




ix USER MANAGER



UNITED PLANET INTREXX XTREME
RELEASE 4.5







Table of Contents

1. Introduction	4
2. Schemes Manager	5
2.1. Object Class	5
2.2. User Class	5
2.3. Container Class	5
2.4. Set Class	6
2.5. Creating a New Class	6
3. Creating an Object	8
4. Filtering Lists	13
5. Context Menu	14
5.1. Properties	14
5.2. Move	14
5.3. Permissions	15
5.4. Delete	15
5.5. Change Password	15
5.6. Generate Password	15
5.7. Lock / Unlock Account	15
6. User / Permissions Menu	15
7. Importing Users and Groups	15
7.1. LDAP Sources	16
7.2. JDBC Sources	21
7.3. Text Sources	21
8. Configuration	22
8.1. Authentication	22
8.1.1. Authentication via Web Server	22
8.1.2. Intrex Authentication	22
8.1.3. Generic Authentication	23
8.1.4. Other Authentication	23
8.2. Security	23
8.3. Organization	23

Writing Conventions

In this handbook, text passages will be displayed in *italics* when they refer to settings in the displayed dialogs. Menu items that are available in context menus can, in addition, always be selected from the main menu. Main menu items will not be described if they are not available in the context menu. A description of the general main menu items can be found in the  *Center* handbook. Programming code in the text will be displayed in the Courier font. Context menus can be opened by clicking with the right mouse button on the described element.

In the following, *<xtreme>* refers to your Intrex installation path; under Windows, for example, this is usually  *C:\xtreme*. On Linux, the normal install path is  */opt/xtreme/*. The following symbols will be used for designation of special kinds of information:

-  Important information
-  Tips and background information
-  References to additional information in an Intrex Xtreme handbook
-  Directories
-  URLs
-  Buttons in dialogs or assistants

Previous Knowledge

For this handbook, you require no special training. You can find helpful information in the Intrex Xtreme handbooks  *Center* and  *Permissions*.

1. **Introduction**

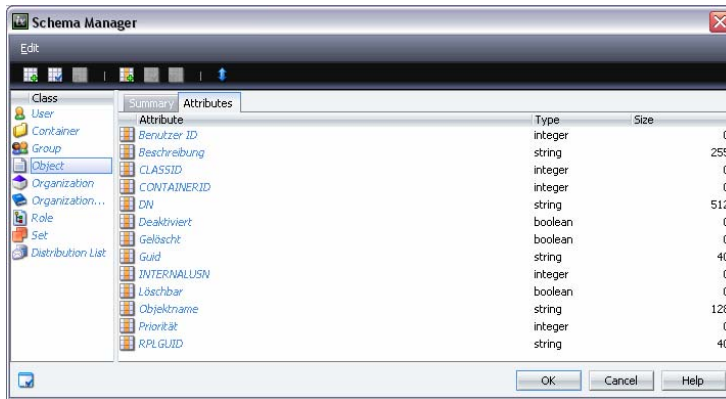
In the *User Manager* module, all user accounts of a portal will be administrated on an object-oriented basis. The objects can be saved in a hierarchical structure that represents your organization. This makes a very flexible data model available to you, which can be expanded for the definition of individualized object classes.

In a newly created portal, object classes will be automatically defined with mandatory attributes, such as the *User* object class with the mandatory attributes *First Name* and *Last Name*. This class possesses a number of attributes, with which a user can be described.

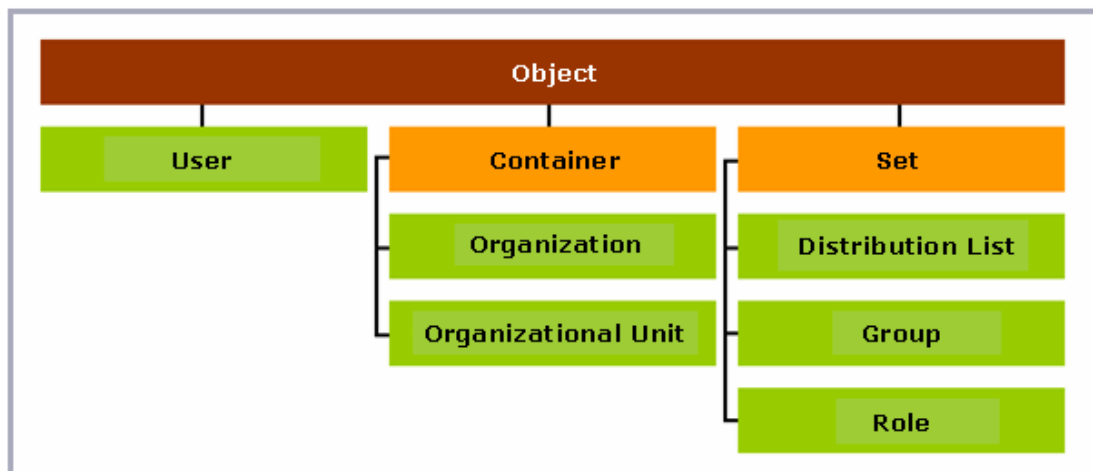
For every attribute there exists a database field, in which the values that you will enter for an object instance will be saved. You may define an unlimited number of additional attributes for an object class; however, the mandatory attributes of a class may not be changed.

Objects (such as a portal user based on the *Users* class) will be created based on object classes. Object classes can be viewed as a type of template for the objects. The specific values of an object will be saved in the attributes.

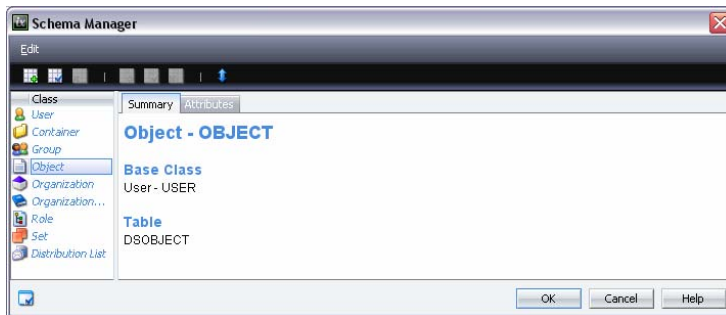
In the Schemes Manager, which you can reach from the menu *Users / Schemes Manager*, you will see the standard object classes of the Intrexx Xtreme User Manager.



The object classes *Object*, *Container*, and *Set* are so-called basic classes. Their attributes will be inherited by the classes that are created from them. So, for example, the *User* class also possesses attributes of the basic class *Object*, from which it is based, in addition to its own attributes. In the following image you will see a diagram of the object class hierarchy in the Intrexx Xtreme User Manager.



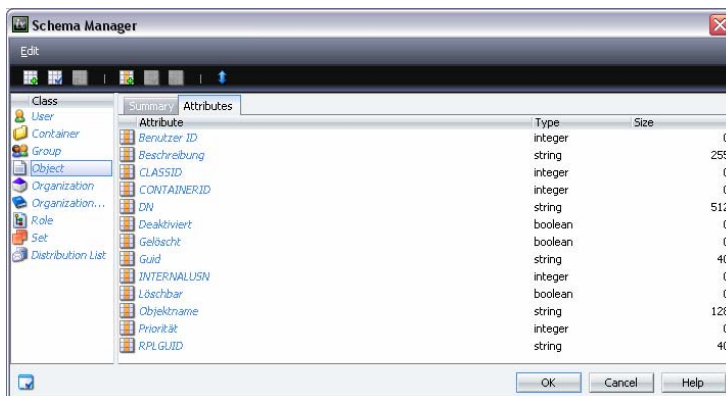
2. Schemes Manager



In the left-hand area of the Schemes Manager, you will see all default object classes and classes that you have defined yourself. Default object classes will be shown with the name colored blue and in italics, and user-defined classes will be shown as normal black text. Mandatory and user-defined attributes will also be differentiated from one another in this way.

For program-internal reasons, default object classes and attributes cannot be deleted or changed.

On the *General* tab, the name of the object class, the basis class, and the name of the database table of the values that were entered for the objects in the currently selected class will be displayed. On the *Attributes* tab, you will see all attributes of the currently selected object class.



2.1. Object Class

This class is the basic class for all object classes in the User Manager. Therefore, all other object classes possess all attributes of the *Object* class.

2.2. User Class

This class is directly derived from the basic class *Object* and represents the individual users of the portal.

2.3. Container Class

This class is the basic class of the object classes:

- **Organization**
For objects that represent an organization or a business
- **Organizational Unit**
For objects that represent organizational units

With objects of these classes, other objects can be grouped in a 1:n relationship. This means, for example, that *Guitarstore* as an *Organization* object may contain the

Management organizational unit. The organizational unit *Management* can, as long as it is contained in the *Guitarstore* organization, not be assigned to a second organizational unit. Likewise, for example, each employee (*Users* object) may only be assigned to one organization, one organizational unit, or one role.

2.4. Set Class

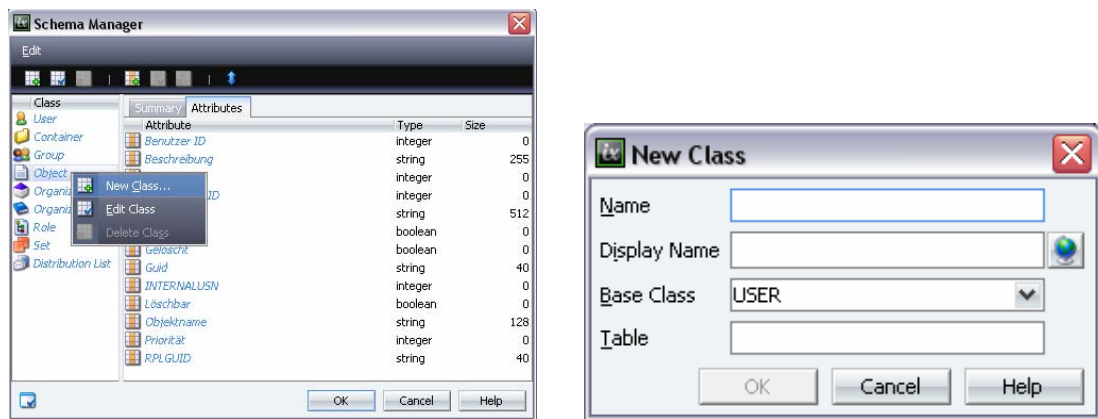
This class is the basic class of the object classes

- **Distribution List**
For objects that represent a distribution list
- **Group**
For objects that represent a user group
- **Role**
For objects that describe specific roles in an organization

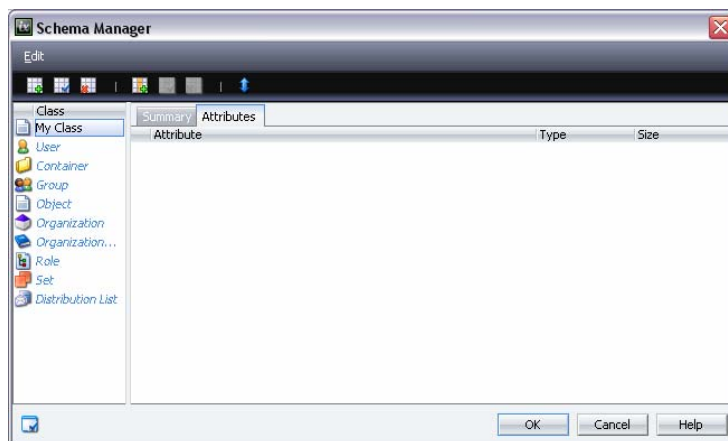
With the *Set* class, a m:n relationship can be created. This means, for example, a user may be both a member of the group object *Press* as well as the group object *Partners*.

2.5. Creating a New Class

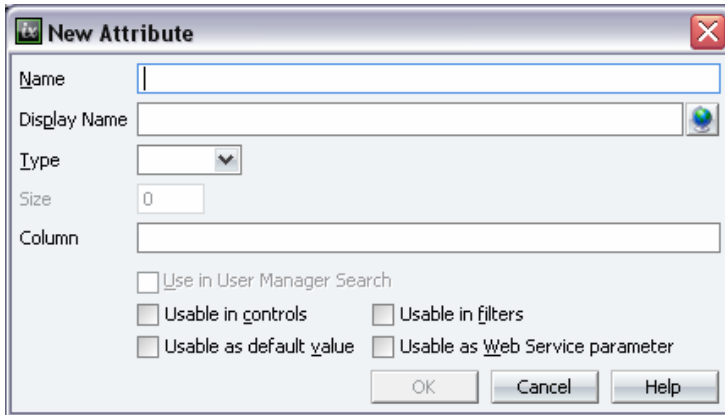
In the Schemes Manager, you have the ability to define your own object classes. Existing classes can be used as basic classes here.



New classes can be created via the context menu item *New Class* in the left-hand area of the schemes manager, or from *New Class* in the toolbar of the Schemes Manager. Enter the *Name* of the new class. The *Display Name* will be used when displaying the class in the Schemes Manager. Select the *Basic Class* from the selection list. Additionally, a table name must be entered, which will be used for the database table underlying the class, in which the attribute values entered will be saved.



The new, self-defined class will be displayed in black, non-italic script. It is not a mandatory class and can be further edited or deleted. With the context menu item *New attribute*, new attributes can be defined on the *General* tab, which will likewise not be entered as mandatory attributes. You can reach this context menu by clicking with the right mouse button in an empty area of the *Attributes* tab.




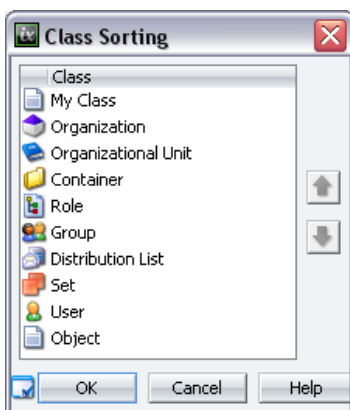
The *Name* that you enter here must be unique. It will be applied systemwide. The *Display Name* will be used when the attribute is applied to controls, filters, and its display in the User Manager.


Select the desired data type in the list *Type*.

In *Size*, the maximum length of characters for text attributes can be defined. In *Column*, the name of the database field, in which the values of the attribute will be saved, will be defined.

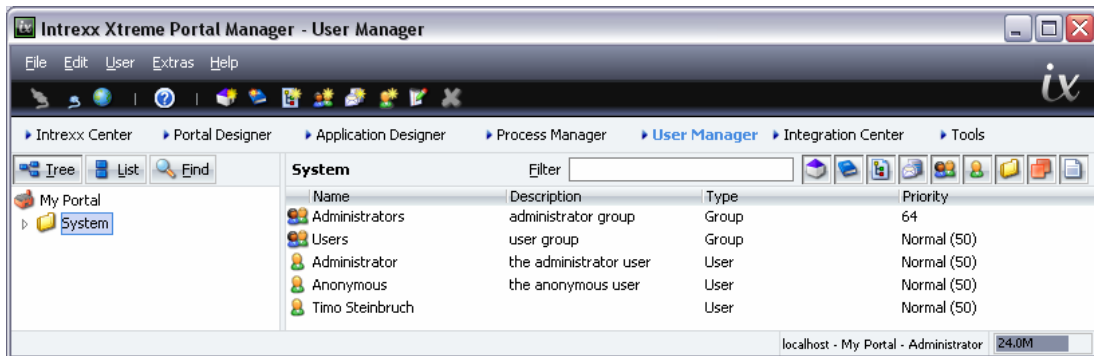
The setting to *Use in User Manager search* allows an attribute to be added to the search in the User Manager. The attribute can be used with the setting *Usable in controls* in Application Designer elements, such as the entries in the view table or the selection list. The setting to *Useable in filters* allows the attribute to be used in filter definitions. *Usable as default value* allows an attribute to be used as default value in edit elements. *Usable as Web Service parameter* allows the attribute to be used in web services (see Handbook [Web Services](#)).

In the *Edit* menu or in the toolbar of the Schemes Manager, you will find the  *Classes Sorting* tool.

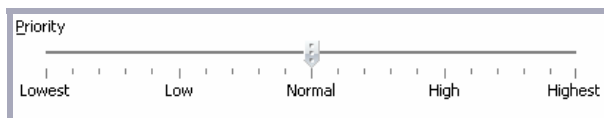


The sorting order for the display of objects, such as in the lists view in the left-hand area of the User Manager, can be defined here. To do so, bring the objects into the desired order with the help of the  arrow buttons.

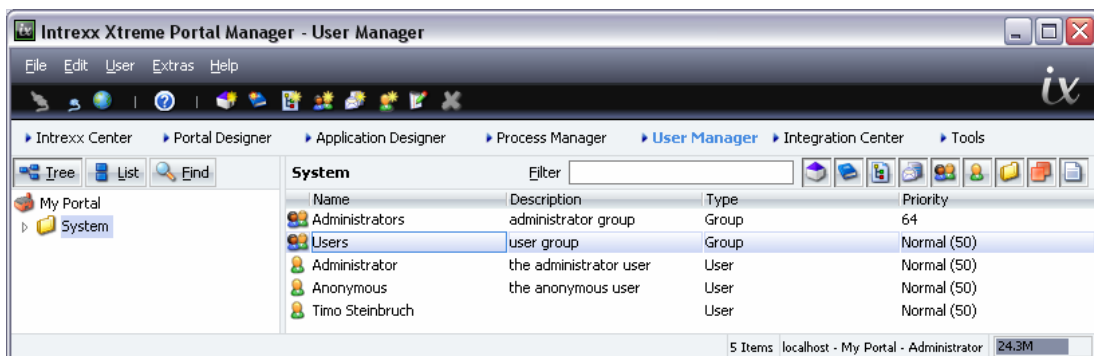
3. Creating an Object



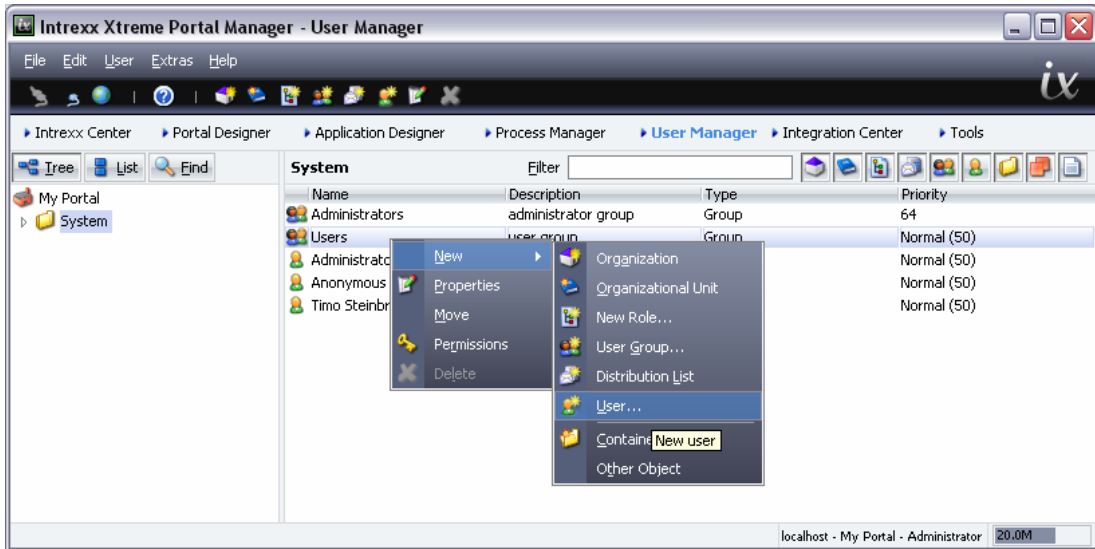
In the left-hand area, you will see a representation of the portal structure in tree format. For a newly created portal, you will see only the portal node and the subordinate folder *system* here. If the portal node is highlighted, all subordinate objects will be listed in the right-hand area of the User Manager. There you will be informed of the *Name* of the object, its *Description*, the *Type*, and its *Priority*. In the *Type* column, you will find the object class to which it belongs.



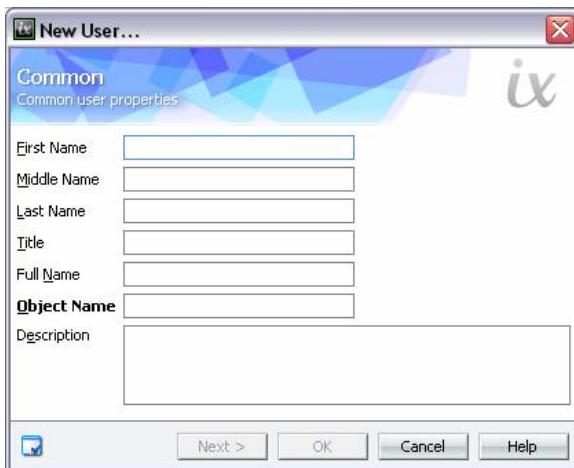
The priority can be set for the majority of objects, which controls the order in which they will be shown in lists in the User Manager.




The *system* folder is a container object. If you highlight this folder, all objects contained within it will be listed.




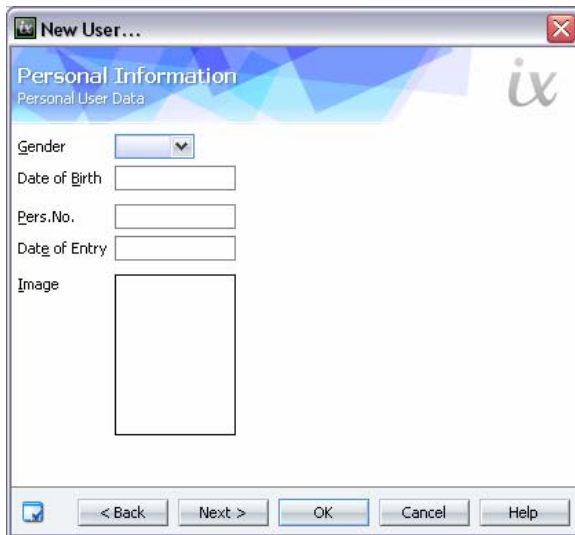
A new object can be created in the left-hand area, as well as in the right-hand area via the context menu item *New*. In the following, you will be lead through the creation of a new object based on the example of the *User* object. When creating an object, the standard attributes of the object will already be inserted into edit fields in the assistants that lead you through the creation process.




Enter the general data for the user here. The *Full Name* and the *Object Name* will be automatically created from the first name and last name entered. Click  *Next* to continue.

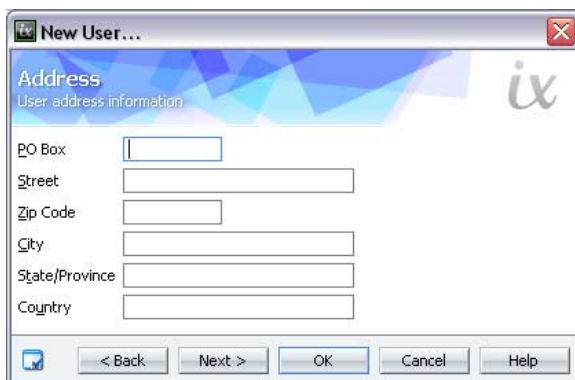


Here you can enter the *User Name*, the *Domain* and the *Password* with *Password Confirmation*. If the setting to *Disable Account* is activated, the user will no longer be able to log onto the portal. Click  *Next* to continue.




The screenshot shows a dialog box titled "New User..." with a close button (X) in the top right corner. The main heading is "Personal Information" with the subtitle "Personal User Data" and the Intrex logo (ix) on the right. The form contains the following fields: "Gender" (a dropdown menu), "Date of Birth" (a text box), "Pers.No." (a text box), "Date of Entry" (a text box), and "Image" (a large empty rectangular area). At the bottom, there are five buttons: a checkmark icon, "< Back", "Next >", "OK", "Cancel", and "Help".

Personal information will be entered here. If you wish to include an image of the user, simply click within the borders of the area intended for it. A dialog will be opened that will allow you to select an image file from your network directories. Click  *Next* when you are done.



The screenshot shows the same "New User..." dialog box, but with the "Address" tab selected. The subtitle is "User address information" and the Intrex logo (ix) is on the right. The form contains the following fields: "PO Box" (a text box), "Street" (a text box), "Zip Code" (a text box), "City" (a text box), "State/Province" (a text box), and "Country" (a text box). At the bottom, there are five buttons: a checkmark icon, "< Back", "Next >", "OK", "Cancel", and "Help".

The address data for the new user will be entered on this page. After entering these details, click  *Next*.

New User...

Contact
Contact Information on User

Telephone

Office Phone Number

Office Mobile Number

Private Phone Number

Private Mobile Number

Facsimile

Pager

eMail

Office eMail-Address

Private eMail-Address

< Back Next > OK Cancel Help

The contact data for the user will be entered here.

New User...

Organization
Organizational Properties

Superior

Deputy

Time Zone: Europe/Berlin

Default Language: Default Language

Default Layout: portal defaultlayout

Priority: Lowest Low Normal High Highest

< Back Next > OK Cancel Help

On this page, the *Manager* of the user can be selected from the list of all users using the magnifier symbol.

Select Superior

Please select the desired entry.

Filter

Name	Description	Path
Administrators	administrator group	System/Administrators
Users	user group	System/Users
Administrator	the administrator user	System/Administrator
Anonymous	the anonymous user	System/Anonymous

OK Cancel Help

With a larger number of users, you can restrict this list with the help of the easy-to-use filter (see chapter *Filtering Lists*). After making your selection, click **OK**.

New User...

Organization
Organizational Properties

ix

Superior

Deputy

Time Zone: Europe/Berlin

Default Language: Default Language

Default Layout: portal defaultlayout

Priority: (Lowest, Low, Normal, High, Highest)

< Back Next > OK Cancel Help

On this page the *Superior* of the user can be selected from the list of all users by clicking the magnify symbol. A *Deputy* can be entered in the same way. In the *Time Zone* selection list the user-specific time zone, used for displaying date and time in the portal, can be selected (see handbook *Multilingual Portals*).

In the *Default Language* selection list, the language that will be loaded in the browser for this user can be defined. The selection of *Default Portal Setting* will load the portal with the language that has been defined as default language in the country settings.

The portal layout that should be displayed upon loading the portal will be selected in the following selection list (see handbook *Portal Designer*).

Underneath, you have the ability to set the priority. The priority influences the order of lists in the User Manager. The higher the priority is set for an object, the further up it will be displayed in the list.

New User...

External Logins
External Login Information (such as ERP systems)

ix

Login 1 Password

Login 2 Password

Login 3 Password

< Back Next > OK Cancel Help

External login information for third-party systems can be entered here.

New User...

More Attributes
Values of additional attributes

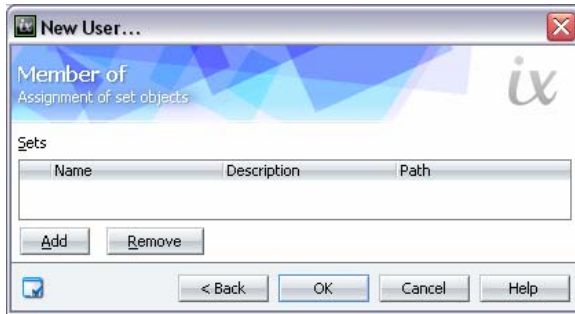
ix

Attribute	Type	Size	Value

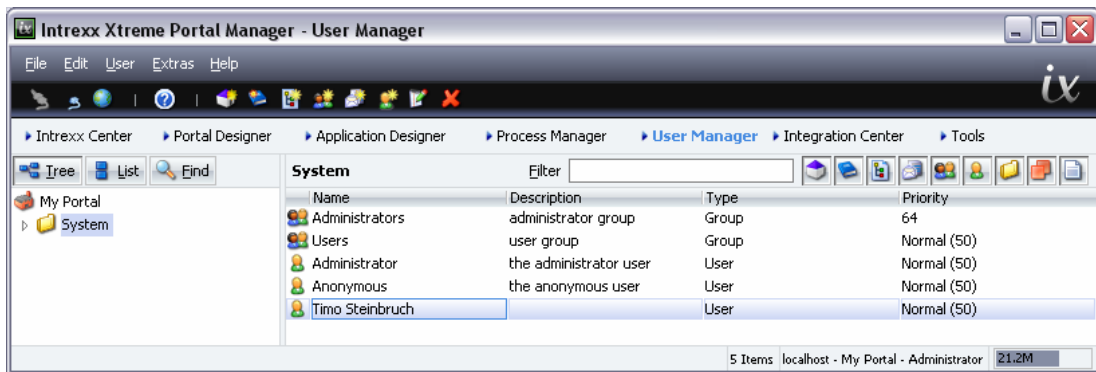
Hint: New attributes can be defined via the schema manager.

< Back Next > OK Cancel Help

If additional attributes have been entered for the *Users* object class in the Schemes Manager, they will be shown here and can be filled with values (see chapter 3 – *Schemes Manager*).

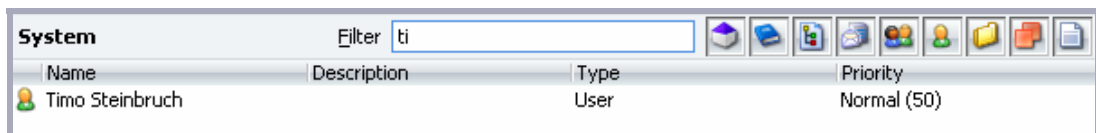


A user can be defined as a member of other objects. ➡ *Add* will open an additional dialog, from which the object can be selected. Clicking ➡ *OK* completes the creation process and saves all entries.



The new user will now be shown in the objects list in the right-hand area of the User Manager.



4. Filtering Lists



In the User Manager, you will have in various places the ability to restrict lists with a filter, which is very helpful with comprehensive lists. The *Filter* search field is available to you for this purpose, which allows you to enter and search for a desired character string. The search takes place in a lexicographic fashion and automatically restricts the results for each character that you enter. So for example, for the *t* search term, all objects will be found whose name contains a *t*. The search term *ti* lists all objects whose name contains the character string *ti*. The results will be continuously additionally restricted in the same manner.

Additionally, you can restrict the search with buttons, such as by

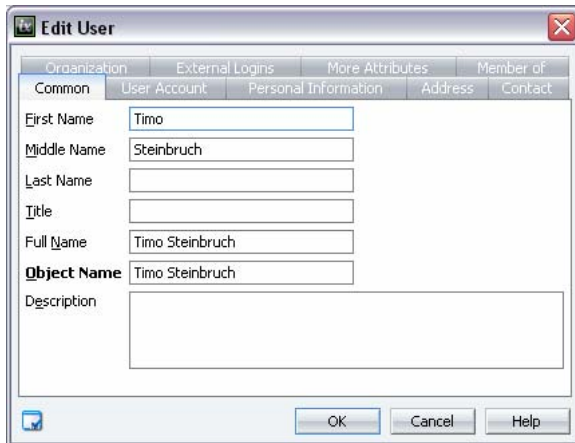
- Organizations
- Organizational units
- Roles
- Distribution lists
- User groups
- Users
- Additional container types

-  Additional grouping types
-  All other permitted types

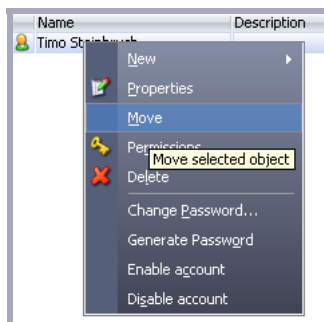
5. Context Menu

5.1. Properties

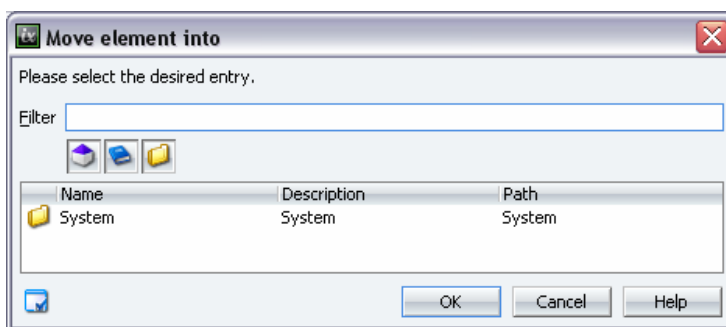
The context menu item *Properties* allows you to reach the attributes of an object, where you can change their values.



5.2. Move




Selecting the context menu item *Move* will open a dialog that will help you to move objects within the hierarchy. This allows you, for example, to move a user to another organizational unit or a container.



All existing objects that are permissible targets in the portal will be shown here. Simply select the desired object and confirm with  *OK*.

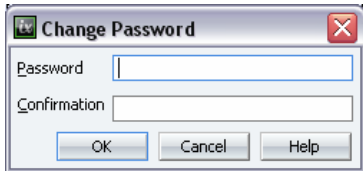
5.3. Permissions

All information on permissions holders can be found in the  *Permissions* handbook.

5.4. Delete

The context menu item *Delete* will delete an existing object. The context menu items described below are only available for the *User* object type.

5.5. Change Password



A user's password can be changed here. Enter the new password and its repetition into the corresponding edit fields.


5.6. Generate Password

This context menu item will automatically generate a password for the user and send it via eMail.

5.7. Lock / Unlock Account

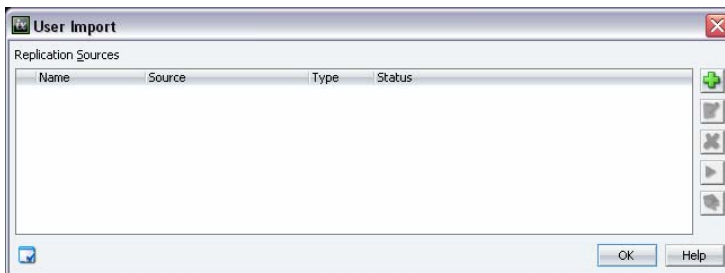
These context menu items allow a user account to be completely deactivated or activated. A user attempting to log in to the portal with a locked account will be automatically rejected.


6. User / Permissions Menu

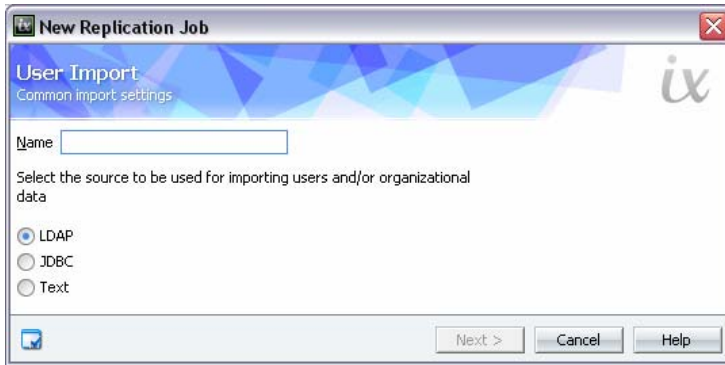
All information on permissions holders can be found in the  *Permissions* handbook.

7. Importing Users and Groups

There are multiple methods in Intrex Xtreme to import users from your existing IT infrastructure. The User Manager supports you with the import assistant when importing data from LDAP directories (such as *Windows Active Directory*), JDBC-sources and ASCII files (such as *Linux/Unix Passwd*). For the import, select the menu item *Users / Users and Groups Import*.



Select  *Add* to create a new replication source.

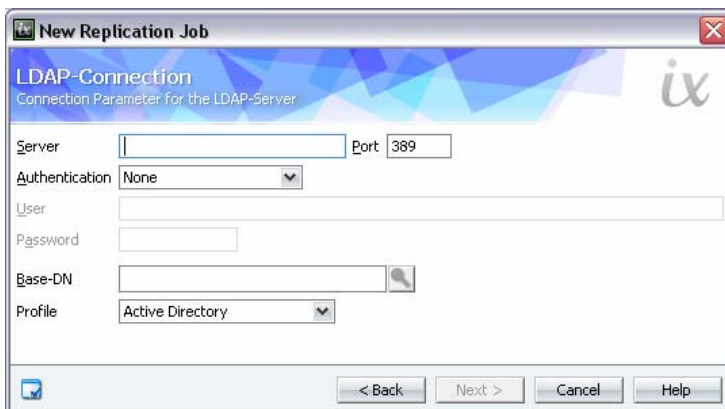


Select the type of import source and enter a name for it here. The *LDAP* option allows all LDAP-conforming sources, such as Microsoft Active Directory or Open LDAP, to be imported. With the standard configuration, the following import profiles are available:


- Microsoft Active Directory
- Sun ONE Directory Server
- Novell Netware.

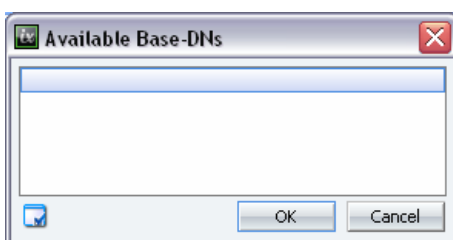
The options *JDBC* and *Text* allow users to be imported from JDBC data sources and text files, respectively.


7.1. LDAP Sources

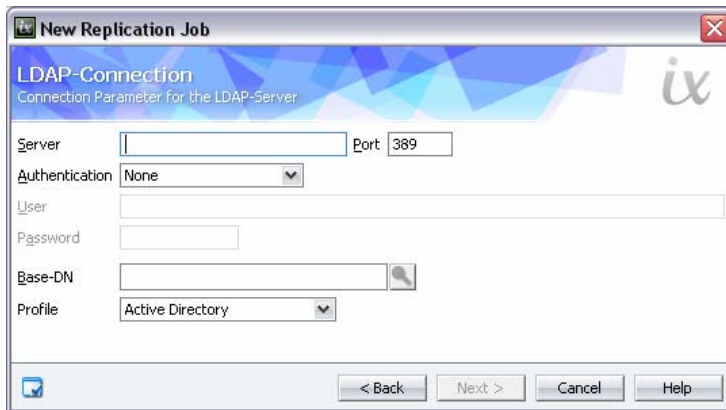


In this way, you can import your organizational structure and users from a LDAP directory (such as *Microsoft Active Directory*). Enter the source server of the LDAP directory in the *Server* field (such as the domain controller). In the *Authentication* selection list, select the type of authentication used by your LDAP server. The *simple* setting is usually the correct selection. Enter a *User*, via whose account the users and organizational units will be imported (such as *john.smith@Domain.com* or *cn=John Smith,ou=IT,dc=YOUR_DOMAIN,dc=US*).

Enter the *Password* of the user. The *Base-DN* (Distinguished Name) is the name of the subtree from which the users and user groups will be imported. Clicking  *Search* allows the Base-DN to be selected from a list.



Click  *OK* after making your selection.



New Replication Job


LDAP-Connection
Connection Parameter for the LDAP-Server

Server: Port: 389

Authentication: None

User:

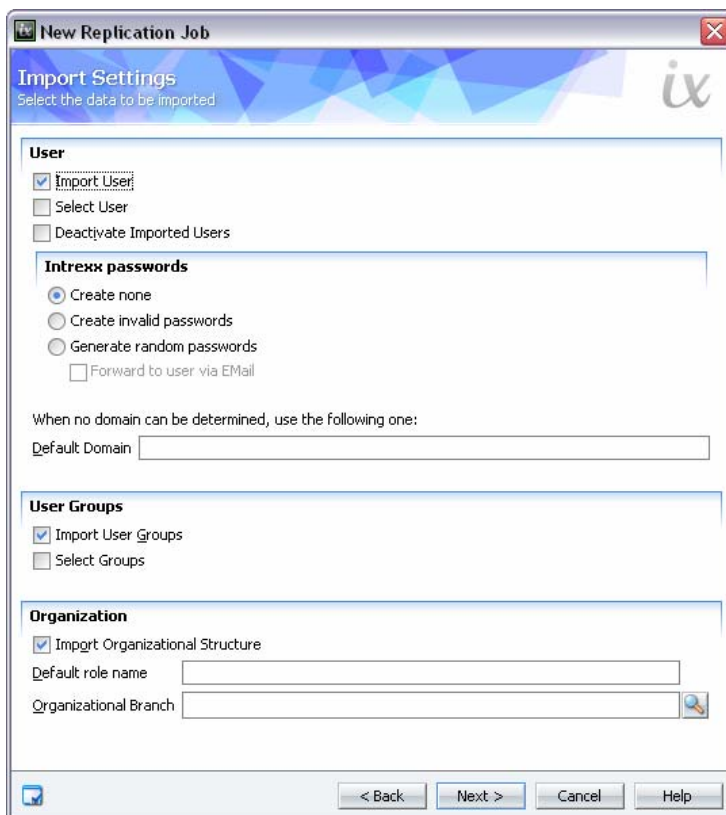
Password:

Base-DN: 

Profile: Active Directory

< Back Next > Cancel Help

Next, select the appropriate *Profile*. Click  *Next* to continue.



New Replication Job

Import Settings
Select the data to be imported

User

Import User

Select User

Deactivate Imported Users

Intrex passwords

Create none

Create invalid passwords

Generate random passwords

Forward to user via EMail

When no domain can be determined, use the following one:

Default Domain:

User Groups


Import User Groups

Select Groups

Organization

Import Organizational Structure

Default role name:

Organizational Branch: 

< Back Next > Cancel Help

With the *Import User* setting, all users will be imported. The setting to *Select User* allows users to be specifically selected on the following page.



New Replication Job

User Selection
Select the Users to be Imported

Select the users to be imported

Name	Login Name	Domain	First Name	Last Name	Path

< Back Next > Cancel Help

Highlight the users that you wish to import in this list. In order to import users from LDAP sources, additional options can be set.

New Replication Job

Import Settings
Select the data to be imported

User

Import User
 Select User
 Deactivate Imported Users

Intrex passwords

Create none
 Create invalid passwords
 Generate random passwords
 Forward to user via EMail

When no domain can be determined, use the following one:
 Default Domain

User Groups

Import User Groups
 Select Groups

Organization

Import Organizational Structure
 Default role name
 Organizational Branch

With the setting to *Deactivate Imported Users*, all user accounts of new users after an import will first be deactivated and must be activated by the administrator.

Passwords cannot be imported, as most source systems do not provide this function for security reasons.

The option to *Do not generate* will cause Intrex Xtreme to not generate any passwords automatically. Users without passwords will have easy access to the portal, as only the user name is required for login. The setting to *Create invalid* will cause Intrex to generate pro forma unique passwords for each user. With these passwords, no login will be possible, but they can be changed by administrators in the User Manager.

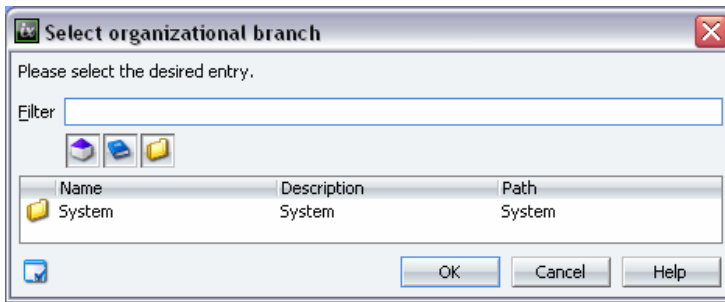
The setting to *Generate random passwords* will create a password for each user after import. If the setting to *Send to user via eMail* is active, each user for whom an eMail address has been saved will be sent the new password automatically via eMail.

If no domains can be found for an LDAP import, a standard domain can be entered into the *Default Domain* field.

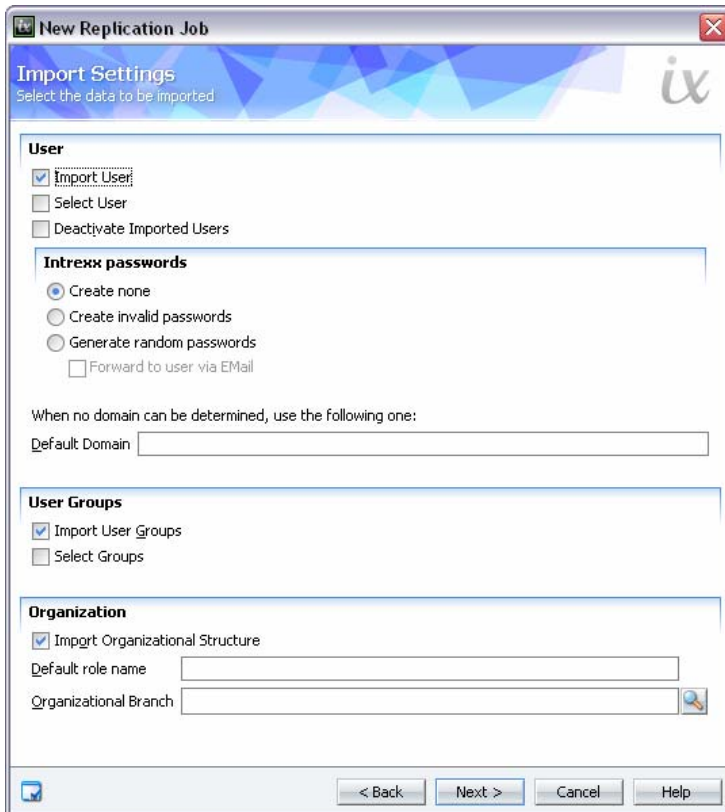
The setting to *Import User Groups* will import user groups. The *Select Groups* setting allows you to select individual user groups on the following dialog page, as with the *Select Users* setting.

The setting to *Import Organizational Structure* will import organizational branches. If organizational units are imported from LDAP directories that contain no assignment of users to positions or roles, the selected position type in *Default Role Name* will be used as the default assignment.

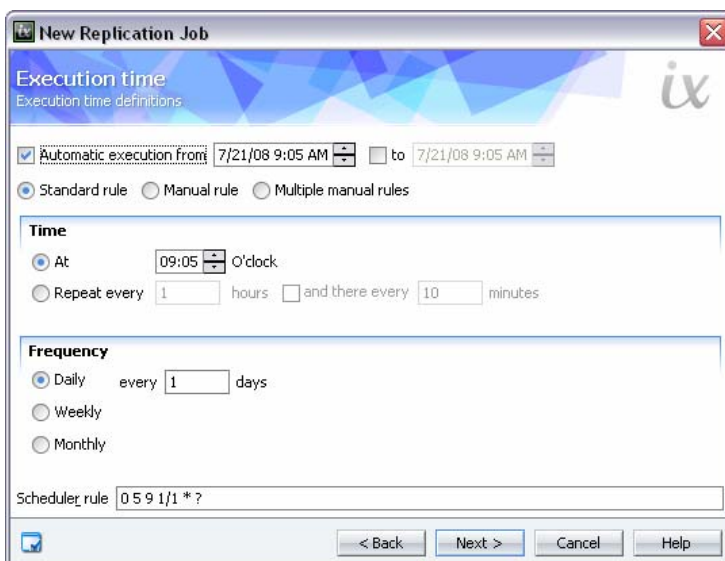
The magnifying glass allows the container in which the new users will be imported to be selected in the following dialog.



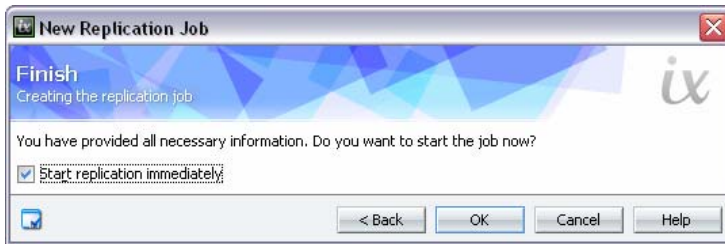
After making a selection, click **OK**.



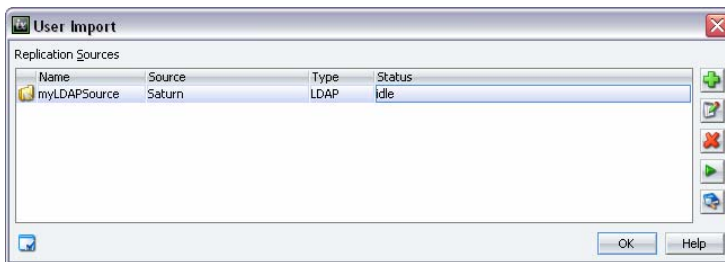
After selecting all required settings, please click **Next**.



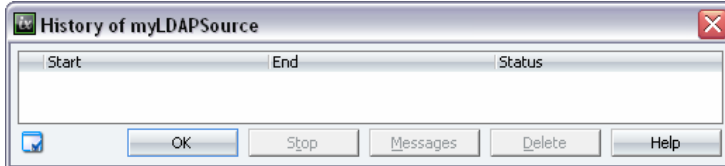
An automatic time of execution can be defined for the import. All information on this topic can be found in the [Integration Center handbook](#) in the *BizWalker* chapter. Click [Next](#) to continue.



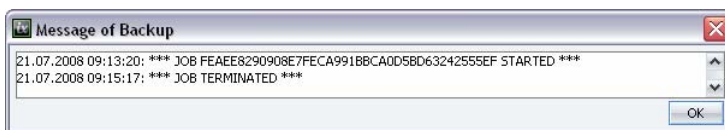
If the setting to *Immediately begin replication* is active, the user import will be started after clicking [OK](#).



The new replication source will now be entered to the list. The configuration of existing sources can be changed by clicking [Edit](#). [Delete](#) deletes a source entered here. When you are ready to initiate the replication, please click [Start replication](#). [Show history](#) will open a dialog that delivers information on replication activity.



Clicking [Stop](#) allows a currently running replication to be halted. Clicking [Messages](#) will open an additional dialog, which will output a detailed report in the case of an error. [Delete](#) allows the selected report to be removed from the list.



7.2. JDBC Sources

The screenshot shows the 'New Replication Job' dialog box with the 'JDBC Connection' step selected. The title bar reads 'New Replication Job'. The main title is 'JDBC Connection' with the subtitle 'Settings for the import from a JDBC datasource'. The 'ix' logo is in the top right. The 'Database settings' section contains four text input fields: 'JDBC-Driver', 'JDBC_Url', 'User', and 'Password'. A 'Wizard' button is located to the right of the 'Password' field. The 'Import settings' section has a 'Profile' dropdown menu currently set to 'sample'. At the bottom, there are four buttons: '< Back', 'Next >', 'Cancel', and 'Help'.


Enter the information for the connection to the JDBC data source here. If authentication is required, please enter the *User Name* and *Password* in addition. The *Assistant* button allows you to access an assistant that will help you to configure the connection. In the import settings, a *Profile* can be chosen. All profiles are located in the directory `<xtreme>/cfg/omjdbcrcplconfig` as XML files. New profiles can also be saved there.


7.3. Text Sources

The screenshot shows the 'New Replication Job' dialog box with the 'Import from Text File' step selected. The title bar reads 'New Replication Job'. The main title is 'Import from Text File' with the subtitle 'Enter Import File and According Format'. The 'ix' logo is in the top right. The 'File' field is a text input with a search icon. Below it are two dropdown menus: 'Column Separator' set to '<Tab>' and 'Field Separator' set to '<None>'. There is an unchecked checkbox labeled 'File Contains Header'. At the bottom, there are four buttons: '< Back', 'Next >', 'Cancel', and 'Help'.

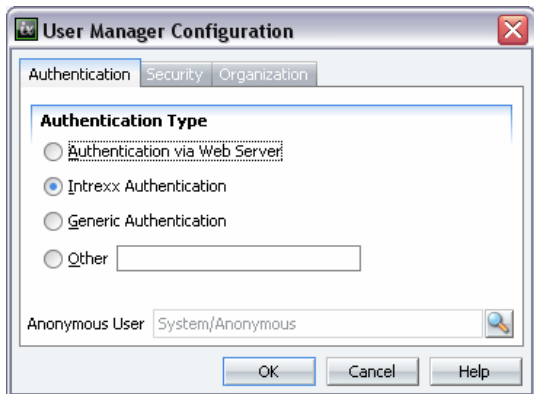
Select the *File* here that contains the import data. Select the column separator and the field separator here that have been used in the text file. With the *File contains header line* setting, the first line will not be imported, but the contents will be used in the following dialog pages for easier assignments. Click *Next* when you are done.

The screenshot shows the 'New Replication Job' dialog box with the 'Text File Field Mapping' step selected. The title bar reads 'New Replication Job'. The main title is 'Text File Field Mapping' with the subtitle 'Assign File Fields to User Data'. The 'ix' logo is in the top right. The interface is split into two panes. The left pane, titled 'Internal', has a sub-header 'Mapped' and lists internal fields: CONTAINERID, City, Country, DIN, Date enter, Date of Birth, Default Language, and Deputy.ID. The right pane, titled 'File', lists file rows: Row 1, Row 2, Row 3, Row 4, Row 5, and Row 6. Two arrow buttons (left and right) are positioned between the panes. At the bottom, there are four buttons: '< Back', 'Next >', 'Cancel', and 'Help'.

Assign the fields of the text file to the internal fields with the help of the  arrow buttons. When the full login name has been assigned, the import data of this field will be used to

find the data for the user name and domain. To continue, click  *Next*. A description of the dialogs that follow can be found in the *LDAP Sources* chapter.

8. Configuration



In the User Manager you will define the settings of authentication, security and organization under the menu item *User / Configuration*.


8.1. Authentication


8.1.1. Authentication via Web Server

With this setting the user account that is used for login to the NT or ADS domain will also be used to log in to the portal. All users must be able to log in to their corresponding domains, or a position of trust must exist in regard to domains of the Intrex Xtreme portal server.

The *Standard Authentication* option is required when users with browsers such as Netscape or Mozilla access the portal. These browsers support no encrypted login (integrated Windows authentication). The password will be transmitted in plain text in this case. Please note that the password may be intercepted with this unencrypted transmission method.

The option for *Integrated Windows Authentication* allows users with Microsoft Internet Explorer to login without entering a password. The users will be authenticated when they log on to Windows.

 When using Tomcat as webserver, both of these options will be unavailable.

 For all Intrex Xtreme versions on Windows 2000, the following conditions apply when changing the authentication to *Authentication via Web Server*:

If the services of the Intrex Xtreme portal server are started via the Service Console, they will always run under Windows 2000 in the context of the logged in user. All users in whose context the portal server runs must possess the privilege to *Act as part of operating system*.

In the local security policies of the server, give these corresponding users and/or groups the permission to *Act as part of operating system* (*Start – Settings – Control Panel – Administration – Local Security Policy – Local Policies – User Permissions Assignment*).

Afterwards, the *Intrex Xtreme Portal Server* service must be restarted under Windows services. After starting, the process javaw.exe will run under SYSTEM. If problems still occur, the permission to *Log on as batch job* (path as above) must be additionally entered.

8.1.2. Intrex Authentication

Regardless of membership in local domains, each user will log on with the user name and the password from the User Manager to the portal.

Select the user who will assume the role of anonymous user from the *Anonymous User* selection list. The anonymous user is the user who accesses the portal without logging on. This account will be used for all users before logging on.

The type of authentication can be changed at a later point in time from *Intrex Authentication to Authentication via Web Server*. The change will take effect only after the users are imported.

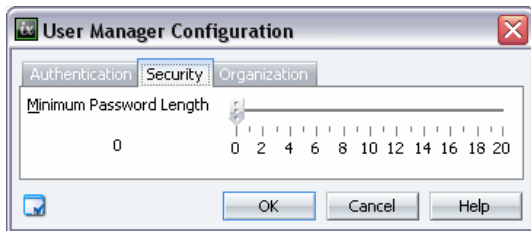
8.1.3. Generic Authentication

Generic authentication allows the configuration of an authentication module for authentication via an LDAP server. In this case, the user name and the password will be transmitted in plain text. Please make sure that the login only is transferred via secure connections. To set up the generic authentication, please contact United Planet consulting.

8.1.4. Other Authentication

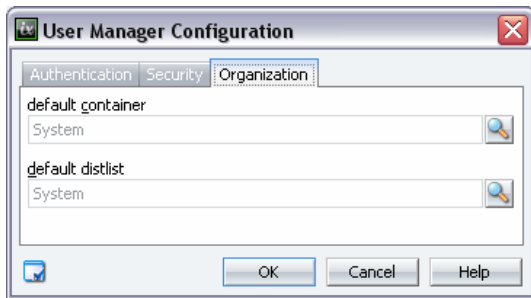
Other authentication modules can be developed based on your needs. As examples, the authentication can be instituted here via X509 certificates, authentication to systems from third party providers, and so on. If you have questions, please contact United Planet consulting.


8.2. Security

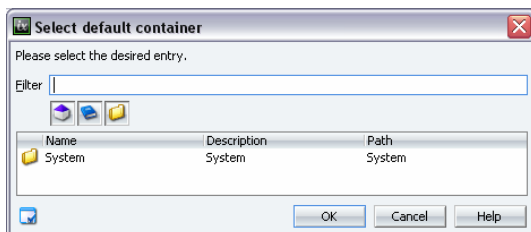


Enter the minimum length of the password here. When passwords are created that fall below this number, an error message will be output.

8.3. Organization



Clicking on the  magnifier symbol here allows the *Default container for new users* and/or *new distribution lists* to be changed.



The default container is relevant for the creation of new users and/or distribution lists from the *Users* application as follows. New users and/or distribution lists that are created in the browser will be automatically assigned to the container entered here.