
pure::variants Server Administration Manual

pure-systems GmbH

Version 4.0.15.685 for pure::variants 4.0

Copyright © 2003-2018 pure-systems GmbH

2018

Table of Contents

1. Introduction	1
2. Import Administration Project	1
3. Manage Users and Roles	3
3.1. Create Users and Roles	4
3.2. Modify Users and Roles	5
3.3. Change User Passwords	5
3.4. Change assigned Roles for a User	5
3.5. Delete Users and Roles	6
3.6. Import and Synchronize User Data	6
4. Server Command Line Options	11

1. Introduction

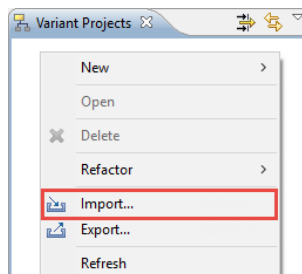
The pure::variants Server Administration allows the administration of the users and roles for a pure::variants model server. It provides an editor to create/delete/modify/import users and roles and assign users to roles and vice versa. These operations require administrative access rights. The access to the user management data of the pure::variants model server is realized by the special administration project "ADMIN".

A printable version of this document is [available](#).

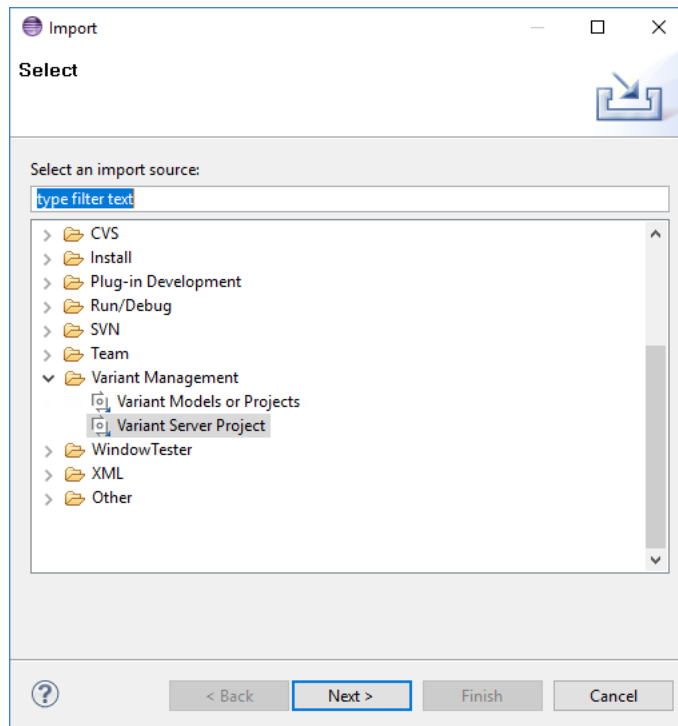
2. Import Administration Project

To import the administration project (ADMIN) of a pure::variants model server, right-click in the "Variant Projects" view and select "Import..." from the context menu.

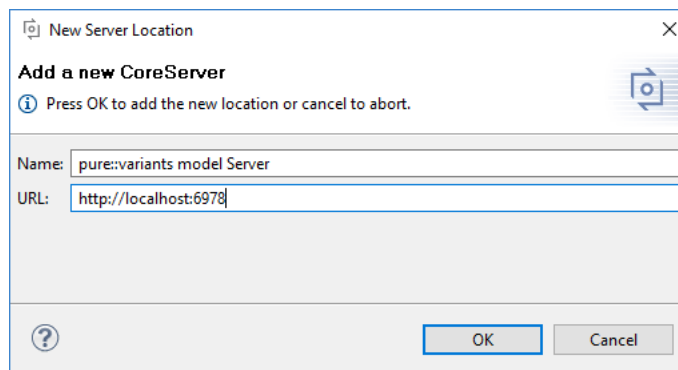
Figure 1. Import from Context Menu



Select "Variant Server Project" item from the list and click "Next".

Figure 2. Import Variant Server Project

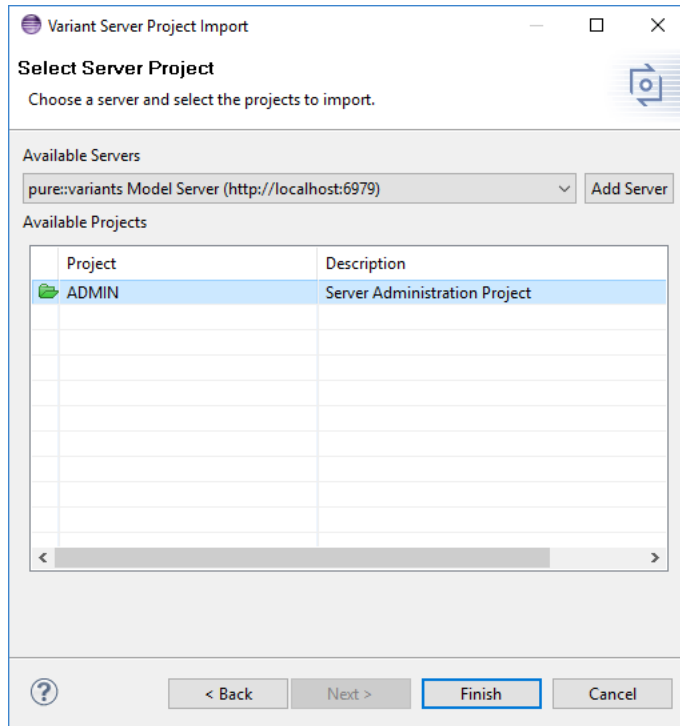
The next wizard page contains a combo box with all “Available Servers”. You can choose one of them and after selection a connection is opened to the selected server. If you cannot see the server you want to administrate in the list, click the “Add server” button. A dialog pops up which allows you to enter a short description of the server and its url in the form “http://servername:port” or “https://servername:port”.

Figure 3. Add a new pure::variants Model Server

After entering the values of the server, click “OK”. If the values are correct and the server is running, a login dialog pops up. If the server was started the first time after installation, only the build-in user "system" exists and has to be used to log into the server. This user has a predefined password and **MUST BE CHANGED** immediately after starting up the server the first time (all pure::variants Server installations share this initial password). Keeping this password renders the server insecure. Please see the "pure::variants Server Quick Installation Guide" for the password.

After authentication was successful, a list of all projects for the selected server is shown in the dialog. You are not allowed to import projects with red (lock) icons because you don't have permissions on them. If the “ADMIN” project has a green (folder) icon, select it and click “Finish” (otherwise contact the server administrator).

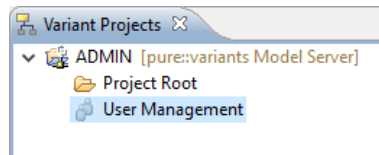
Figure 4. pure::variants Model Server and Project Selection Page



3. Manage Users and Roles

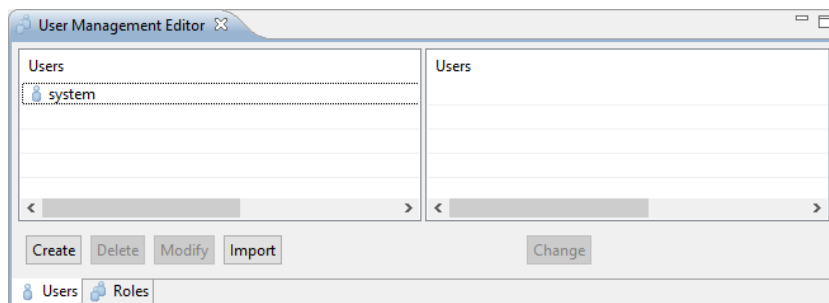
To manage users and roles double-click the “User Management” item in the “ADMIN” project.

Figure 5. Open User Management

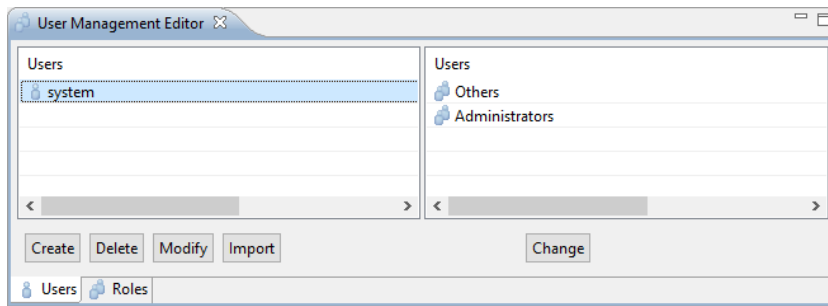


The “User Management” editor opens and shows all available users in the left table. Initially after installation there is only one user. This is the build-in user "system".

Figure 6. “UserManagement” Editor

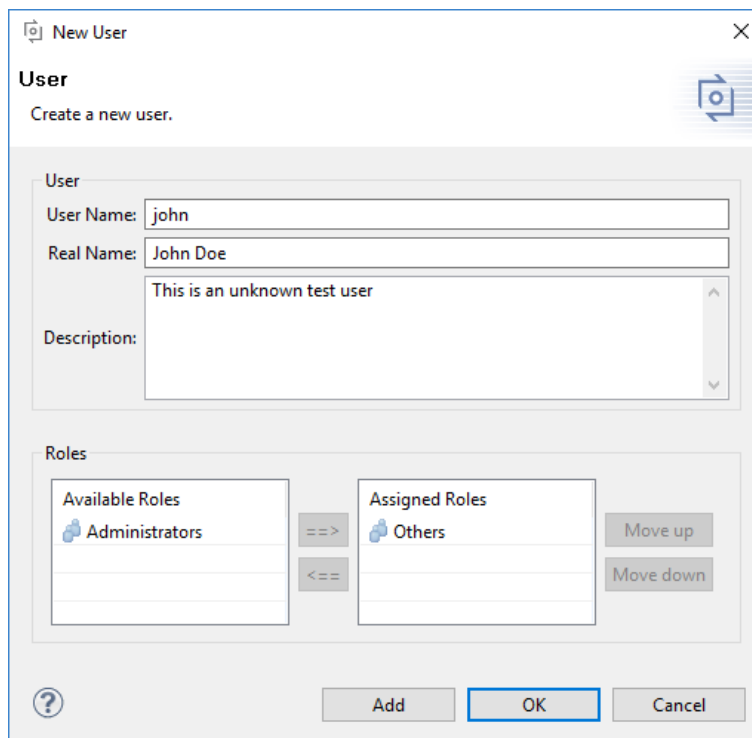


If you select a user in the table, the right table shows all roles assigned to this user. Initially there are two roles named “Administrators” and “Others”.

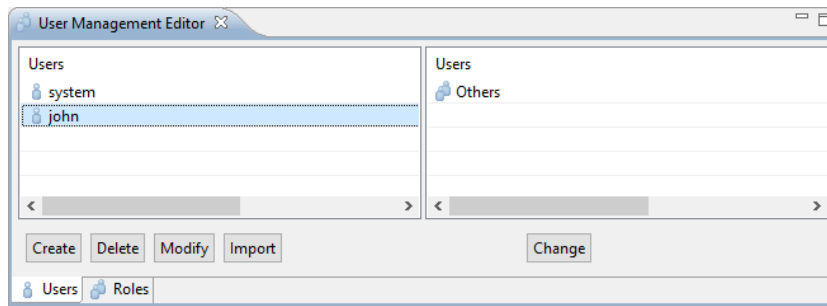
Figure 7. Selected User

3.1. Create Users and Roles

To create a new user click the “Create” button on the lower left of the editor. A dialog pops up where you can enter the 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 the user to a role by selecting the role on the left side and click the “==>” button, or simply by double-clicking on a 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 on the role.

Figure 8. Create a new User

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

Figure 9. New created User

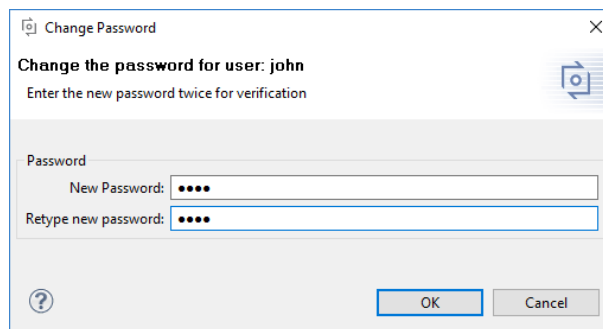
Creating a role works the same way like creating a user. You only have to select the “Roles” tab on the lower left part of the editor.

3.2. Modify Users and Roles

To modify a user select the user in the left table of the editor and click the “Modify” button (or double-click the user). The modification dialog opens which is the same dialog as for creating users. Clicking the "OK" button applies the modifications for the selected user.

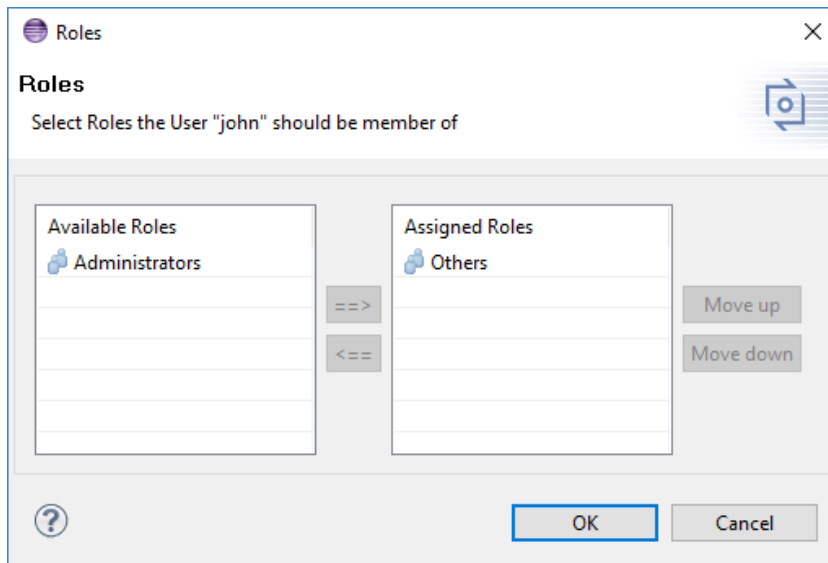
3.3. Change User Passwords

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 10. Change User Password

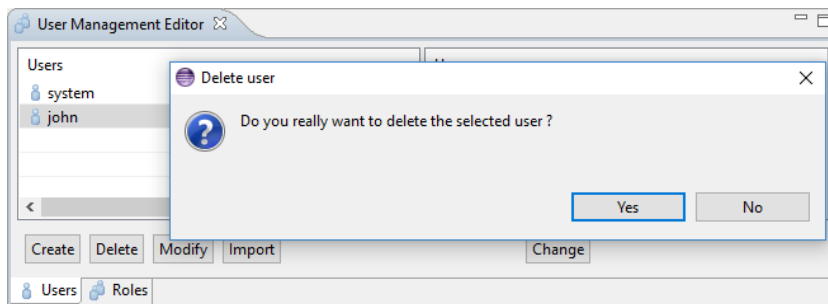
3.4. Change assigned Roles for a User

To change the assigned roles of a user, select the user in the left table of the "User Management" editor and click the “Change” button below the role list. The role assignment 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 11. Role Assignment Dialog

3.5. Delete Users and Roles

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

Figure 12. Delete Dialog

Note

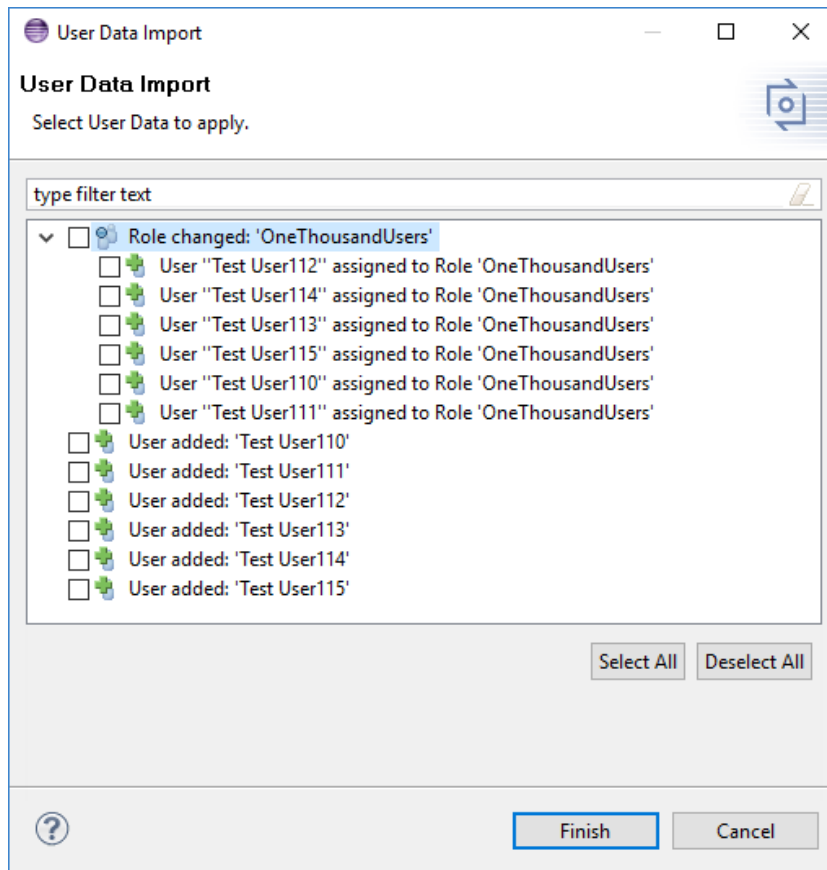
For the correct function of the clients the user management information has to be readable by all users.

3.6. Import and Synchronize User Data

pure::variants supports the import of external user data. It is possible to import users, roles, and role assignments. To import user data click the "Import" button below the left table of the "User Management" editor, or select and right-click the users and roles in the "User Management" editor and choose "Synchronize" from the context menu. On the "Users" tab a user import is performed. On the "Roles" tab a role import is performed. A "User Data Import" wizard opens up and allows the administrator to define the import settings.

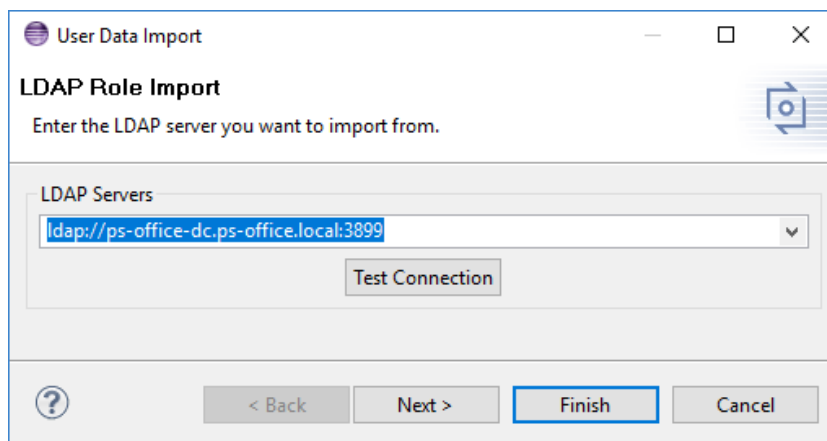
Currently LDAP is supported as external user data source. See [the section called “Import User Data from LDAP”](#).

After finishing the "User Data Import" wizard the import is performed and the result is presented in another dialog. The administrator has to select the user data which shall be imported to the "User Management" project. After finishing the dialog the user data is applied.

Figure 13. User Import Result Page

Import User Data from LDAP

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

Figure 14. LDAP Server Settings Page

The connection to the LDAP server can be tested by clicking button "Test Connection". This will open a login dialog where you have to enter the LDAP bind-user and password. The bind-user usually needs to be entered with its full distinguished name (e.g. "uid=username,cn=users,dc=company,dc=com").

To change the used LDAP bind-user and password, just click the "Test Connection" button again.

The next wizard page allows to enter the LDAP directory specific settings for accessing the user and role data.

Note

Please ask your LDAP directory administrator for the correct settings for your LDAP directory.

Figure 15. LDAP Basic Settings Page

The screenshot shows a window titled "User Data Import" with a sub-header "LDAP Role Import" and "Basic LDAP Settings".

User Settings:

- Search Base:
- Object Class:
- Username Attribute:
- Real Name Attribute:
- Description Attribute:
- Import Role Membership
 - Membership Attribute:
- Delete Users Without Role Membership

Role Settings:

- Search Base:
- Object Class:
- Name Attribute:
- Real Name Attribute:
- Description Attribute:
- Import Role Members
 - Members Attribute:
 - Members Attribute Contains Distinguished Names

At the bottom, there is a help icon (?), and four buttons: "< Back", "Next >", "Finish", and "Cancel".

Following settings are required to access user data in the LDAP directory.

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.
Username Attribute	LDAP attribute holding a user's login identifier, i.e. the username (e.g. "uid"). Only latin letters, digits, and underlines are allowed in a username.
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.
Description Attribute (optional)	LDAP attribute holding the description of a user (e.g. "description").

Import Role Membership (optional)	Enable 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.
Membership Attribute (optional)	LDAP attribute holding a user's role memberships (e.g. "memberOf").
Delete Users Without Role Membership (optional)	Enable to delete users not member of any role after the import. This option especially is useful when synchronizing imported roles, to automatically cleanup users that have been revoked from the role in the LDAP directory.

Following settings are required to access role data in the LDAP directory.

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.
Name Attribute	LDAP attribute holding a role's name (e.g. "cn"). Only latin letters, digits, and underlines are allowed in a role's name.
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 to also import the users that are member of the role. If enabled, each member of the role is searched in the LDAP directory and imported as well, using the configured user 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 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.

On the final wizard page the LDAP search operation is set up. You can leave all the defaults except for the search filter.

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.

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.

If synchronizing users or roles, then this filter is constructed automatically using the configured user or role objectclass and name LDAP attributes. It is not possible to enter a search filter in this case.

Figure 16. LDAP Search Settings Page

The screenshot shows a window titled "User Data Import" with a subtitle "LDAP Role Import" and a main heading "LDAP Search Settings". The window is divided into three main sections:

- Filter Settings:** A "Search Filter" field containing the text "cn=OneThousandUsers".
- Search Limits:** Three input fields: "Search Result Count Limit" with the value "200", "Search Time Limit" with the value "60", and "Search At Once" with the value "100".
- Server Side Settings:** Two checkboxes, "Paged Search" and "Server Side Sort", both of which are unchecked. Below each checkbox is an empty input field for "Page Size" and "Sort Attribute" respectively.

At the bottom of the window, there is a navigation bar with four buttons: a help icon (?), "< Back", "Next >", and "Finish" (which is highlighted with a blue border). A "Cancel" button is also present to the right of "Finish".

Following search limits can be configured.

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 bind 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 searched.

Following LDAP server extensions are supported.

Note

The LDAP server has to support these extensions in order to use them. Please ask your LDAP administrator if these extensions are supported before using them. The search operation will fail if an extension is enabled but the LDAP server does not support it.

Paged Search	Enable 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	<p>Enable 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.</p> <p>Example: If you want to import all users from the LDAP server matching filter "(&(uid=*)(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 "uid". 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 "uid" lexicographically greater than the last user returned by the previous search, e.g. "(&(uid>=user500)(objectclass=user))". Repeat this until you could import all the users.</p>

4. 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
/sslcert [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).