
Bitrix Site Manager

Quick Guide To Using
The AD/LDAP Module

Contents

Introduction.....	3
Chapter 1. The Principal Features Of The Module.....	4
Chapter 2. How It Works	6
Chapter 3. Configuring AD/LDAP Authorization.....	7
Adding A Server	7
NTLM Authorization	12
Configuring The Module For AD/LDAP or NTLM Authorization	12
Chapter 4. Import From LDAP Directory	15
Final Notes	17

Introduction

Integrating a site with the corporate information system usually requires that the employees' permissions are distributed between the site and the network in order to achieve transparent access to the site resources and management functions. A common solution to this problem is creating user groups with different access permissions applied to them and further adding users to these groups. In this case, an administrator may face the need to transfer the existing corporate user groups to the site management system (hereinafter referred to as CMS) to allow users to assess and manage the corporate site resources. This incurs doubling of the efforts required to change access permissions or add a new user to both the corporate network and the CMS: the administrator has to create or edit a user profile in the corporate system as well as in the CMS.

The **AD/LDAP** module is developed especially for use with Bitrix Site Manager. It permits mapping corporate network user groups to those of the CMS thus allowing to manage user groups of the corporate information system in a centralized fashion.

This manual describes the scope and implementation of the functions encapsulated in the Bitrix Site Manager's AD/LDAP module. An approach to set up the module and assign corporate user groups to those of the Bitrix Site Manager is also highlighted.

<p>Note: Bitrix Site Manager and Bitrix Intranet Portal share absolutely the same version of the AD/LDAP module. Any information about this module is also applicable to Bitrix Intranet Portal.</p>

Chapter 1.

The Principal Features Of The Module

The **AD/LDAP** module has been developed with respect to LDAP (Lightweight Directory Access Protocol) and AD (Active Directory) protocols one of which must be installed at the corporate server.

The **AD/LDAP** module is built on the concept of storing data as records containing a set of attributes; these records are stored in a hierarchical database. The following figure illustrates how the user group information is stored on the LDAP/AD server:

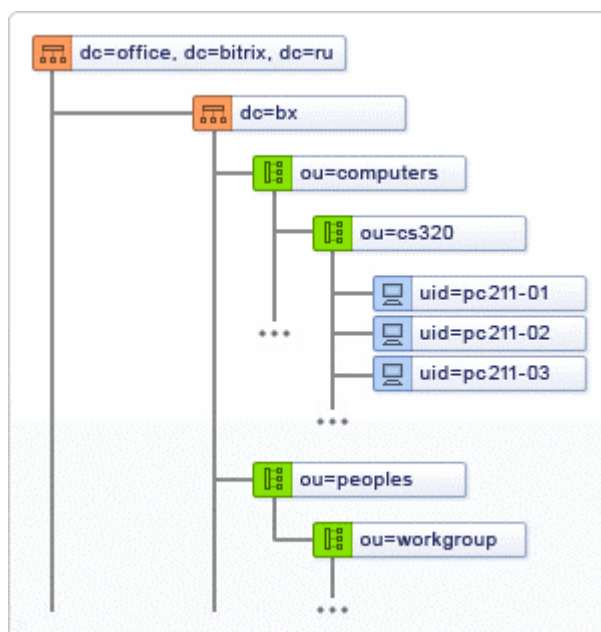


Fig. 1.1 The structure of the server records

Using this structure to store user data, the AD/LDAP module can assign corporate user groups to the site user groups.

The assignment rules exist in a special **Assignment Table** in the site's Control Panel. The assignment allows user groups of the site and the corporate network to have different names. For example, a corporate network user group **Techsupport** can be mapped to a site user group **Techsupport stuff**. Having this assignment made, the administrator enables *the corporate network* techsupport members to provide consultancy *on the site*.

The corporate user groups are given permissions to access the corporate network resources. The corresponding site user groups have permissions to access the site resources. For example, the **Techsupport** group users can access the corporate

mail server; while the **Techsupport stuff** group users can access the **Helpdesk** module of the site.

According to this example, a **Techsupport** corporate user will be automatically added to the site **Techsupport stuff** user group upon successful authorization on the site. After that, the system automatically creates the user account stored on the corporate server.

A user can be assigned to one or more user groups. The system may contain user groups not mapped to those of the corporate network. The administrator has to add users to such groups manually. All changes made to the user profile on the corporate server will be automatically transferred to the CMS user profile at the next authorization time. In this case, only the user groups mapped to those of the corporate network are updated.

The AD/LDAP module enables to:

- integrate Bitrix Site Manager in the corporate network;
- map the corporate network user groups to the website user groups;
- automatically create user profiles as per **Assignment Table** upon successful registration. (The system creates the profile using data requested from the corporate server database);
- manage user profiles via the corporate server in a centralized fashion.

Another advantage proposed by the **AD/LDAP** module is **NTLM authorization**. This requires an **IIS** or **Apache** web server with **mod_ntlm** or **mod_auth_sspi**.

Chapter 2.

How It Works

A common AD/LDAP module's sequence of operation is as follows.

1. A user opens the site and authorizes by typing the login and password they use to authorize in the corporate network.
2. The system connects to the server specified in the AD/LDAP module settings and verifies whether a user with the supplied credentials exist in the corporate server database:
 - if no user with the supplied credentials exists in the corporate network, the system declines authorization;
 - if the user is found, the system determines the corporate network user group for this user. After that, the system searches for the site user group using the **Assignment Table**.
3. The system verifies whether the user profile exists:
 - if the user profile is not found, the system attempts to obtain the user data from the corporate server and then creates a new profile;
 - if the user profile exists (which means a user had previously been authorized), the system checks whether any change were made to the user profile on the corporate server. If so, the CMS user profile becomes updated to reflect changes.
4. The user is granted permission to access the site resources and becomes authorized. The user permissions are defined according to their user group settings.

If a site user (a member of any group registered in the **Assignment Table**) is deleted from the corporate network user list, their authorization on the website will fail. At the same time, the user profile is still stored in the CMS database.

To allow the user authorize on the website via the common interface, enable *internal authorisation check*. To do so, set the **Authorisation Type** value to "internal check" in Control Panel and then update the user credentials (login and password).

Note: if the **AD** tree contains N domains (e.g. each for the company departments OD1, OD2 etc.) and these domains has groups with identical names, the **Assignment Table** displays such groups N times, each group for each domain. To avoid confusion, change the **Group Name Attribute** in the server settings on the **Field Mapping** tab. A good choice is **DistinguishedName (DN)**.

Chapter 3.

Configuring AD/LDAP Authorization

You will configure the **AD/LDAP** module in Control Panel: *Settings > System Settings > Module Settings > AD/LDAP Connector*.

Adding A Server

First, you have to create a new record which will contain information about the corporate server (a *server record*) whose database will be used to map user groups.

Each server record regulates access to one root in the catalog tree. If the corporate network user groups are stored on multiple servers or in several databases on a single server, you should create an individual server record for each storage point.

To create a server record, click **Add** on the context toolbar of the **AD/LDAP** form (*Settings > AD/LDAP*).

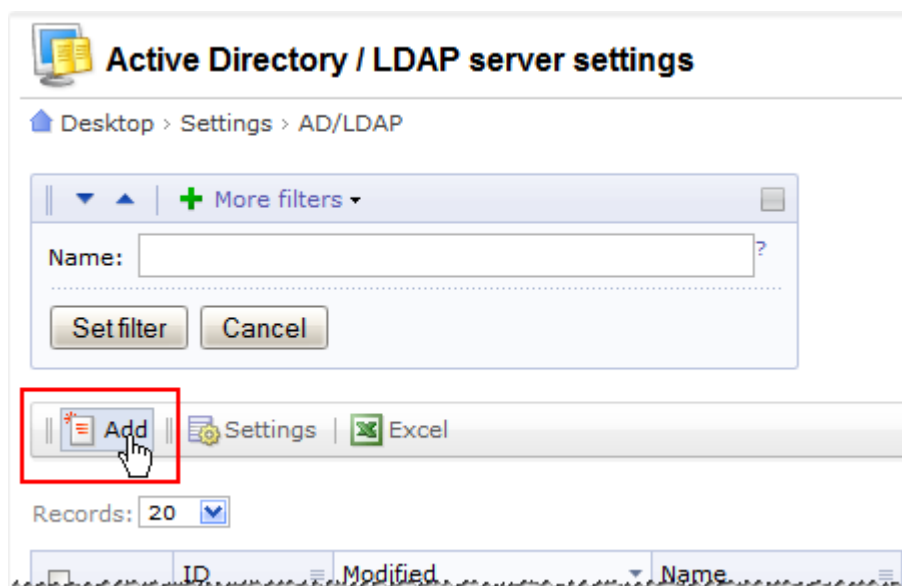


Fig. 3.1 The AD/LDAP servers page; starting to add a server record

On the **Server** tab, specify the server connection parameters. Name the server as you wish to see it in the servers table.

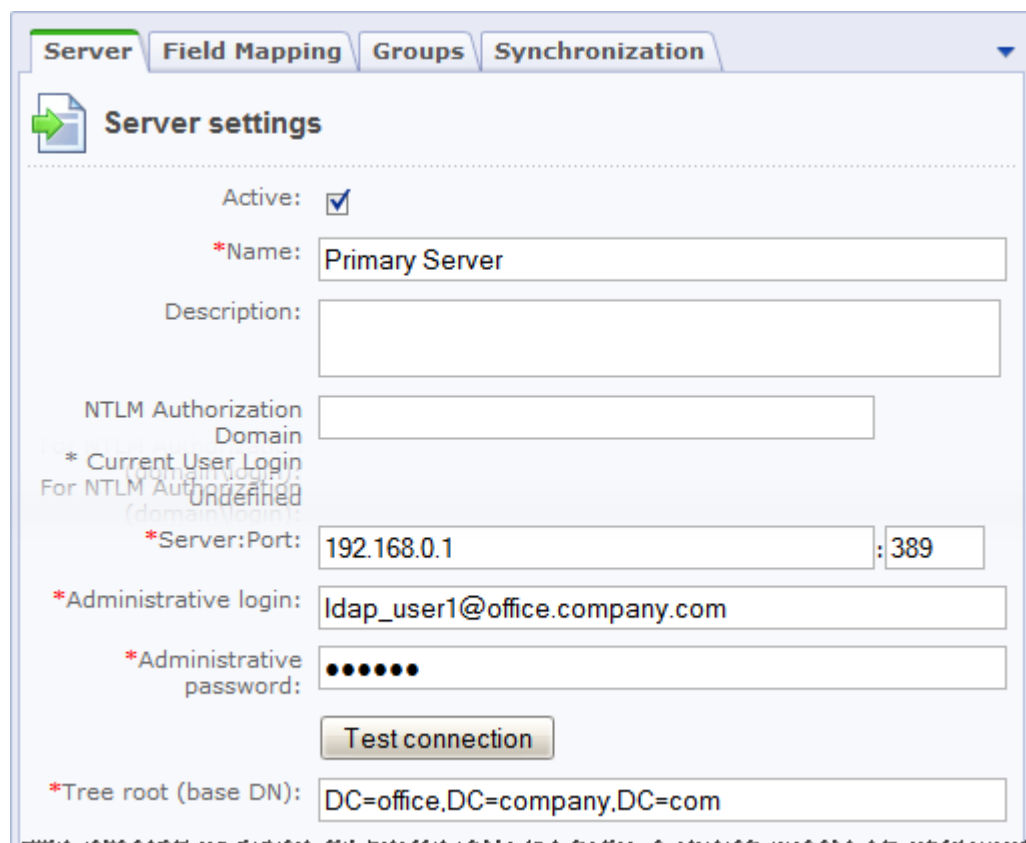


Fig. 3.2 Specifying the server parameters

□ Provide information on the **Server** tab (fig. 3.2):

- **Active:** if this box is checked, this server is used for the user profile lookup when a user attempts to authorise. Otherwise, this record is ignored.
- **Name:** the name of the record to be created as it will be shown in lists.
- **Description:** type here the server description.
- **NTLM Authorization Domain:** used to resolve the required **AD\LDAP** server for the **<domain\login>** authorization. It is also used for automatic NTLM authorization in which case it must be the same as the company domain.

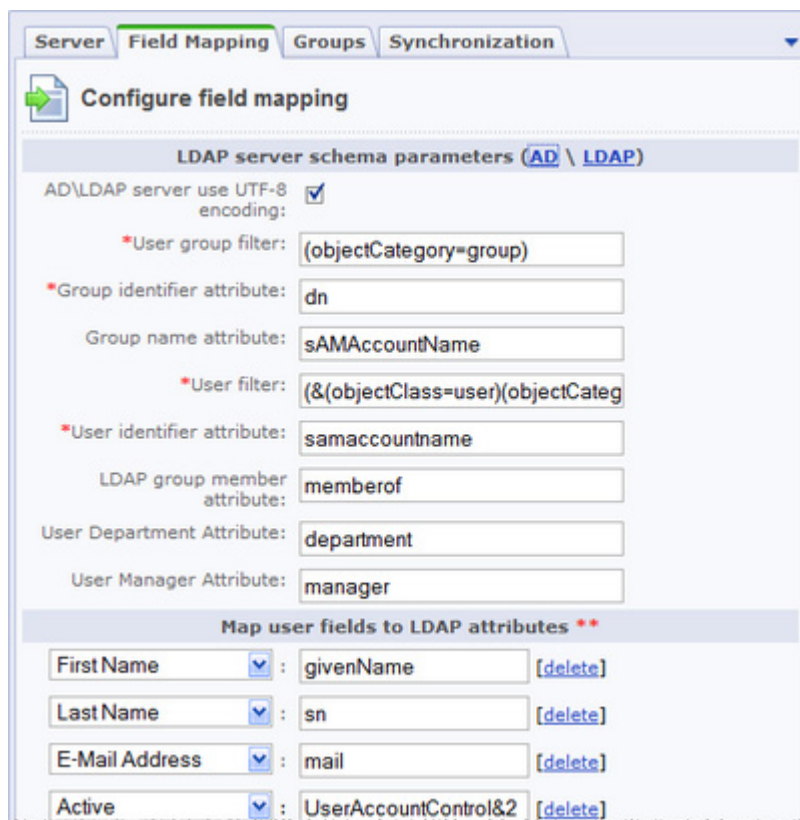
If there are multiple **LDAP** servers, this field becomes essential for proper resolving of the user name because multiple users with the same name may potentially exist on the servers. In such case, the mnemonic name will help to resolve the record unambiguously pointing to the server and the catalog tree root in which the user account lookup is to be performed.

- **Server:Port:** the IP address and the port number of the corporate server hosting the user group database. The port 389 is standard for LDAP servers.
- **Administrative Login:** the login string for administrative access to the server. (as **login@domain** or **domainlogin**).

- **Administrative Password:** password for administrative access to the server.
 - **Tree Root:** after the successful trial connection (see below), this field contains the catalog tree roots. Select the one which will be used for the user profile lookup when authorizing.
- ❑ Click **Test Connection**.

The system will attempt to connect to the specified server. If the test succeeds, the server will return a list of available tree roots. Otherwise, the system will display the error description showing the error description.

- ❑ Click the **Field Mapping** tab (fig. 3.3). Here you will set the fields selected when importing records.



The screenshot shows the 'Configure field mapping' window with the following configuration:

- LDAP server schema parameters (AD \ LDAP)**
 - AD\LDAP server use UTF-8 encoding:
 - *User group filter: (objectCategory=group)
 - *Group identifier attribute: dn
 - Group name attribute: sAMAccountName
 - *User filter: (&(objectClass=user)(objectCateg
 - *User identifier attribute: samaccountname
 - LDAP group member attribute: memberof
 - User Department Attribute: department
 - User Manager Attribute: manager
- Map user fields to LDAP attributes ****
 - First Name : givenName [delete]
 - Last Name : sn [delete]
 - E-Mail Address : mail [delete]
 - Active : UserAccountControl&2 [delete]

Fig. 3.3 Server field configuration

The standard values appropriate for **AD** or **LDAP** server can be inserted automatically by clicking the **AD** or **LDAP** link in the group header (fig. 3.3).

To add more mapping fields, click **[add..]** link in the **Map user fields to LDAP attributes** http://localhost:6448/bitrix/admin/ldap_server_edit.php?lang=en&ID=0_-notes section. Note that it is best to specify here only the fields that are essential for authorization. Other fields can be added in the user import form (*Settings > Manage users > User import*) on the field configuration tab.

Each field you specify here will be verified for change when performing synchronization and updated in Bitrix Site Manager, if necessary. In practice, it means that if a user changes a field in their profile, the field will be restored at the next synchronization time.

So the best practice is to add as many fields as needed when importing users for the first time, and then delete fields that need not be constantly updated.

- ❑ Click the **Groups** tab.
- ❑ To add user groups to the assignment table, click **Refresh group list** (fig. 3.4). This will also verify parameters you have specified previously.

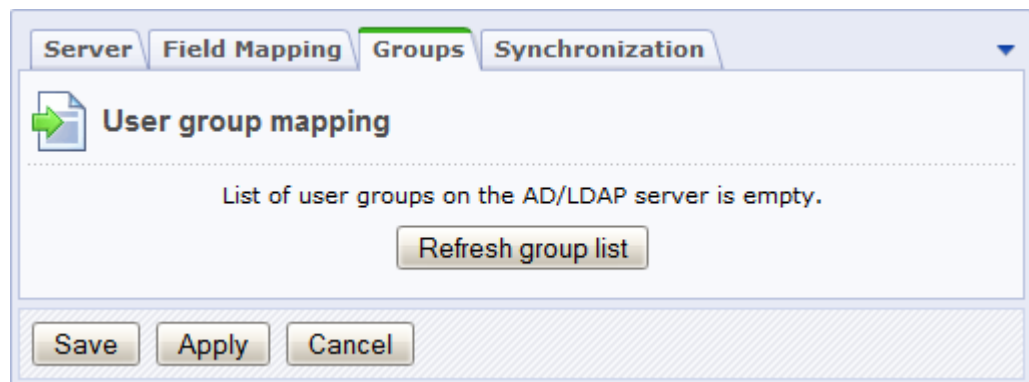


Fig. 3.4 The Groups tab

After the groups have been updated, the tab will show the **Assignment Table** (fig. 3.5):

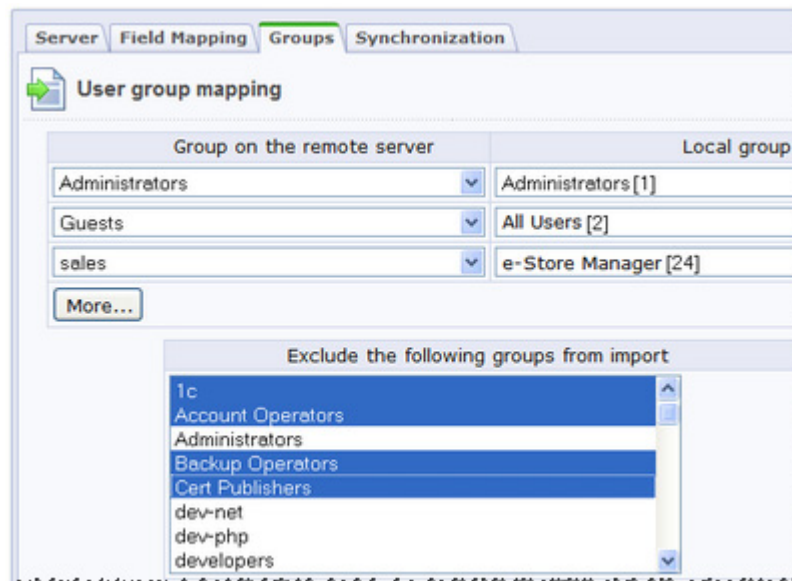


Fig. 3.5 The groups assignment table

- ❑ Map the groups by selecting the *remote* group and the corresponding *local* group.

On this screen (and as assumed by the **AD/LDAP** module), the *remote* user groups are those of the corporate network. On the contrary, the *local* user groups are the website's Bitrix Site Manager groups. This is because an entity here is assumed *local* with respect to the website location.

The **Exclude the groups from import** list contains the remote (corporate server) user groups. If you do not want to have some of the groups included in the import, select them here. The selected groups will be excluded even if they are selected in the assignment table.

To add more assignment options, click **More....**

If the users of a corporate user group have to be assigned to multiple website or portal user groups, select such remote server user group in as many assignment table rows as needed and assign the required local group to each.

If the same local group is assigned to different remote server user groups, only the users contained in both user groups will be added (i.e. intersection occurs).

- ❑ Now open the **Synchronization** tab (fig. 3.6).

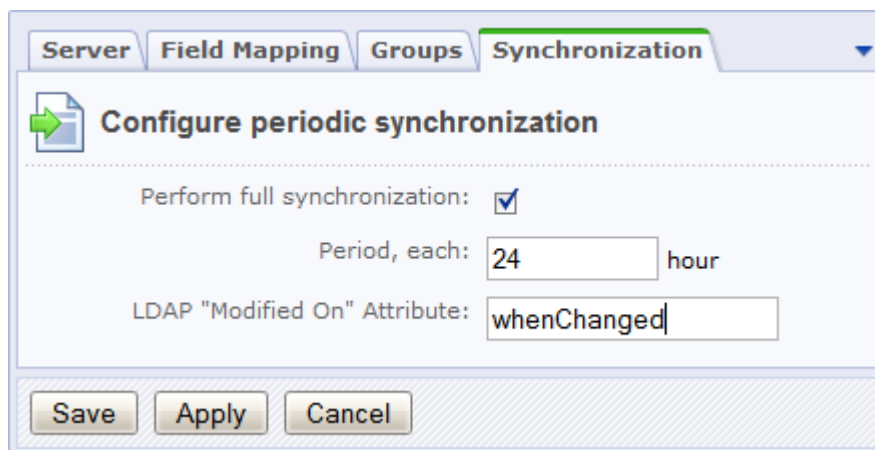


Fig. 3.6 Synchronization parameters

- ❑ To provide for recurring synchronizations, enable the fields by checking the corresponding box. Type the name of the LDAP attribute from which the modification date and time will be set.

Note: The **Agent** technology may come in handy for periodic synchronization. It allows to run the specified functions at a given time interval without using external tools. The agents are discussed in details in the [online help](#).

- Save changes.

Now, a new server record appears in the **AD/LDAP** form (fig. 3.7):

<input type="checkbox"/>		ID	Modified	Name	Act.	UTF-8	Mnemonic code	Server
<input type="checkbox"/>		2	11.11.2009 10:45:08	My Serv	Yes	Yes		192.168.0.1
Selected: 0		Checked: 0						

Fig. 3.7 New server added

NTLM Authorization

Bitrix Site Manager and Bitrix Intranet Portal support **NTLM** authorization by default. This is done by including the Apache's **mod_auth_sspi** module in Bitrix Environment package. If you do not use this package, you will have to install the module manually.

- Download **mod_auth_sspi** at <http://sourceforge.net/projects/mod-auth-sspi/>.
- Copy the module files to `c:\...\apache\modules\`.
- Add the following line to **httpd.conf**:

```
LoadModule sspi_auth_module modules/mod_auth_sspi.so.
```

- Add the following line to **.htaccess**:

```
AuthName "My Intranet"
AuthType SSPI
SSPIAuth On
SSPIPackage NTLM
SSPIDomain MYDOMAIN
SSPIPerRequestAuth On
SSPIAuthoritative On
SSPIOfferBasic On
Require valid-us
```

If you use Bitrix Environment, the above lines are already in the file but you have to uncomment them.

- Change MYDOMAIN in "SSPIDomain MYDOMAIN" to your domain.
- Save changes.

Configuring The Module For AD/LDAP or NTLM Authorization

- Open the **AD/LDAP Connector** module settings page (*Settings > System settings > Module settings > AD/LDAP Connector*) (fig. 3.8).

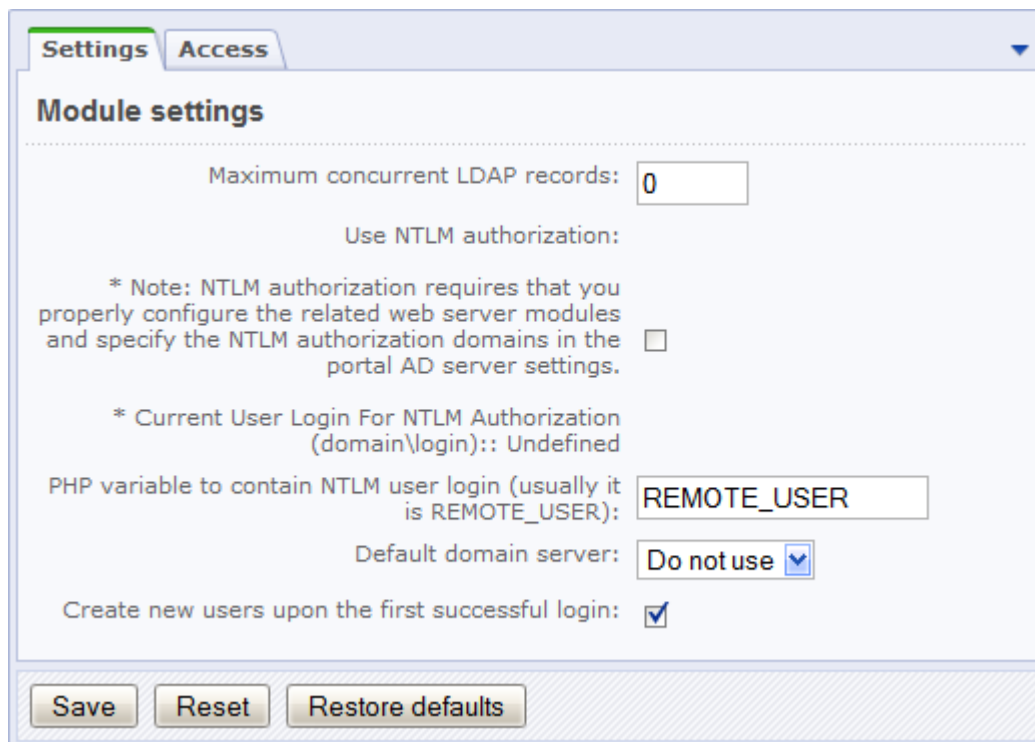


Fig. 3.8 The AD/LDAP Connector module settings

- ❑ Set the maximum concurrent LDAP records to more than **0**. This is the number of users the server can simultaneously process.

Larger number of concurrent records (multiple users) can noticeably slow down the LDAP server. This value should be estimated empirically.

- ❑ Check the **Use NTLM Authorization** box if required.

The system uses the value of the **REMOTE_USER** key in the **\$_SERVER** array to access the user login (in the form of **login** or **domain/login**). It is unlikely that you will have to use any other key name. However, you can change it in the **PHP variable...** field if required.

- ❑ If your network has multiple LDAP servers, and you use NTLM authorization, select the NTLM authorization server in **Default domain server**.

The **Create New Users On First Successful Login** option may be very important, and here's why. First of all, if it is checked, new users do not have to wait for the upcoming synchronization to update the records so they could log in to the website. However, such convenience may potentially compromise the security. If you are using the AD protocol, you can strictly fix the users allowed to access the website: simply create the required users and then uncheck this option. Only the users you have explicitly added will be able to authorize on the website.

- Save changes.

Notes

The computer running the **Apache** server must be included in Windows domain.

Bitrix Intranet Portal users may rarely encounter problems with Internet Explorer (web page buttons may fail to function properly). To solve this problem, add the "**SSPIPerRequestAuth On**" instruction to the **.htaccess** root file.

Chapter 4.

Import From LDAP Directory

Importing users from LDAP directory is rather straightforward.

- ❑ Open the **Import Users** form (Settings > Manage users > User import).
- ❑ Select **Active Directory / LDAP** and click **Next** (fig. 4.1):

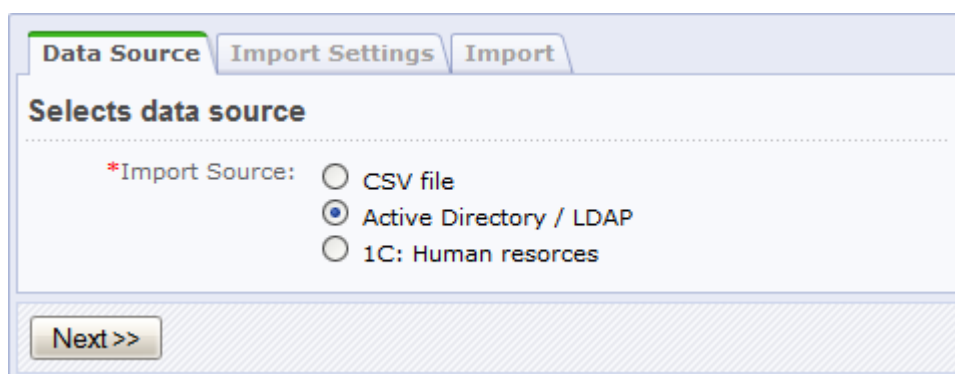


Fig. 4.1 Selecting AD/LDAP as the data source

- ❑ Then, select the server from which the users will be imported. Click **Next** (fig. 4.2).

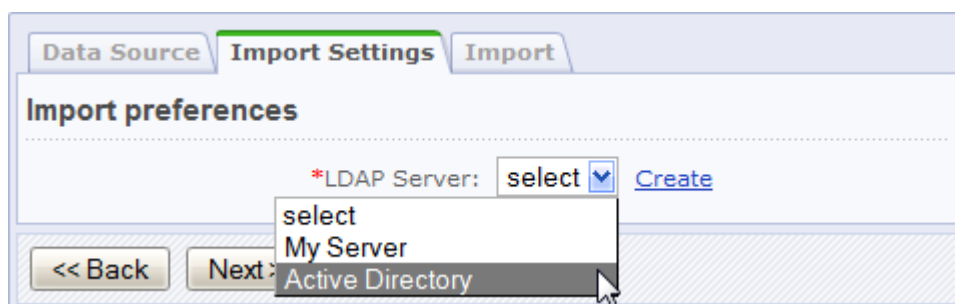
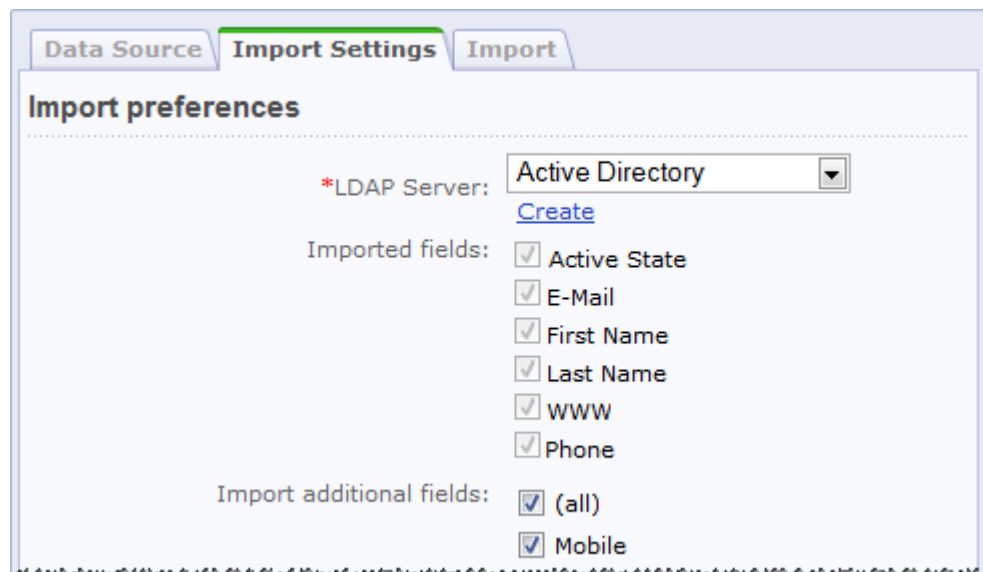


Fig. 4.2 Selecting the data source server

- ❑ After you have selected the server, the form will show the fields that would be imported (fig. 4.3). Uncheck the unnecessary additional fields.



The screenshot shows a web interface with three tabs: 'Data Source', 'Import Settings' (which is active), and 'Import'. Below the tabs is a section titled 'Import preferences'. It contains the following elements:

- '*LDAP Server:' followed by a dropdown menu set to 'Active Directory' and a 'Create' link below it.
- 'Imported fields:' followed by a list of checkboxes:
 - Active State
 - E-Mail
 - First Name
 - Last Name
 - WWW
 - Phone
- 'Import additional fields:' followed by a list of checkboxes:
 - (all)
 - Mobile

Fig. 4.3 The fields to import

- Click **Next**. The form will open the final tab (**Import**) in which it will import the records.

Final Notes

This document gave the readers the basic principles of using the AD/LDAP module.

You can ask your questions at the Bitrix corporate forum:

<http://dev.bitrixsoft.com/community/forums/>

Should you have any difficulty using Bitrix software, do not hesitate to send a request to the technical support service:

<http://dev.bitrixsoft.com/support/>