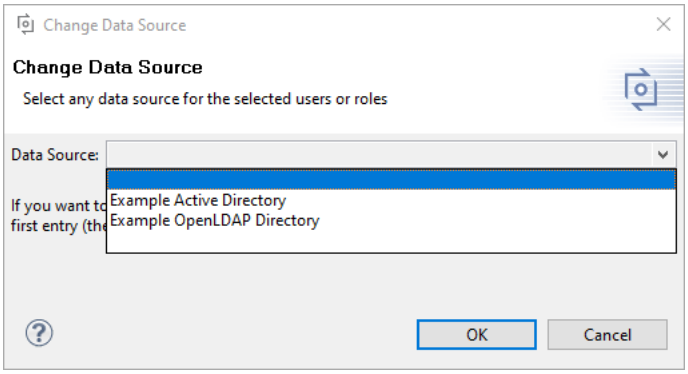

This will open a dialog where you can choose the new data source.

**Figure 31. Select new Data Source**



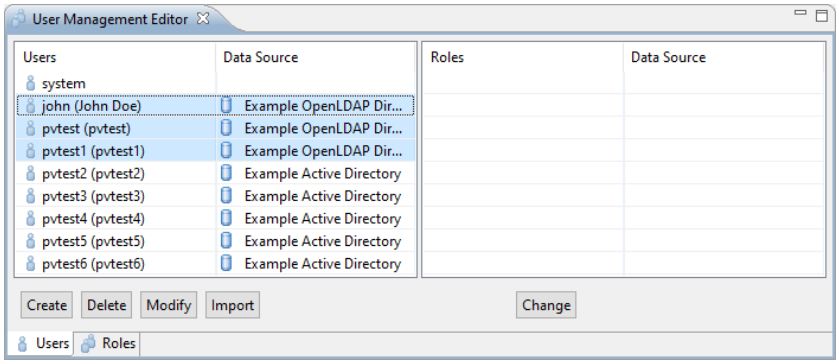

You can also remove the data source of the selected users or roles by choosing the first (the empty one) entry from the data sources list.

**Figure 32. Remove Data Source**




The new data source is applied by clicking “OK”.

**Figure 33. Data Source Changed**



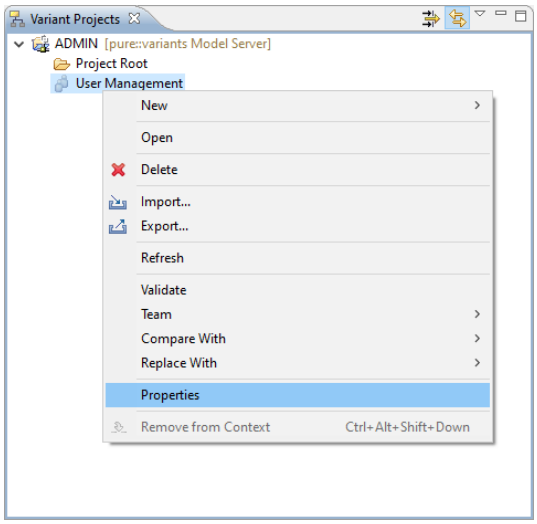

# 4. Data Sources

The data sources for user and role imports and synchronization are stored in the “User Management” of a pure::variants model server. As for now LDAP directory servers are the only supported data source.

## 4.1. Manage Data Sources

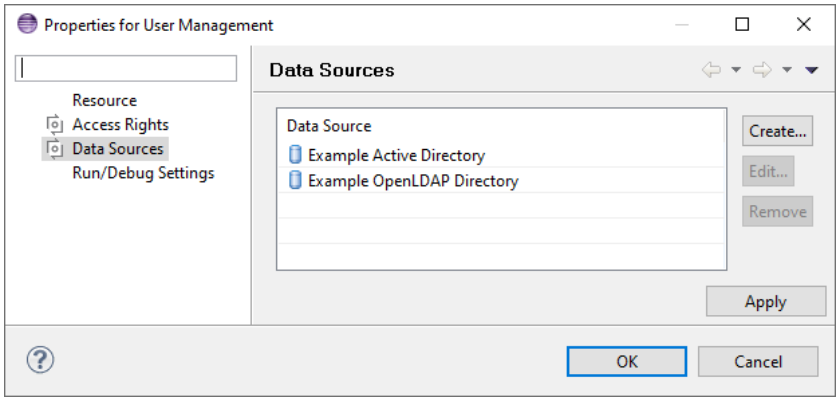
Data sources can be added, changed, and removed. Right-click the “User Management” in the “Variant Projects View” and select “Properties” in the context menu.

**Figure 34. Open User Management Properties**



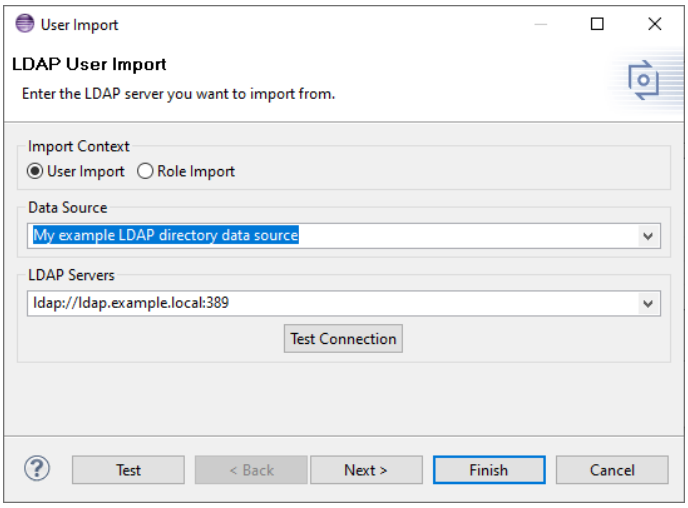

Select the entry “Data Sources” to open the data sources management page.

**Figure 35. Data Source Management**




You can add new data sources by clicking “Create...”. This will open a data source type dependent dialog to setup the settings for the data source.

**Figure 36. New Data Source (LDAP)**




To change an existing data source, left-click the data source and then click “Edit...”, or simply double-click the data source. This will also open a data source type dependent dialog to change the name or settings of the data source.

A data source can be deleted by selecting the data source and clicking “Remove” or pressing “Del” key on the keyboard. This also works if multiple data sources are selected. Data sources can only be deleted if they are not assigned to any user or role.

## 4.2. LDAP Directories

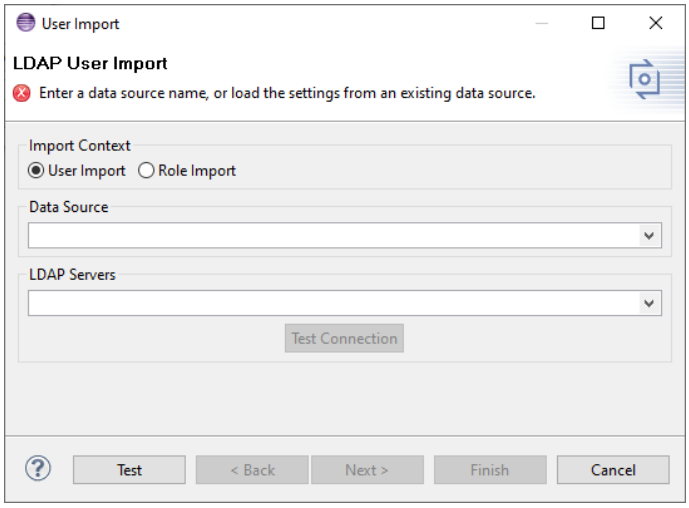
Users and roles can be imported from and synchronized with LDAP directory servers. This requires read access to the LDAP directory server. Since LDAP directories usually are highly configurable, some information is needed in order to retrieve user and role data from the LDAP directory.

The following sections describe the dialog that is used to import users or roles from an LDAP directory server, or to setup and change a corresponding data source.

### 4.2.1. Server Settings

On the first page of the dialog the LDAP data source is configured.

**Figure 37. LDAP Data Source**



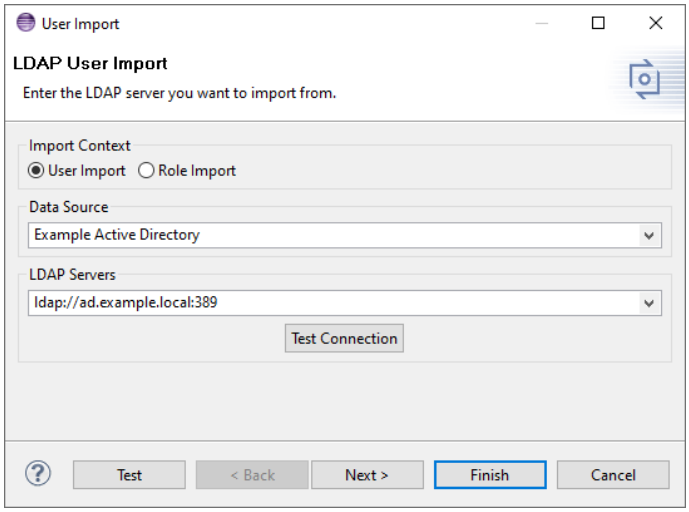

When adding or editing an LDAP data source, you have the possibility to select an import context for testing purposes. If you select “User Import”, then you can test user imports. If you select “Role Import”, role imports can be tested.

You can start an import test by clicking “Test” in the lower left of the dialog. This will not do any changes, but you will be presented with the list of changes to the users and roles that an import from the data source with the current settings could result in.

If no data source is selected, you either have to enter a new data source name to store the data source settings under this name. Or you choose an existing data source which then is loaded into the dialog.

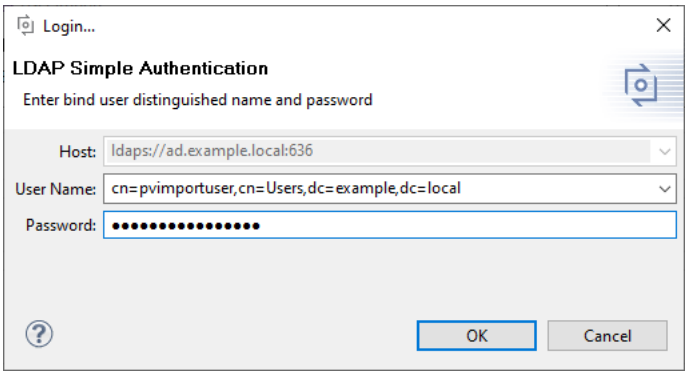
To import user and role data from an LDAP directory server, the URL of the LDAP directory server needs to be entered, according to RFC 2255 supporting protocols “ldap” and “ldaps” (e.g. "ldaps://ad.company.com:636").

**Figure 38. Data Source Name and LDAP Server URL**




The entered LDAP server URL can be tested by clicking “Test Connection”. This will open a login dialog where you have to enter the username and password needed to connect to the LDAP server. The username usually needs to be entered with its full distinguished name (e.g. “cn=username,cn=Users,dc=company,dc=com”). This user must have at least read and search rights in the branches of the LDAP directory containing the users and roles. Please ask your LDAP server administrator to provide you with a suitable (bind) user.

**Figure 39. Login to LDAP Server**




If the connection to the LDAP server fails, then the error message from the LDAP server is shown in the upper part of the dialog. There can be several reasons for a connection attempt to fail: the username or password could be wrong, the LDAP server URL could be wrong, or the LDAP server cannot be reached because the firewall is blocking it.

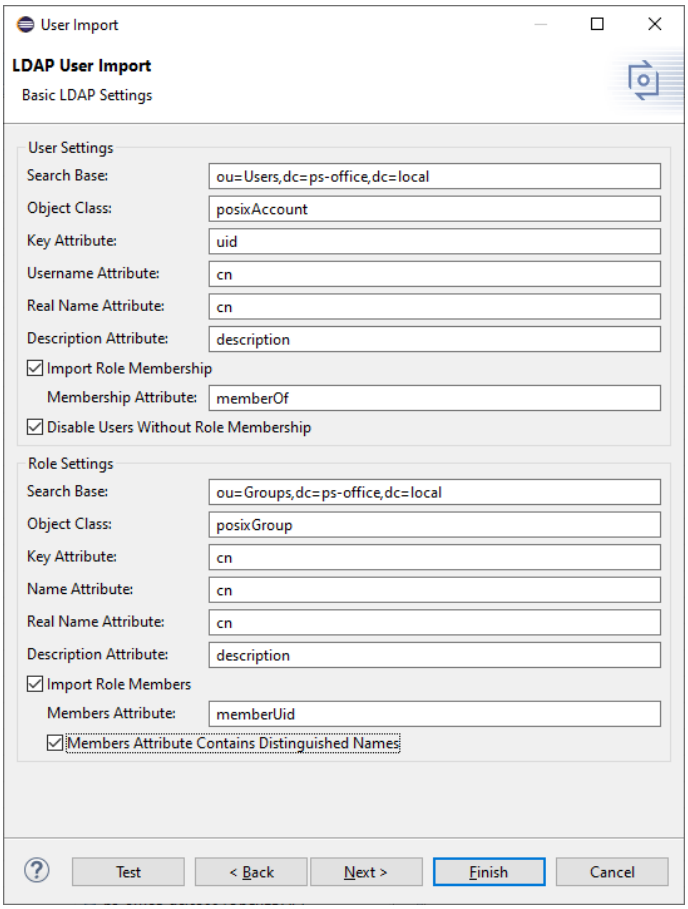
If no error is shown, the connection test succeeded.

Click “Next” to open the basic LDAP settings page.

## 4.2.2. User and Role Settings

The basic LDAP settings strongly depend on the LDAP directory server that you want to import users and roles from. Please ask your LDAP directory server administrator for the correct values.

**Figure 40. Basic LDAP Settings**



**Settings for user access:**

| | |
|---|---|
| Search Base | Distinguished name of the subtree in the LDAP directory where to start searching for users (e.g. “cn=Users,dc=company,dc=com”). The entire subtree is searched when importing users, thus it is not recommended to enter just the LDAP root here. |
| Object Class | LDAP objectclass for user entries (e.g. “user”). The objectclass is used when synchronizing users and should unambiguously identify user entries in the LDAP directory. |
| Key Attribute | LDAP attribute holding a user's LDAP key identifier. This is usually the same as the username attribute. |
| Username Attribute | LDAP attribute holding a user's login identifier, i.e. the username (e.g. “uid”). The value of this attribute will be used as the name of the imported user and thus the username you need to enter when connecting to the pure::variants model server as this user. |
| Real Name Attribute (optional) | LDAP attribute holding a user's real name (e.g. “displayName”). The real name usually is the user's firstname followed by its lastname (e.g. “John Doe”). |
| Description Attribute (optional) | LDAP attribute holding the description of a user (e.g. “description”). |
| Import Role Membership (optional) | Enable this option to also import a user's role memberships. If enabled, then the user is assigned to all roles that both exist in the pure::variants server's “User Management” and are listed in the role membership attribute of the user in the LDAP directory. If you rather want to import roles than users, then you usually should disable this option. |
| Membership Attribute (optional) | LDAP attribute holding a user's role memberships (e.g. “memberOf”). |
| Disable Users Without Role Membership (optional) | Enable this option to disable users that are not member of any role after the import. This option especially is useful when synchronizing imported roles, to automatically disable users that have been revoked from the role in the LDAP directory. |

**Settings for role access:**

| | |
|---|---|
| Search Base | Distinguished name of the subtree in the LDAP directory where to start searching for roles (e.g. “cn=groups,dc=company,dc=com”). The entire subtree is searched when importing roles, thus it is not recommended to enter just the LDAP root here. |
| Object Class | LDAP objectclass for role entries (e.g. “group”). The objectclass is used when synchronizing roles and should unambiguously identify role entries in the LDAP directory. |
| Key Attribute | LDAP attribute holding a role's LDAP key identifier. This is usually the same as the name attribute. |
| Name Attribute | LDAP attribute holding a role's name (e.g. “cn”). |
| Real Name Attribute (optional) | LDAP attribute holding a role's real name (e.g. “displayName”). |
| Description Attribute (optional) | LDAP attribute holding the description of a role (e.g. “description”). |
| Import Role Members (optional) | Enable this option to also import the users that are member of the role in the LDAP directory. If enabled, each member of the role is searched in the LDAP directory and imported as well, using the configured user's objectclass and username LDAP attributes. |

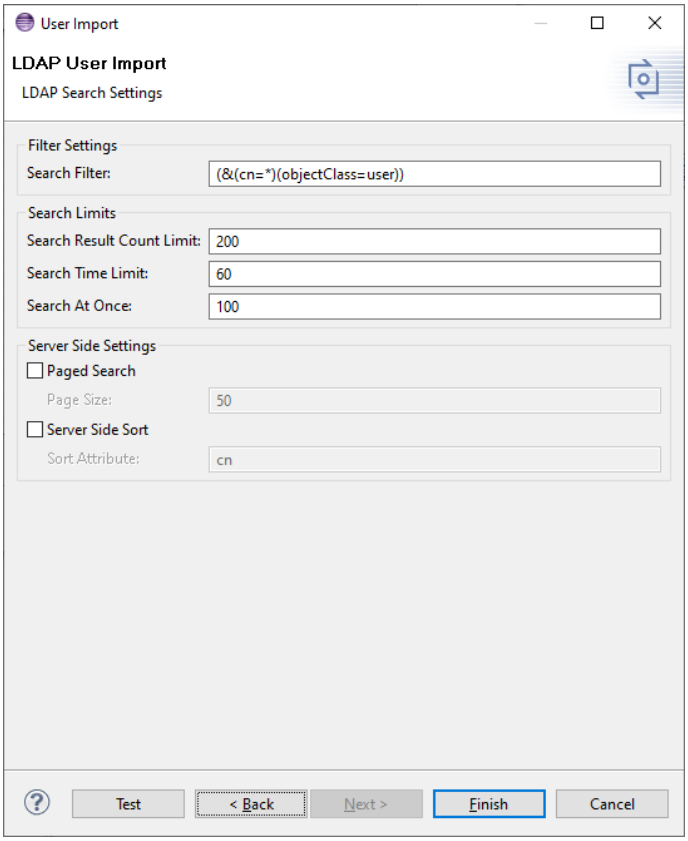
| | |
|---|---|
| Members Attribute (optional) | LDAP attribute holding a role's members list (e.g. “member”). |
| Members Attribute Contains Distinguished Names (optional) | Enable this option if the members attribute of roles in the LDAP directory lists members by their distinguished name instead of their plain username. OpenLDAP usually lists the plain usernames, whereas Active Directory usually lists members by their distinguished name. |

Click “Next” to open the LDAP search settings page.

### 4.2.3. Search Settings

On the LDAP search settings page you can usually leave all the defaults except for the search filter.

**Figure 41. LDAP Search Settings**




## Note

Please discuss the search settings with your LDAP directory administrator to ensure that the resulting search operation will not have any negative impact on the overall performance of the LDAP directory server.

If importing users or roles, a suitable LDAP search filter needs to be entered according to RFC 2254 section 4. If importing users then this filter must match users in the LDAP directory, otherwise it must match roles.

The basic syntax of an LDAP search filter is “(<*attribute*><*operator*><*value*>)”, where <*attribute*> is the name of an LDAP attribute, <*operator*> is “=” (equal to), “>=” (greater than or equal to), “<=” (less than or equal to), or “~=” (approximately equal to), and <*value*> is the expected value. The value also can contain the wildcard character “*” at the beginning or the end which is a placeholder for any text.

Single search filters can be combined to more complex search filters using the operators “&” (and), “|” (or), and “!” (not).

**Examples:**

| | |
|---|---|
| (cn=pvtest) | Matches all LDAP entries that have the value “pvtest” in the attribute “cn”. |
| (cn=pvtest*) | Matches all LDAP entries that have a value in the attribute “cn” that starts with “pvtest”. |
| (!(cn=pvtest*)) | Matches all LDAP entries that have a value in the attribute “cn” that does not start with “pvtest”. |
| (&(cn=pvtest)(objectclass=user)) | Matches all LDAP entries that have the value “pvtest” in the attribute “cn”, and the value “user” in the attribute “objectclass”. |
| (\|(cn=pvtest1)(cn=pvtest2)) | Matches all LDAP entries that have the values “pvtest1” or “pvtest2” in the attribute “cn”. |
| (&(objectclass=user)(cn=pvtest*)(!(cn=pvtest3))) | Matches all LDAP entries that have the value “user” in the attribute “objectclass”, and that have a value starting with “pvtest” in attribute “cn”, but do not have the value “pvtest3” in the attribute “cn”. |

If synchronizing users or roles, then this filter is constructed automatically using the configured user or role objectclass and username LDAP attributes.

The search operation in the LDAP directory can be limited as follows:

| | |
|---|---|
| Search Result Count Limit | Maximum number of search results (users, if searching users, and roles, if searching roles) to retrieve from the LDAP directory. This limitation strongly depends on the LDAP directory's configuration and the user used to access the LDAP directory. If you want to import more users or roles than the LDAP directory is willing to return in one search, then “Server Side Sort” may help. |
| Search Time Limit | Timeout for LDAP search operations in seconds. Increase this value if your LDAP directory needs more than a minute to deliver the matching users or roles. |
| Search At Once | Number of users to search at once when importing role members or synchronizing users. Decrease this value if your LDAP directory will not deliver that much users in one search operation. Otherwise not all users may be imported or synchronized. Value “1” means that the users are searched in the LDAP directory one after the other. This may take a lot longer than searching multiple users at once. This also may have a negative impact on the performance of the LDAP directory due to many immediately consecutive search operations if a lot of users need to be imported. |

Following LDAP server extensions are supported by pure::variants. Please ask your LDAP server administrator if any of these extensions are supported by your LDAP directory server before using them. The search operation will fail if an extension is enabled but the LDAP server does not support it.

| | |
|---|---|
| Paged Search | Enable this option to let the LDAP server return the search results paged instead of all at once, to reduce negative performance impacts of large search results on client and LDAP server side. This requires the “Simple Paged Results” control to be supported by the LDAP server. Enter the number of LDAP entries to be returned by the LDAP server per page of search results. This number must not exceed the limitation of the LDAP server for the number of search results delivered in one search operation. |
| Server Side Sort | Enable this option to let the LDAP server sort the search results by a given LDAP attribute. This requires the “Server Side Sorting” control to be supported by the LDAP server. Use this extension if you need to import more users or roles than the LDAP server is willing to return in one search operation. |

Example: If you want to import all users from the LDAP server matching filter “(&(cn=*)(objectclass=user))” and 2000 users would match (e.g. user0000 to user2000) but the LDAP server only returns 500, then you could instruct the LDAP server to sort all matches by LDAP attribute “cn”. The LDAP server then will return the first 500 users of the sorted search result set of 2000 users. To get the next 500 users you have to change the search filter to get only users with a “cn” lexically greater than the last user returned by the previous search, e.g. “(&(cn>=user500)(objectclass=user))”. Repeat this until you have imported all the users.

# 5. Access Rights

pure::variants implements a role-based authorization scheme for accessing project and model data on a pure::variants model server. This means that access rights are granted to roles instead of users. For a user to be granted access to any data on a pure::variants model server, this user has to be assigned to a correspondingly authorized role. To grant access to single users without the need to define extra roles for this purpose, each user also acts as a role with that user as the only member of that role.

If a user or role is disabled, then any access rights granted do not apply.

Following access rights can be granted:

| | |
|---|---|
| Read | Permission to read the data. |
| Change | Permission to change the data, but not to delete it. |
| Delete | Permission to delete the data. |
| Change Permission | Permission to change the access rights for the data. |

These access rights can be granted for the following data on a pure::variants model server:

| | |
|---|---|
| “Project Root” | “Read” access to “Project Root” (part of the “ADMIN” project) is required in order to get the list of projects that exist on a pure::variants model server. “Change” right is required for the ability to create new and delete existing projects on the server. |
| “User Management” | “Read” access to “User Management” (part of the “ADMIN” project) is required in order to open the pure::variants user management, and “Change” right for the ability to add, delete, or change users and roles. |
| Projects | “Read” access to a project is required in order to see and open that project. “Change” right is required for the ability to create top-level project entries (e.g. top-level folders, models, configuration spaces). To delete a project, “Delete” right must be granted for the project, and “Change” right for “Project Root”. |
| Folders | “Read” access to a folder is required in order to see and open that folder. “Change” right is required for the ability to create or delete top-level folder entries. To delete a folder, “Delete” right must be granted for the folder, and “Change” right for the parent project entry (e.g. a folder or the project itself). |
| Configuration Spaces | “Read” access to a configuration space is required in order to see and open that configuration space and the configuration space properties. “Change” right is required for the ability to create or delete variant description models, and to setup or change transformations and other configuration space settings. To delete a configuration space, “Delete” right must be granted for the configuration space, and “Change” right for the parent project entry (e.g. a folder or the project itself). |

Feature and Family Models
: “Read” access to a feature or family model is required in order to see and open that model. “Change” right is required for the ability to add constraints and restrictions, and to change model properties and the pvSCL code library. To delete a feature or family model, “Delete” right must be granted for the model, and “Change” right for the parent project entry (e.g. a folder or the project itself).

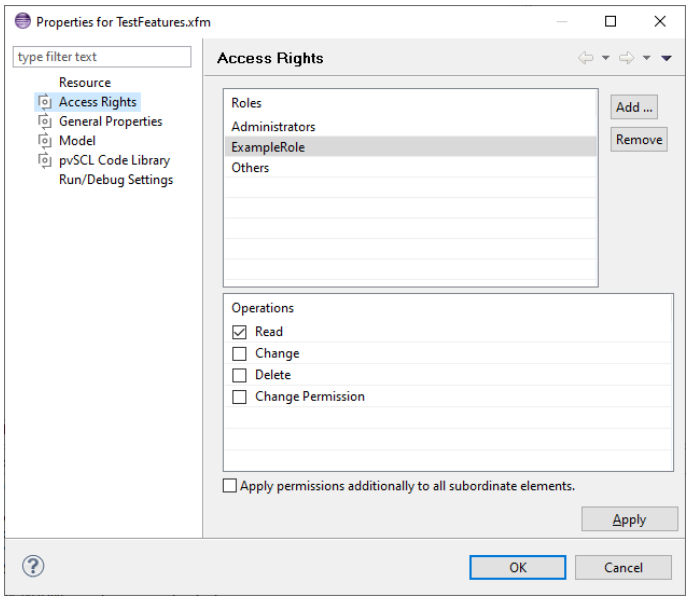
Variant Description Models
: “Read” access to a variant description model is required in order to see and open that model. “Change” right is required for the ability to make explicit changes to the selection of model elements, to set or change the value of non-fixed element attributes, and to change model properties and the inheritance hierarchy. To delete a variant description model, “Delete” right must be granted for the model, and “Change” right for the parent project entry (e.g. a folder or configuration space).

Model Elements
: “Read” access to a model element is required in order to see that element and its properties. “Change” right is required for the ability to add and delete direct children of that element, and to make changes to the element, its relations and attributes. To delete a model element, “Delete” right must be granted for the element, and “Change” right for the parent element.

If a user creates a new project, folder, configuration space, model, or model element, then this user will get full access rights on it. Other roles get the same access rights as on the parent project or model entry.

Access rights are granted or revoked using the “Access Rights” editor. To open this editor for an item (i.e. project, model, model element, etc), right-click it to open the context menu, select “Properties” and then switch to the “Access Rights” page.

**Figure 42. Access Rights Editor**




If access rights are changed without enabling the option “Apply permissions additionally to all subordinate elements”, then the previous access rights are copied to the direct children (i.e. child model elements, child project entries, etc) if they didn't have access rights set before and just inherited them from their parent. Otherwise, if this option is enabled, the new access rights are applied to the current item and all its direct and indirect children.

Each pure::variants model server initially has the following two predefined roles:

Administrators
: This role comes with “Read” right on the “ADMIN” project, and full rights on “Project Root” and the “User Management”.

| | |
|---|---|
| Others | This role comes with “Read” right on “Project Root” and the “User Management”. Thus, users with that role neither can access the “ADMIN” project nor make any changes to the “User Management”. |

A special user in all pure::variants model servers is the user named “system”.

### Note

If a user has the reserved name “system”, then this user is treated as a super user for which no access limitations exist in a pure::variants model server. Even if this user has no roles assigned, he can read, change and delete everything. It is very important to choose a strong password for this user which is provided only to the people that need to know it.

# 6. Service Logon

If the pure::variants server does not support username/password authentication and for any administrative task only username/password authentication may be possible, then the pure::variants client can be forced to use the pure::variants server's service logon. All pure::variants model servers support service logon.

Examples for situations where service logon may be required are:

- Administrative tasks shall be automated (e.g. using ANT or JavaScript) but the pure::variants server only supports interactive logon types such as OpenID authentication.
- Administrative tasks shall be performed but the pure::variants server only supports logon types that require a trusted third-party authentication service which is not accessible from the administrative network location.

In order to use service logon, there must exist a user in the pure::variants server for which a password has been set.

Service logon is forced on pure::variants client side by setting the environment variable PV_FORCE_SERVICE_LOGON to value "true". Please consult the documentation of your operating system on how to set environment variables.

You can also set this variable as a Java Virtual Machine variable directly in the Eclipse configuration file of the pure::variants client or the third-party Eclipse you installed pure::variants into. Just go to the installation directory of the pure::variants client or the third-party Eclipse application to find there a file named "eclipse.ini" (usually located in an "eclipse" sub-directory). Open this file in a text editor (this may require administrative access). If there is no line "-vmargs" in that file, add it (without the parentheses) at the end of the file on a new line. Finally add the new line "-DPV_FORCE_SERVICE_LOGON=true" at the end of the file (without the parentheses). The result could look like this:

```
...
-vmargs
-DPV_FORCE_SERVICE_LOGON=true
```

# 7. Server Command Line Options

Following list describes the command line options of the pure::variants server. Not all command line options may be available for your edition of the pure::variants server.

| | |
|---|---|
| -a, /address [ADDRESS] | Address to which the server has to be bound (default 127.0.0.1) |
| /config [FILE] | Path to the server configuration file (containing command line options line separated) |
| -d, /shutdown | Shutdown the server after the last session has been closed |
| /disablehistory | Disable the model history |
| /domain [DOMAIN] | The used domain for system logon |

| | |
|---|---|
| -E, /prolog [PATH] | Path to the Prolog interpreter executable |
| /enableweb | Enable HTTP Web access |
| -h, /help | Show the command line help |
| -i, /info | Print server information as XML |
| /install | Install the server as Windows service |
| -l, /logfile [FILE] | File for server logging output |
| -L, /loglevel [LEVEL] | Level for server logging (0-9) |
| /ldapsysuser [USER] | LDAP user mapped to 'system' user (full distinguished name) |
| /ldapuidattr [UID ATTRIBUTE] | LDAP username attribute of users (e.g. uid, or cn) |
| /ldapurl [URL] | LDAP server URL (ldap://server:port or ldaps://server:port) |
| /ldapusersdn [USERS DN] | LDAP users branch distinguished name |
| /license [PATH] | Path to the server license or license pool |
| /licenselog | Enable License Server logging |
| /licenseuserlist [PATH] | Path to the file containing allowed/denied users for License Server |
| /licenseuserlog | Enable License Server logging including full user data |
| /logon [LOGON TYPES] | Enable server logon types, comma separated (defaults to local) |
| /odbcdsn [NAME] | Name of ODBC connection |
| /odbcpwd [PASSWORD] | Password for ODBC connection |
| /odbcuid [UID] | User id for ODBC connection |
| -p, /port [PORT] | Port on which the server has to listen |
| -P, /plugindir [PATH] | Semi-colon separated list of additional plugin directories |
| /printinfo | Print server information as XML and exit |
| /projectsdata [PATH] | Path to the local project data directory |
| -r, /rmlog | Remove old server log file on startup |
| -R, /plprog [PATH] | Path to the Prolog resource data executable |
| /remove | Remove the server as Windows service |
| -S, /xsltdir [PATH] | Path to the XSLT scripts directory |
| /service | Start the server as Windows service |
| /servicedesc [DESCRIPTION] | Description of the Windows service to install |
| /servicename [NAME] | Name of Windows service to install or remove |
| /sslcacert [PATH] | Path to the file containing trusted certificates |
| /ssldh [PATH] | Path to the Diffie-Hellmann parameters file for key exchange |

| | |
|---|---|
| /sslkeyfile [PATH] | Path to the server's SSL key file |
| /sslpassword | Password of the server's SSL key file |
| -t, /clienttimeout [SECONDS] | Timeout in seconds before killing a dead client connection (defaults to 15 minutes) |
| -w, /writeinfo | Write server information as XML |
| /webpwd [PASSWORD] | Password of the HTTP Web access |

## Note

The prefix of the long names of the command line options differ for Linux and Windows (“--” on Linux and “/” on Windows).