Creatio Academy

Synchronize users with LDAP

Version 7.17

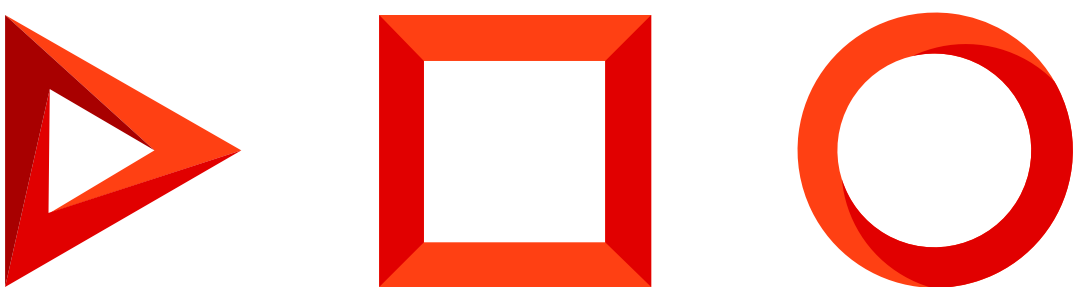


Table of Contents

Set up LDAP synchronization

PRODUCTS: ALL CREATIO PRODUCTS

LDAP directory synchronization lets you automate user account administration in Creatio. Users synchronized with LDAP can log in to Creatio with their domain credentials.

Creatio supports synchronization with Active Directory and OpenLDAP.

The synchronization procedure consists of three stages:

1. LDAP integration setup. Performed once, unless the LDAP directory structure changes. This step is required to enable the LDAP synchronization features. You will also need to set up Active Directory user filtering to define synchronization parameters. Read more: Set up Active Directory filters.
2. Connecting Creatio items (i. e. users and organizational structure elements) with the respective items in the LDAP directory. Performed when adding new users or organizational roles. You can connect existing Creatio user accounts or import users from Active Directory.
3. Synchronization of Creatio users and organizational structure elements with the connected LDAP directory elements. Required to update Creatio data so that it reflects changes to the LDAP directory since the previous synchronization. Creatio performs this step regularly. You can also synchronize data manually by clicking [*Synchronize with LDAP*] in the [*Organizational roles*] section.

> **Note.** Each organizational role is an element in a tree-like structure of roles, where each element is an organization or a department.

Users will be able to log in with LDAP after the synchronization. Read more: Set up LDAP authentication.

Set up LDAP integration

To set up LDAP integration, connect LDAP directory elements with Creatio users and roles. Basic knowledge about the structure of the relevant LDAP directory is required to set up the integration.

This article contains LDAP setup examples for Active Directory and OpenLDAP.

> **Attention.** Depending on the structure of each LDAP directory, LDAP element attributes in your directory may differ from the attributes specified as examples.

1. Click the button to open the System Designer.
2. Click the “LDAP integration setup” link in the “Import and integration” block. The setup page will open. Fill out the highlighted fields. You can keet the default values in the other fields.

Fig. 1 LDAP integration setup page for Active Directory

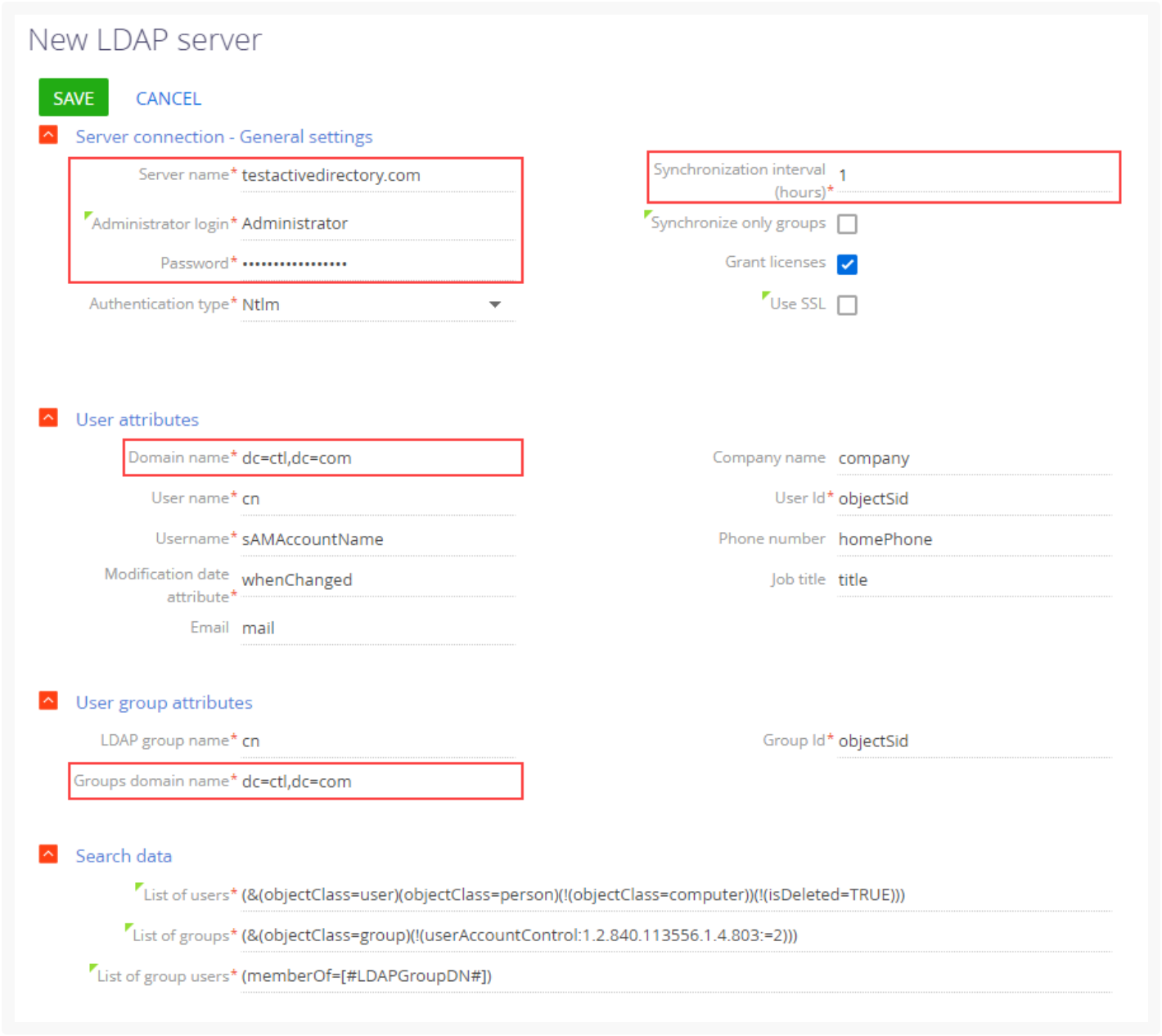
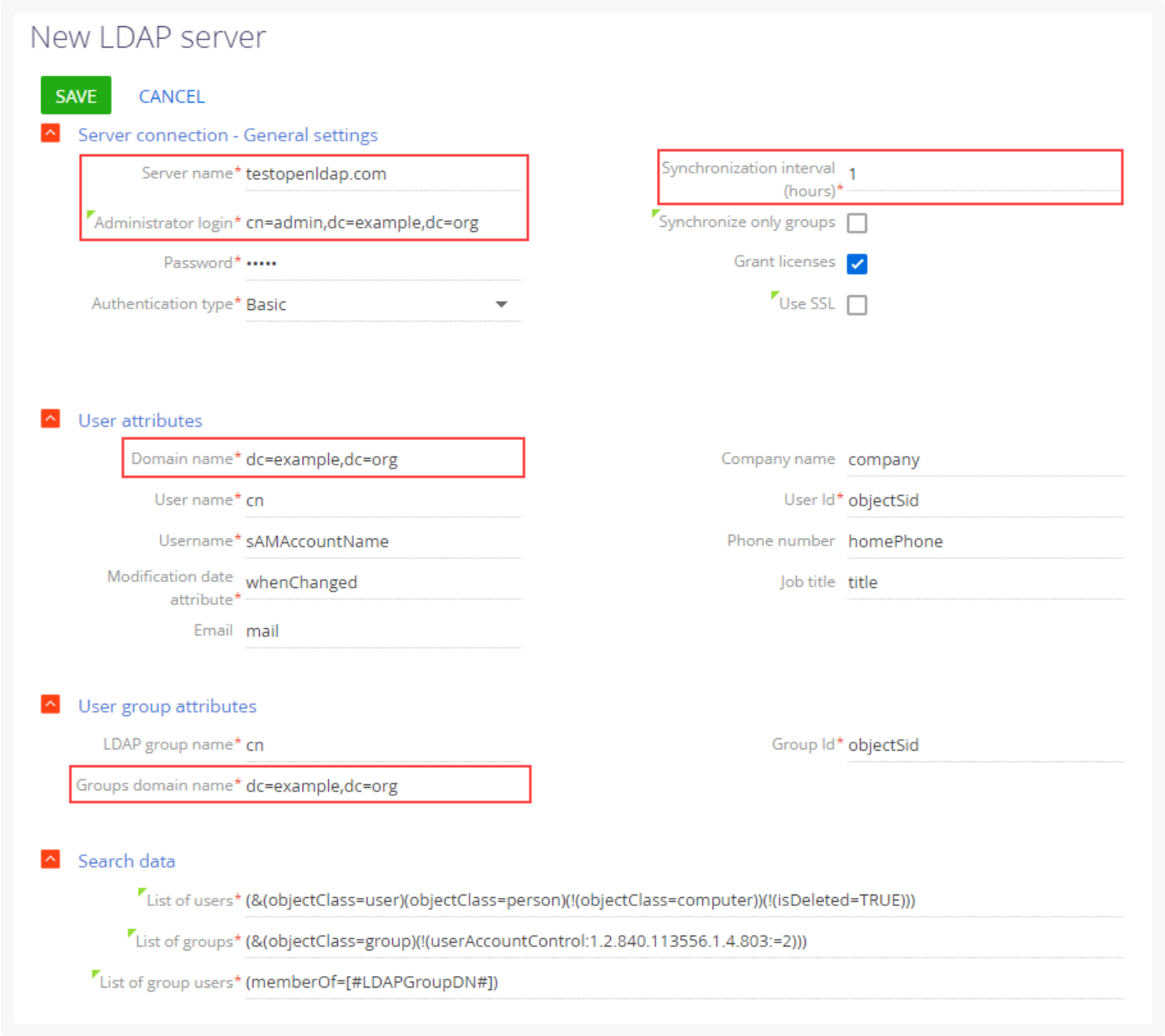


Fig. 2 LDAP integration setup page for Open LDAP



1. Set up the connection to the server

Specify the general server connection settings:

1. Enter the LDAP server name or the IP address in the [*Server name*] field.
2. Select the LDAP server connection protocol in the [*Authentication type*] field. The authentication type depends on your LDAP server and the authentication security requirements. For example, select the “Ntlm” type to authenticate “NT LanManager” supported by Windows.

> **Note.** If you select the “Kerberos” authentication type, the [*Server name*] and [*Key Distribution Center*] fields will only support URLs, not IP addresses. Your Creatio application server has to be joined to the same domain as the LDAP server and the key distribution center.

3. Specify administrator credentials in the [*Administrator login*] and [*Password*] fields. If your Creatio server is

installed on Linux, use the “domain\login” format.

> **Note.** Make sure that the administrator has sufficient permissions to read the user and group information.

4. Specify the automatic LDAP synchronization interval in the [*Synchronization interval (hours)*] field. Read more: Run the LDAP syncrhonization.
5. Select the [*Synchronize only groups*] checkbox to automatically deactivate and activate Creatio users that are manually excluded from and included in the synchronized groups in the LDAP catalog.
6. Select the [*Grant licenses*] checkbox to grant licenses to users on LDAP synchronization automatically.
7. Select the [*Use SSL*] checkbox to enable SSL for the synchronization. If you select the checkbox, specify the value of the [*Server name*] field in the “server:port” format.

   The default port value is “636” for the LDAPS connection. Only Creatio on Windows supports LDAPS synchronization.

   The default port value for the LDAP connection is “389.”

> **Note.** If you use a self-signed certificate in Creatio cloud, use the extracted block service and send the certificate to Creatio support so that they can mark it as trusted.

2. Set up the user synchronization

To set up the user synchronization, specify the attributes of the LDAP directory elements that contain the user data you need to import.

1. Map the **required** attributes:
   a. Specify the the unique name of the LDAP organizational structure element that contains the synchronized users in the [*Domain name*] field. You will only be able to synchronize users subordinate to the specified LDAP element, either directly or to its child elements. For example, if you specify the root element of the directory structure, you will be able to synchronize all users in the directory.
   b. Specify the the LDAP attribute that contains the full name of an LDAP user in the [*User name*] field. Creatio populates the [*Full name*] field on the contact page with the attribute's value during import. For example, the “name” or “cn” (Common Name) attributes can contain the full name of the user.
   c. Specify the attribute that contains the LDAP username used for login in the [*Username*] field. The synchronized LDAP user will log in to Creatio with this name. For example, “sAMAccountName.”
   d. Specify a unique user ID in the [*User Id*] field. The value of this attribute must be unique for each user.
   e. Specify the attribute that stores the time and date of the last change to the LDAP element in the [*Modification date attribute*] field.

> **Attention.** If any of these attributes are missing, LDAP synchronization will throw an error.

2. You can also map **optional** attributes Creatio will use to populate the user contact page:
   a. Specify the attribute that contains the name of the user's employer in the [*Company name*] field.

Populates the [*Account*] field on the contact page. If an account name matches the value of the specified attribute verbatim, Creatio will link the user's contact to that account during synchronization

b. Specify the attribute that contains the user's job title in the [*Job title*] field. Populates the [*Job title*] field on the contact page. If an existing job title matches the value of the specified attribute verbatim, Creatio will select this job title for the user during synchronization.

> **Note.** If the value of the corresponding attribute does not match any existing accounts and job titles verbatim, Creatio ignore such values during the synchronization and leave the corresponding fields on the user's contact page empty, rather than create new entries.

c. Specify the attribute that contains the user's phone number in the [*Phone number*] field. Populates the [*Business phone*] field on the contact page.

d. Specify the attribute that contains the user's email address in the [*Email*] field. Populates the [*Email*] field on the contact page.

> **Attention.** If you leave any additional attribute fields empty, Creatio will not populate them when importing users from an LDAP directory.

3. Set up synchronization between LDAP user groups and Creatio roles

Group synchronization settings let you link LDAP groups to Creatio organizational structure elements. To set up the synchronization, map the attributes of the LDAP directory elements that contain the user data to be imported.

1. Specify the attribute that contains the name of the user group in LDAP in the [*LDAP group name*] field. For example, the “cn” (“Common Name”) attribute.
2. Specify the attribute to use as a unique group ID in the [*Group Id*] field. The value of this attribute must be unique for each group. For example, you can use the “objectSid” attribute.
3. Specify the unique name of the LDAP element that contains all synchronized user groups in the [*Groups domain name*] field. All user groups subordinate to the specified LDAP element, directly or to its child elements, will be available for synchronization. For example, if you specify the root element of the LDAP directory, all user groups in the directory will be available for synchronization.

> **Note.** Creatio verifies users included in the synchronization groups during the synchronization process. If the date stored in the modification date LDAP user attribute is later than the last synchronization date, Creatio will update this user entry in Creatio organizational structure.

> **Attention.** If any of these attributes are missing, LDAP synchronization will throw an error.

4. Set up the filter conditions

Filter conditions determine which criteria to use to include LDAP elements in the list of synchronized groups and

users. Set up the general server connection settings for Active Directory:

1. Specify the elements to synchronize with Creatio users from the general LDAP element catalog in the [*List of users*] field. The search filter must select active elements only.
2. Specify the LDAP elements to synchronize with Creatio organizational roles (user groups) in the [*List of groups*] field. The search filter must select active elements only.
3. Build a list of users included in the LDAP group in the [*List of group users*] field. One or more attributes determine whether a user is a member of a group. For example, most directories use the “memberOf” attribute. The (memberOf=[#LDAPGroupDN#]) filter contains a Creatio macro and will filter out all objects (users) included in the [#LDAPGroupDN#] group.

Note. Enclose each logical expression in brackets () to ensure the filter works correctly both on Windows and Linux. Read more: Set up Active Directory filters.

Link LDAP elements to Creatio users and roles

In Creatio, you can synchronize the organizational and functional user roles with the Active Directory groups.

You can transfer the company organizational structure and role settings from Active Directory to Creatio after the LDAP synchronization.

Set up the synchronization between Creatio organizational roles and Active Directory groups

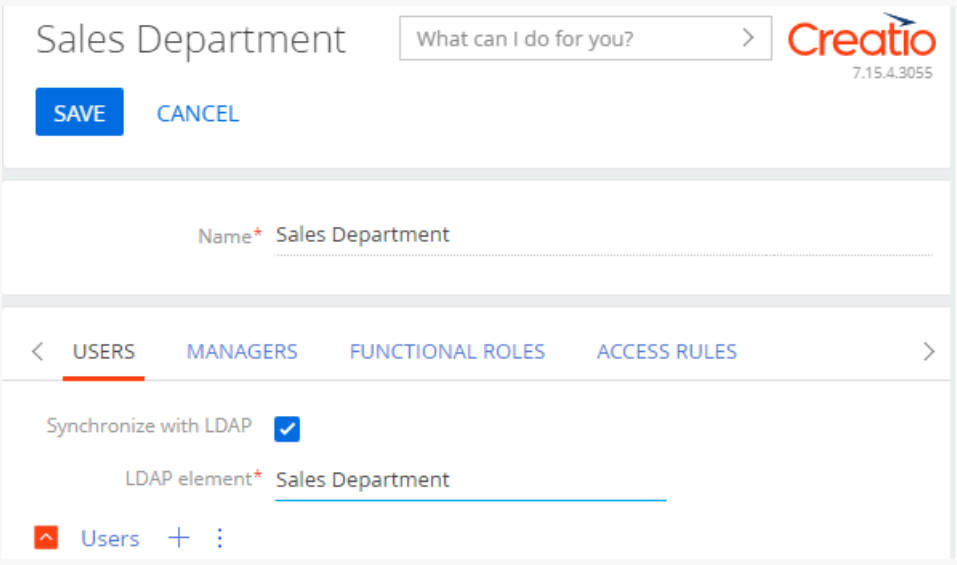
1. Click the button to open the System Designer.
2. Click “Organizational roles” in the “Users and administration” block.
3. Select the needed role from the organizational tree on the newly-opened page (Fig. 3).

   If there is no such role, click [*New*] and select “Organization” or “Division” depending on the type of role you need to add. Specify the group name on the newly-opened page.

Fig. 3 Selecting the organizational role for the synchronization setup

4. Select the [*Synchronize with LDAP*] checkbox in the [*Users*] tab. Select the Active Directory group that corresponds to this Creatio organizational role in the [*LDAP element*] field (Fig. 4).

Fig. 4 Selecting the Active Directory group for the synchronization setup



5. If necessary, add new users by clicking the + button on the [*Users*] detail.

   To synchronize large numbers of users not yet registered in Creatio, import these users from the LDAP directory. Read more: Import new users and roles from Active Directory.

6. Click [*Save*].

As a result, Creatio will synchronize the selected organizational role during the next synchronization session.

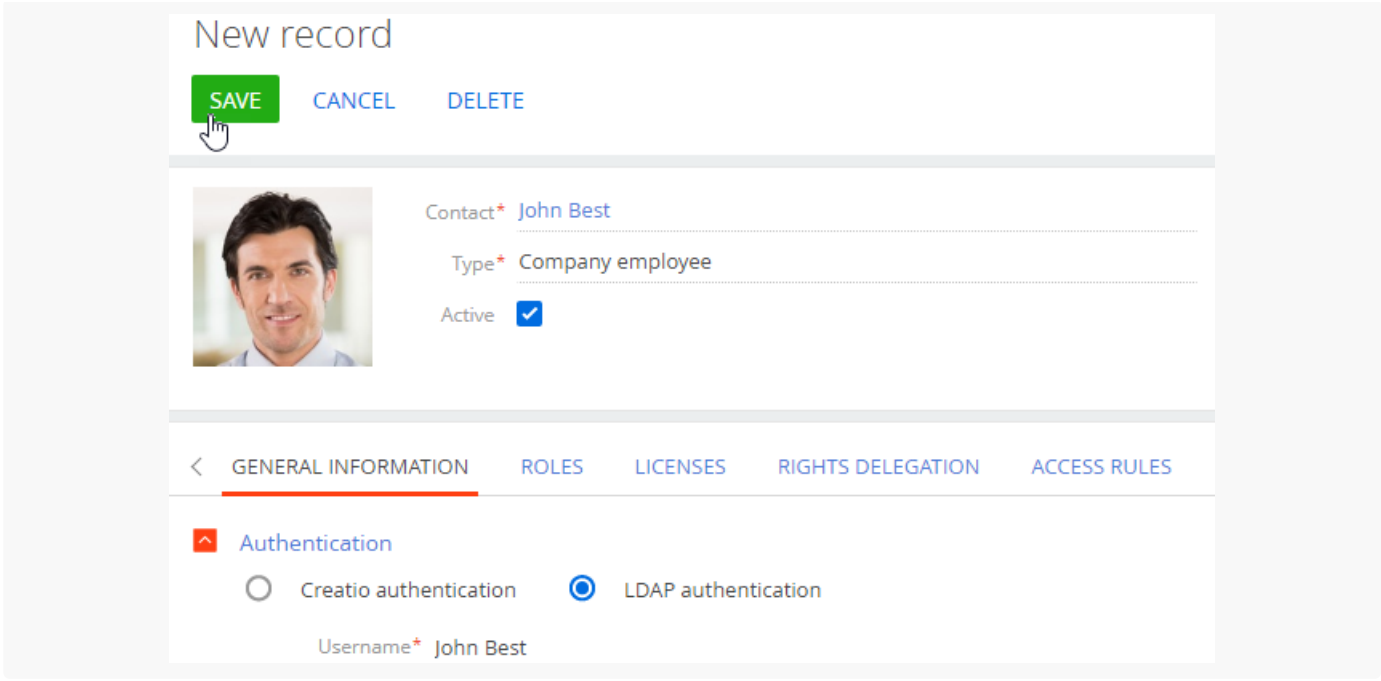
Set up the synchronization between Creatio functional roles and Active Directory groups

1. Click the button to open the System Designer.
2. Click “Functional roles” in the “Users and administration” block.
3. Repeat **steps 3 through 5** of the Creatio organizational roles and **Active Directory** groups synchronization setup, described above.

Connect Creatio user accounts with LDAP users

1. Click the button to open the System Designer.
2. Click “Organizational roles” or “Functional roles” in the “Users and administration” block, depending on what user groups you would like to synchronize.
3. Select the relevant user's role on the newly-opened page.
4. Go to the [*Users*] tab, select the relevant user, and double-click the row to open the record page.
5. Select the [*LDAP authentication*] option in the [*General information*] tab.
6. Select the relevant LDAP user in the [*Login*] field.
7. Click [*Save*] (Fig. 5).

Fig. 5 Connecting a user



This will connect the Creatio user with the LDAP user. The user will be able to log in to Creatio with credentials stored in the LDAP directory, such as the domain login and password.

Creatio will apply all changes made to users and groups in the LDAP directory to the connected user accounts and Creatio organizational structure elements during the synchronization session.

Run the LDAP synchronization

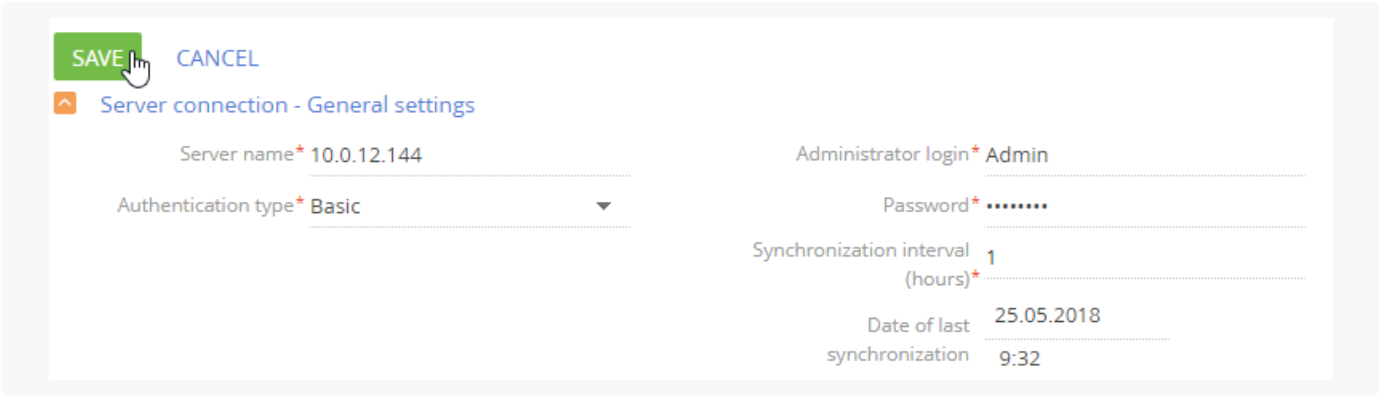
Set up the automatic synchronization

1. Click the button in the top right to open the System Designer.
2. Click “LDAP integration setup” in the “Import and integration” block.
3. Fill out the [*Synchronization interval (hours)*] field on the newly-opened page. Creatio will automatically synchronize users with LDAP after every specified interval.

> **Note.** Learn more about filling out other fields on the [*LDAP integration setup*] page: Set up LDAP integration.

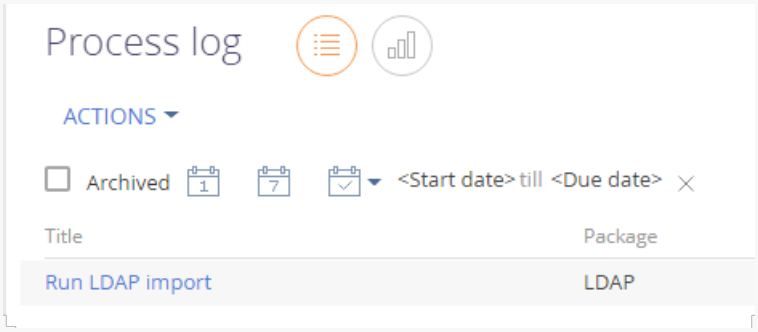
4. Click [*Save*] (Fig. 6).

Fig. 6 Save the filled out LDAP integration setup page



After you save the LDAP integration setup page, Creatio will automatically start the synchronization by running the “Run LDAP import” process (Fig. 7).

Fig. 7 The “Run LDAP import” process



Run the synchronization manually

1. Click the button in the top right to open the System Designer.
2. Click the “Organizational roles” link in the “Users and administration” block.
3. Select the [*Synchronize with LDAP*] action in the section menu (Fig. 8). This will run the “Run LDAP synchronization” process, which will, in turn, call the “Synchronize user data with LDAP” process (Fig. 9).

Fig. 8 The [*Synchronize with LDAP*] action

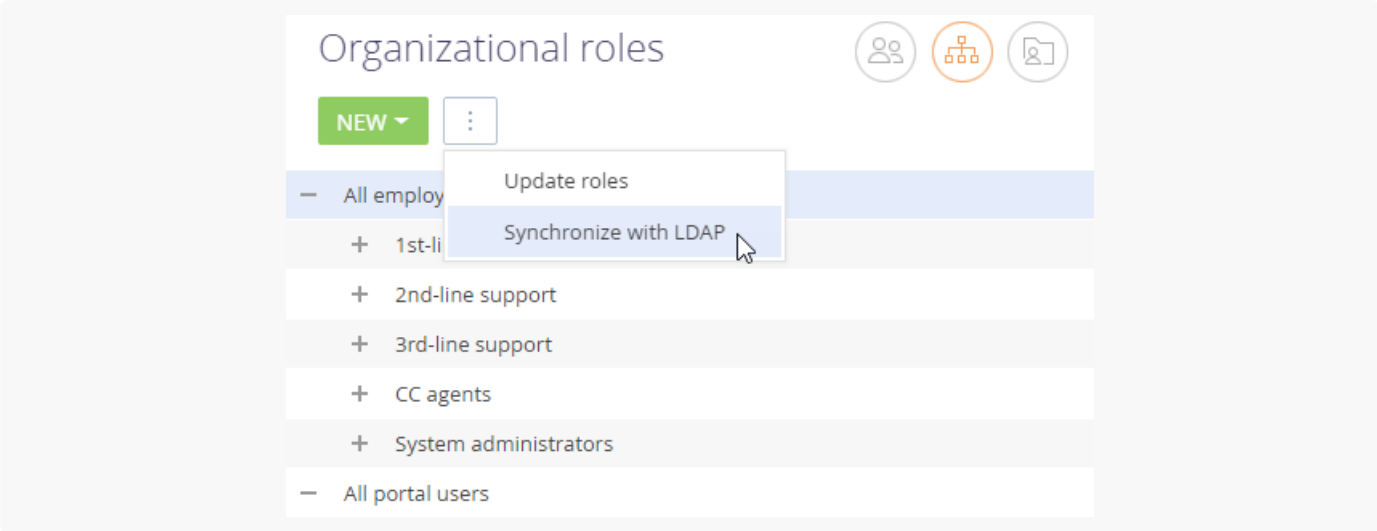
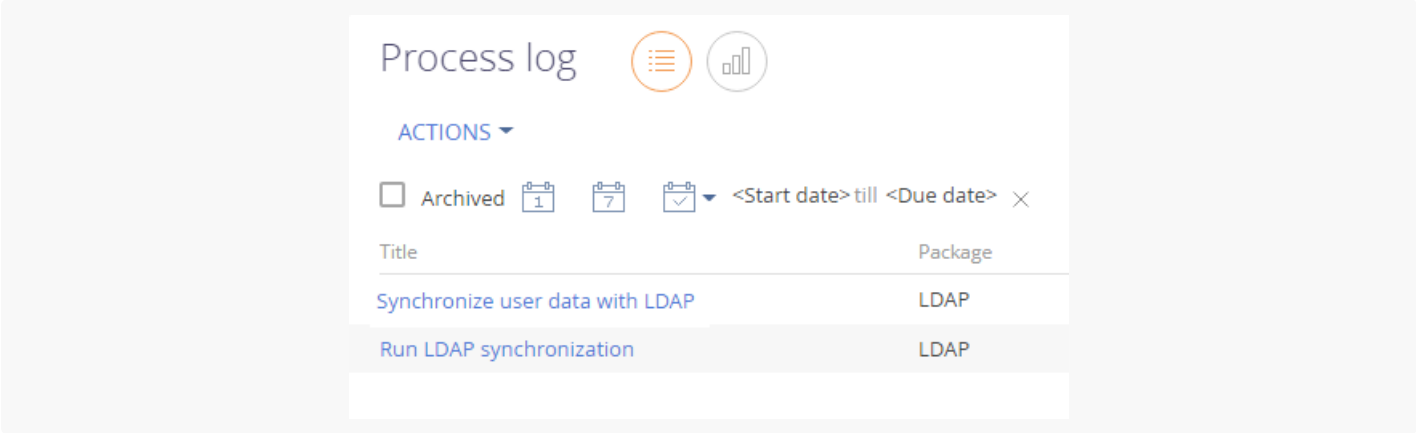


Fig. 9 The “Synchronize user data with LDAP” and “Run LDAP synchronization” processes



Creatio will notify you when the synchronization is complete.

Note. Should the number of synchronized users exceed the number of active licenses, Creatio will notify the system administrators via the communication panel and email.

Synchronization results

- If an LDAP user is no longer among the active users, Creatio will clear the [*Active*] checkbox on the corresponding Creatio user page, and the user will not be able to log in.
- If you activate a previously inactive LDAP user, Creatio will select the [*Active*] box on the corresponding Creatio user page.
- If you rename an LDAP user or a group of users, Creatio will rename the synchronized Creatio users and roles as well.
- If you select the [*Synchronize only groups*] checkbox and exclude an LDAP user from the LDAP group connected with a Creatio organizational structure element, Creatio will deactivate the corresponding user and exclude them from the organizational structure element.
- If you select the [*Synchronize only groups*] check box and include a user to the LDAP group connected with

a Creatio organizational structure element, Creatio will activate the corresponding user and include them in the organizational structure element.

- If you add new unsynchronized users to the synchronized LDAP element, Creatio will import the users.
- If there are Creatio users whom you did not import from LDAP yet their names match LDAP user names, Creatio will not synchronize them.
- If you delete a synchronized LDAP user from a group connected with a Creatio organizational structure element, the user will remain active in Creatio but will not be able to log in.
- Creatio will grant licenses to all synchronized users if you select the corresponding checkbox. Read more: Set up the connection to server.

Set up Active Directory filters

PRODUCTS: ALL CREATIO PRODUCTS

Configure Active Directory filters to set the synchronization parameters for users, groups, and users of a specific group.

The filter format

In general, the Active Directory filter format is as follows:

```
(<operator><filter1><filter2>)
```

Where <filter1> is as follows:

```
(<attribute><operator><value>)
```

You can use any number of filters and operators during the setup. Use the following operators to add and set up filters:

`=` – equal to

`~=` – approximately equal to

`=>` – greater than or equal to

`<=` – less than or equal to

`&` – “AND”

`|` – “OR”

`!` – “NOT”

The values represent the actual values of Active Directory attributes. The values are not case-sensitive and should not be enclosed in quotes. You can also use the wildcard character “*.” For example, this condition will retrieve all elements: `(objectClass=*)`.

Enclose each logical expression in brackets “()” to ensure the filter works correctly both on Windows and Linux.

A correctly set up filter

```
(&(objectClass=group)(!(userAccountControl:1.2.840.113556.1.4.803:=2))(|(cn=szgroup)(cn=CoreCC*)
```

An incorrectly setup filter

```
(&(objectClass=group)(!(userAccountControl:1.2.840.113556.1.4.803:=2))(|(cn=szgroup)(cn=CoreCC*)
```

Filter users

If your company uses the Active Directory service, we recommend the standard active user synchronization filter:

```
(&(objectClass=user)(objectClass=person)(!(objectClass=computer))(!(isDeleted=TRUE)))
```

Where:

`&` – the “AND” operator. Indicates that all filter conditions must be met.

`objectClass=user` – selects all “user” objects in the array.

`objectClass=person` – selects all “person” objects in the array.

`!(objectClass=computer)` – excludes all “computer” objects.

`!(isDeleted=TRUE)` – specifies that the objects are not deleted.

Filter groups

Set up group filtering to synchronize Active Directory users with Creatio organizational structure. The standard user group filter for all active users is as follows:

```
(&(objectClass=group)(!(userAccountControl:1.2.840.113556.1.4.803:=2)))
```

Where:

`&` – the “AND” operator. Indicates that all filter conditions must be met.

`objectClass=group` – selects all “group” objects in the array.

`userAccountControl` – user account control flags, in numerical format.

`:1.2.840.113556.1.4.803:` – the bitwise “AND” in LDAP format.

`2` – the “ACCOUNTDISABLE” flag.

As such, the `(!(userAccountControl:1.2.840.113556.1.4.803:=2))` filter excludes deactivated (inactive) user accounts. Read more in the Microsoft Docs article.

Standard Active Directory group user filters

Besides user and organizational structure filters, you also need to retrieve a list of users included in the Active Directory group and therefore in LDAP. The standard filter that retrieves a list of all group users is as follows:

```
(memberOf=[#LDAPGroupDN#])
```

Where:

`memberOf` – standard Active Directory object attribute that determines the object group.

`#LDAPGroupDN#` – Creatio macro used to retrieve the list of group users with unique DN (Distinguished Name) attribute values.

The macros are not a standard LDAP attribute. Creatio only uses them to form an object selection request. Depending on the AD settings, you can also use the following parameters:

`#LDAPGroupName#` – the name of the group specified in the [*LDAP group name*] field of LDAP integration settings.

`#LDAPGroupIdentity#` – the unique group Id specified in the [*Group Id*] field of LDAP integration settings.

Set up user/group synchronization filters

You can create custom user and group synchronization filters depending on your business needs.

Example. Distinguish between employees with identical full names during the Active Directory synchronization.

To do so, make changes to the user synchronization filter. By default, Creatio uses the CN (Common Name) attribute to select objects. This attribute is required for correct operation as it is connected with the [*User name*] field. You can also include the “displayName” attribute in the filter conditions. This attribute will be unique for each user. As such, you need to synchronize users with the “displayName” attribute. To do this:

1. Open the LDAP synchronization settings.
2. Add the “(displayName=*)” condition to the default user list filter. This condition requires the “displayName” attribute to contain data. The filter will look as follows:

   ```
   (displayName=*)(&(objectClass=user)(objectClass=person)(!(objectClass=computer))(!(isDeleted=
   ```

3. Add the logical “AND” operator to make both filter conditions required:

```
(&(displayName=*)(&(objectClass=user)(objectClass=person)(!(objectClass=computer))(!(isDelete
```

4. Replace the standard filter in the [*List of users*] field with the new filter.
5. Save the settings and run the LDAP synchronization.

Import new users and roles from Active Directory

PRODUCTS: ALL CREATIO PRODUCTS

If you use the Active Directory service, you can import users from your directories to Creatio via LDAP synchronization. This will let you copy users and roles from Active Directory to Creatio.

Prepare the directory for integration

Prepare the directory for integration before you start adding users via LDAP synchronization:

1. Make sure that the users are assigned to the AD user groups you are going to synchronize with Creatio. Creatio will not import Active Directory (AD) users that do not belong to any AD user group. Creatio only imports the organizational structure represented by the AD user groups.
2. Set up LDAP integration. After you click [*Save*] on the LDAP integration setup page, Creatio will run a business process that imports users and roles from LDAP in the background and send you a corresponding notification.

Import new users from LDAP

1. Click the  button to open the System Designer.
2. Navigate to the “Users and administration” block and click “Organizational roles” or “Functional roles” depending on what user groups you would like to synchronize.
   You can also create a new role for the AD user group in your Creatio organizational structure. To do so:
   a. Select a parent role. For example, “All employees” to add regular users or “All portal users” to add portal users → [*New*] → [*Organization*].
   b. Specify the name for your new role. You can use the name of your Active Directory user group or specify a different name.
3. Select the element where Creatio will import the LDAP users in the role tree.
4. Select the [*Synchronize with LDAP*] checkbox in the [*Users*] tab. Select the Active Directory group that corresponds to this Creatio role in the [*LDAP element*] field.
5. Click [*Save*].
6. Run the [*Synchronize with LDAP*] action in the section menu. Once the synchronization is complete, all users from the LDAP server group will be imported to the selected Creatio organizational or functional group.

Note. Should LDAP synchronization result in an error, review the “Synchronize user data with LDAP” process in the [*Process log*] section to find out the reason.

As a result, Creatio will add contacts and user accounts that correspond to the selected LDAP users. Creatio will automatically add new user accounts to the selected organizational structure element. Creatio populates the contact page fields with values of LDAP element attributes specified during the synchronization setup.

Attention. The LDAP user list displays all users regardless of whether they are included in the LDAP element connected to the organizational structure element.

Creatio will only synchronize the users included in the LDAP element that is connected to the organizational structure.

Note. Creatio will license the user account connected to the LDAP user automatically if you select the corresponding checkbox. Read more: Set up the connection to server.

Set up LDAP authentication

PRODUCTS: ALL CREATIO PRODUCTS

Set up user authentication through LDAP on .NET Framework

To enable user authentication through LDAP, modify the Web.config file in the Creatio root folder. Active Directory and OpenLDAP settings are different.

1. Specify “Ldap” and “SspLdapProvider” in the list of available authentication providers. The step is the same for Active Directory and OpenLDAP.

```
<terrasoft>
<auth providerNames="InternalUserPassword,Ldap,SSPLdapProvider" autoLoginProviderNames="" def
<providers>
```

Attention. Upper/lowercase characters must be as in the example. Also, note that the provider names must be separated by commas with no blank spaces.

2. Specify the server IP or URL, as well as user domain parameters in the “Ldap” section. Active Directory and OpenLDAP parameters are different.

For Active Directory

```
<provider name="Ldap" type="Terrasoft.WebApp.Loader.Authentication.Ldap.LdapProvider, Terraso
<parameters>
```

```
...
    <add name="ServerPath" value="testactivedirectory.com" />
    <add name="AuthType" value="Ntlm" />
    <add name="DistinguishedName" value="dc=tscrm,dc=com" />
    <add name="UseLoginUserLDAPEntryDN" value="false" />
    <!--<add name="SearchPattern"
    value="(&amp;(objectCategory=person)(objectClass=user)
    (!(userAccountControl:1.2.840.113556.1.4.803:=2))
    memberOf=CN=SVNUsers,OU=groups,OU=Terrasoft,DC=tscrm,DC=com))" />-->
    <add name="SearchPattern"
    value="(&amp;(sAMAccountName={0})(objectClass=person))" />
    <!--With Kerberos authentication-->
    <add name="KeyDistributionCenter" value="ctl.com" />
</parameters>
```

For OpenLDAP

```
<provider name="Ldap" type="Terrasoft.WebApp.Loader.Authentication.Ldap.LdapProvider, Terraso
<parameters>
...
    <add name="ServerPath" value="testopenldap.com" />
    <add name="AuthType" value="Basic" />
    <add name="DistinguishedName" value="dc=example,dc=org" />
    <add name="UseLoginUserLDAPEntryDN" value="true" />
    <add name="SearchPattern"
    value="(&amp;(uid={0})(objectClass=inetOrgPerson))" />
    <!--With Kerberos authentication-->
    <add name="KeyDistributionCenter" value="ctl.com" />
</parameters>
```

- **ServerPath** – the LDAP server domain name. It must be a URL, not an IP address.
- **KeyDistributionCenter** – the domain name. It must be a URL, not an IP address.

Note. If you select “Kerberos” authentication type, make sure your Creatio application server is joined to the same domain as the LDAP server and the key distribution center.

3. Specify the server IP or URL, as well as portal user domain parameters in the “SspLdapProvider” section. The step is the same for Active Directory and OpenLDAP:

```
<provider name="SSPLdapProvider" type="Terrasoft.WebApp.Loader.Authentication.SSPUserPassword
<parameters>
...
     <add name="ServerPath" value="ldapserver.domain.com" />
```

```
...
     <add name="DistinguishedName" value="dc=domain, dc=com" />
...
</parameters>
```

4. Save the changes in the Web.config file.
5. **Additional step for OpenLDAP**: before you synchronize with the OpenLDAP server, specify the “true” value for “UseLoginUserLDAPEntryDN” in the Web.config file of Terrasoft.WebApp.

```
<appSettings>
...
    <add key="UseLoginUserLDAPEntryDN" value="true" />
```

This setting ensures that Creatio does not us an empty [*LDAPEntryDN*] field in the [*SysAdminUnit*] table to synchronize the users. An empty [*LDAPEntryDN*] field is known to cause authentication issues.

Set up user authentication through LDAP on .NET Core

To enable user authentication through LDAP, modify the Terrasoft.WebHost.dll.config file in the Creatio root folder. Active Directory and OpenLDAP settings are the same.

1. Specify “Ldap” in the list of available authentication providers. Add the “SspLdapProvider” provider to allow portal users to log in to Creatio:

```
<terrasoft>
<auth providerNames="InternalUserPassword,Ldap,SspLdapProvider" autoLoginProviderNames="" def
<providers>
```

Attention. Upper/lowercase characters must be as in the example. Also note that the provider names must be separated by commas with no blank spaces.

2. Specify the “Ldap” authentication provider settings:

```
<provider name="LdapProvider" type="Terrasoft.Authentication.Core.Ldap.NetStandardLdapProvide
<parameters>
    <add name="ServerPath" value="testldap.com" />
    <add name="DistinguishedName" value="dc=ctl,dc=com" />
    <add name="UseLoginUserLDAPEntryDN" value="false" />
    <add name="SearchPattern" value="(&amp;(sAMAccountName={0})(objectClass=person))" />
    <!--With Kerberos authentication-->
    <add name="KeyDistributionCenter" value="ctl.com" />
    <!--When using LDAPS-->
    <add name="SecureSocketLayer" value="false" />
    <add name="CertificateFileName" value="" />
```

```
</parameters></provider>
```

- **ServerPath** is the LDAP server domain name. It must be a URL address, not an IP address.
- **KeyDistributionCenter** is the domain name. It must be a URL address, not an IP address.

> **Note.** If you select “Kerberos” authentication type, make sure your Creatio application server is joined to the same domain as the LDAP server and the key distribution center.

To use the **secure LDAPS protocol**, specify the following parameters in the authentication provider settings:

- **SecureSocketLayer** is the flag that enables LDAPS.
- **CertificateFileName** is the name of the SSL certificate that validates the LDAPS connection. The certificate must be located in the Creatio root folder. This is a requried parameter if “SecureSocketLayer=true” is specified. For instance:

```
<add name="CertificateFileName" value="ldap_certificate_example.cer" />
<add name="SecureSocketLayer" value="true" />
```

3. Specify the server IP or URL, as well as portal user domain parameters in the “SspLdapProvider” section.

```
<provider name="SSPLdapProvider" type="Terrasoft.WebApp.Loader.Authentication.SSPUserPassword
<parameters>
    <add name="ServerPath" value="ldapserver.domain.com" />
...
    <add name="DistinguishedName" value="dc=domain, dc=com" />
…
</parameters>
```

4. Save the changes in the Terrasoft.WebHost.dll.config file.

Set up the authentication providers

The authentication provider setup is the same for Creatio **.NET Framework** and Creatio **.NET Core**. Modify the following files in the Creatio root directory:

- **Web.config** for Creatio **.NET Framework**.
- **Terrasoft.WebHost.dll.config** for Creatio **.NET Core**.

Open the file in a text editor and specify the authentication providers:

```
auth providerNames="InternalUserPassword,SSPLdapProvider,Ldap" autoLoginProviderNames="NtlmUser,
```

- **InternalUserPassword** – the default provider. If you would like to provide NTLM authentication only to the users not synchronized with LDAP, do not specify additional values for the [*providerNames*] parameter.
- **Ldap** – add this provider to the [*providerNames*] parameter value to provide NTLM authentication to the users synchronized with LDAP.
- **SSPLdapProvider** – add this provider to the [*providerNames*] parameter value to provide NTLM authentication to the self-service portal's users synchronized with LDAP.
- **NtlmUser** – add this provider to the [*autoLoginProviderNames*] parameter value to provide NTLM authentication to the main application's users regardless of their LDAP synchronization status and the authentication type configured for the users in Creatio.
- **SSPNtlmUser** – add this provider to the [*autoLoginProviderNames*] parameter value to provide NTLM authentication to the self-service portal's users regardless of their LDAP synchronization status and the authentication type configured for the Creatio users.
- The order of records in the [*autoLoginProviderNames*] parameter defines the order in which Creatio checks if its users are available in the main application's user list (NtlmUser) or the self-service portal's user list (SSPNtlmUser). For example, if you would like Creatio to check the main application's user list first, put the **NtlmUser** provider at the head of the list of [*autoLoginProviderNames*] parameter values.

Attention. Only specify the [*SSPNtlmUser*] provider as the **autoLoginProviderNames** parameter's value if you also specify the **NtlmUser** provider. However, you can use the **NtlmUser** parameter without the other providers.

Set up the domain authentication

If you would like to activate the **pass-through authentication** that lets users authenticate in Creatio without visiting the login page, specify the “true” value for the [*UsePathThroughAuthentication*] parameter of the <appSettings> element:

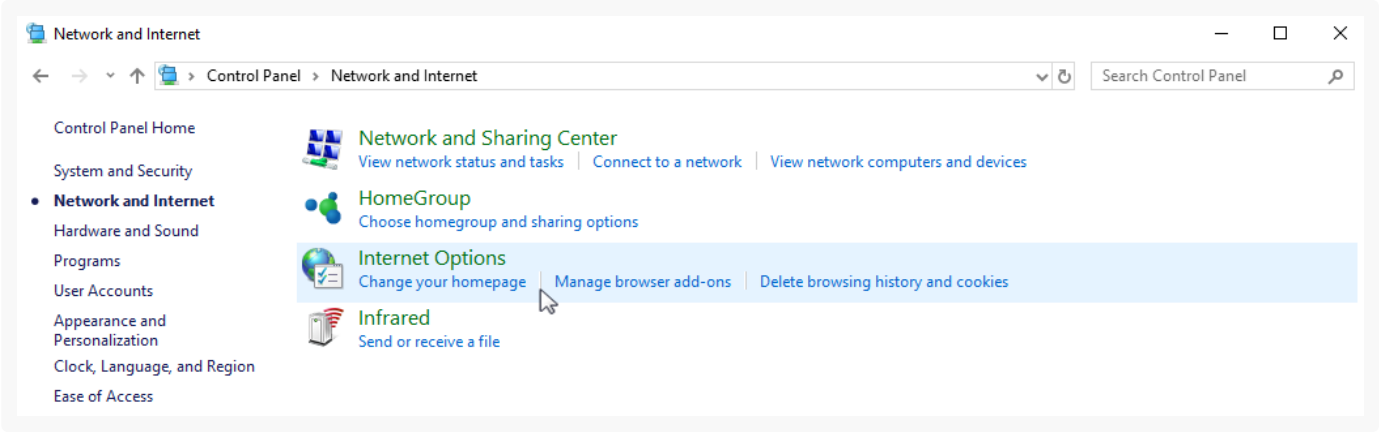
```
<appSettings> <add key="UsePathThroughAuthentication" value="true" /> ... </appSettings>
```

If you would like to **display the login page** with the available [*Log in as domain user*] link, specify the “false” value for the [*UsePathThroughAuthentication*] parameter. The pass-through authentication will be performed only when accessing the main Creatio page. Add “/Login/NuiLogin.aspx” to the Creatio website address to display the login page.

As a result, users will be able to log in to Creatio as domain users. They may still be required to enter their credentials in a domain authentication window, which will pop up on a login attempt. Modify Windows settings to prevent the domain authentication window from being displayed:

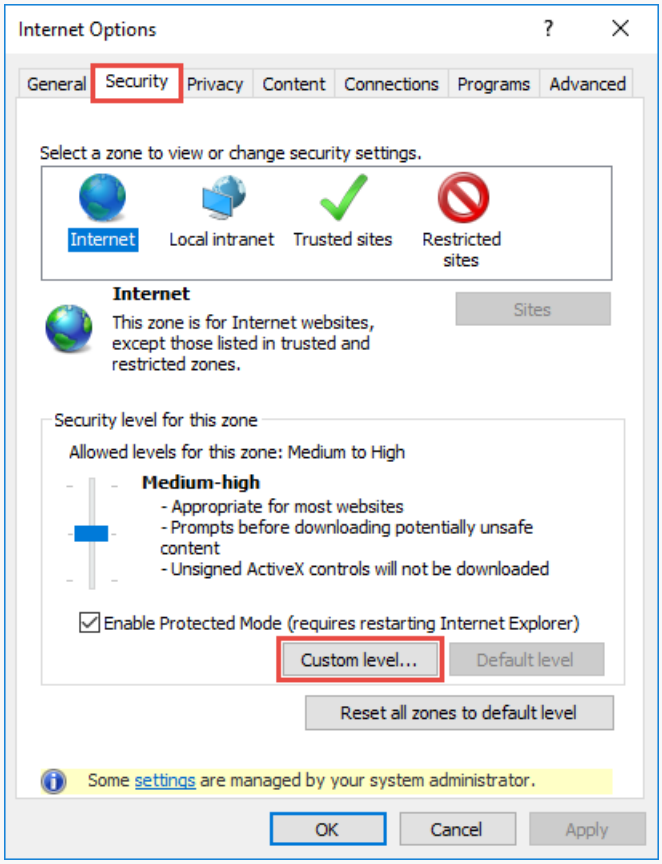
1. Click “Start” → “Settings” → “Control Panel” → “Network and Internet” menu. Select “Internet options” (Fig. 1).

Fig. 1 Modifying Windows settings



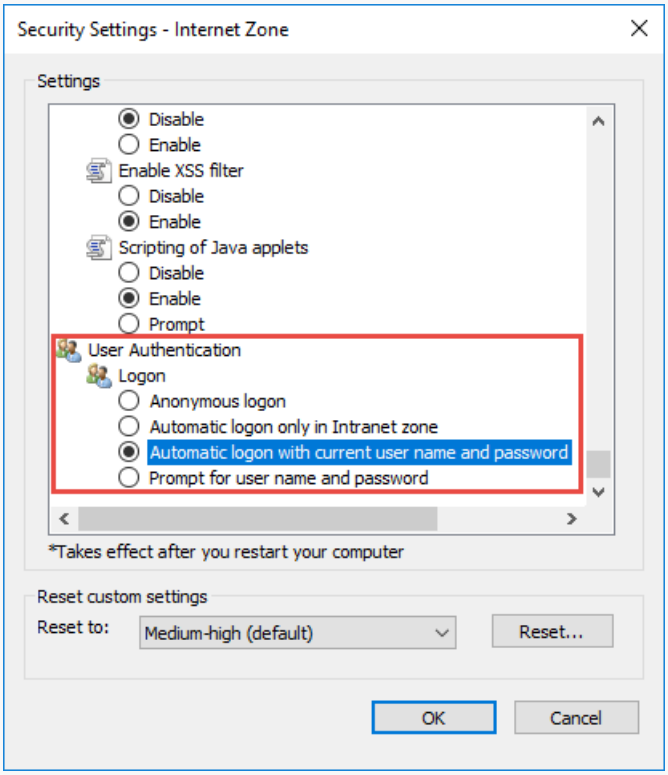
2. This will open a new window. Select the “Security” tab and click “Custom level” to go to security settings (Fig. 2).

Fig. 2 Security settings



3. Select the “Automatic logon with current user name and password” authentication methods in the “User authentication” settings group (Fig. 3).

Fig. 3 Selecting the authentication method



4. Click “OK.”

As a result, the domain authentication window will not pop up and the users will not have to re-enter their domain credentials each time they access Creatio.

LDAP synchronization FAQ

PRODUCTS: ALL CREATIO PRODUCTS

Why did Creatio not import all users from the LDAP directory?

There could be several reasons:

- There are directory users with a matching “User name” attribute who also have empty or matching “Email” and “Phone number” attributes. Creatio checks for duplicates by “User name”, “Email” and “Phone number” attributes automatically during LDAP synchronization.
- The date in the “Maximum modification date of LDAP entry” (“LDAPEntryMaxModifiedOn” code) Creatio system setting is later than the date in “whenChanged” LDAP user attribute. Creatio will import a user only if the date in “Maximum modification date of LDAP entry” is earlier than the date in “whenChanged” LDAP user attribute.

Why did Creatio not import all Active Directory users after the LDAP synchronization?

Active Directory page size may be shorter than the number of users. Since Creatio does not support pagination when synchronizing users through LDAP, it will only process records from the first page. To resolve this issue,

increase the “MaxPageSize” value in Active Directory so all the users fit on the first page.

Why is it impossible for a user to log in under their domain account after setting up LDAP?

To resolve this issue in Creatio **on-site**, navigate to the website's roote directory, open the Web.config file, and specify the authentication providers in the “auth providerNames” parameter:

```
auth providerNames = "InternalUserPassword,Ldap,SSPLdapProvider"
```

After you save the changes, restart the LDAP synchronization.

To resolve this issue in Creatio **in the cloud**, contact Creatio support.

Is it possible to connect a user imported from Active Directory to a specific Creatio account?

- If the user's “Company name” attribute matches a Creatio account name exactly, Creatio will automatically connect the imported user to that account.
- If the account specified in the “Company name” attribute does not match any Creatio account names verbatim, Creatio will automatically connect the imported user to “Our company”.

Why is it impossible to import users from the “Domain users” group?

“Domain users” group is a primary group. The “memberOf” attribute does not display primary groups. To import these users, add them to a different, non-primary group.

What causes error “22021: invalid byte sequence for encoding "UTF8": 0x00” when synchronizing Active Directory by LDAP?

This error occurs in Creatio with PostgreSQL. It is caused by system groups that support pre-2000 Windows versions in the imported data. To resolve this issue, exclude those system groups from synchronization and change the group filter to:

```
(&(objectClass=group)(!userAccountControl:1.2.840.113556.1.4.803:=2)(!(isCriticalSystemObject=TR
```

What causes error “Cannot insert duplicate key row in object 'dbo.SysAdminUnit' with unique index

'IUSysAdminunitNameDomain'. The duplicate key value is (...)”?

This synchronization error occurs if there is a directory user you have previously added to Creatio manually.

How can I set up a specific LDAP filter?

You can learn more about setting up LDAP filters in Internet Engineering Task Force's String Representation of Search Filters manual. You may also find Microsoft's Active Directory: LDAP Syntax Filters documentation useful.