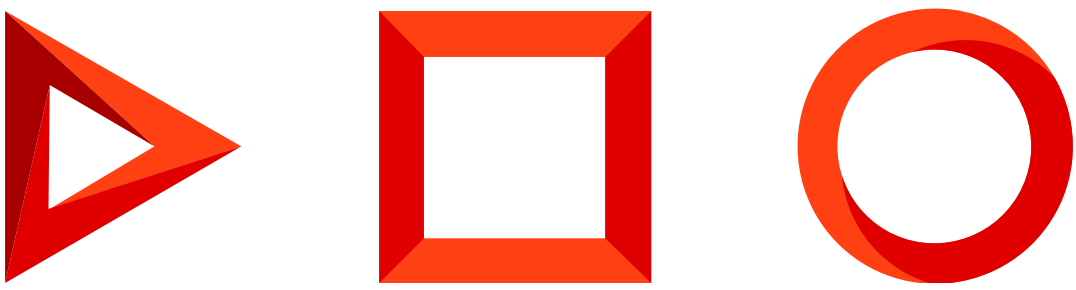
Creatio Academy

Настройка аутентификации

Настроить аутентификацию с LDAP

Версия 8.0



Эта документация предоставляется с ограничениями на использование и защищена законами об интеллектуальной собственности. За исключением случаев, прямо разрешенных в вашем лицензионном соглашении или разрешенных законом, вы не можете использовать, копировать, воспроизводить, переводить, транслировать, изменять, лицензировать, передавать, распространять, демонстрировать, выполнять, публиковать или отображать любую часть в любой форме или посредством любые значения. Обратный инжиниринг, дизассемблирование или декомпиляция этой документации, если это не требуется по закону для взаимодействия, запрещены.

Информация, содержащаяся в данном документе, может быть изменена без предварительного уведомления и не может гарантировать отсутствие ошибок. Если вы обнаружите какие-либо ошибки, сообщите нам о них в письменной форме.

© 2022 Terrasoft. Все права защищены.

Содержание

© 2022 Terrasoft. Все права защищены.

Настроить аутентификацию с LDAP

ПРОДУКТЫ: ВСЕ ПРОДУКТЫ

Настроить аутентификацию пользователей через LDAP на .NET Framework

Для включения возможности авторизации пользователей с помощью LDAP внесите изменения в файл Web.config в корневой папке приложения. Настройки для Active Directory и OpenLDAP имеют некоторые различия.

1. Укажите “Ldap” и “SspLdapProvider” в списке доступных провайдеров авторизации. Шаг выполняется одинаково для Active Directory и OpenLDAP:

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

Важно. Необходимо соблюдать регистр согласно примеру. Также обратите внимание, что названия провайдеров должны быть приведены через запятую и без пробелов.

2. Укажите IP или адрес сервера, а также параметры домена для пользователей в секции “Ldap”. Параметры для Active Directory и OpenLDAP различаются.

Для 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))" />
    <!--При “Kerberos” аутентификации-->
    <add name="KeyDistributionCenter" value="ctl.com" />
</parameters>
```

© 2022 Terrasoft. Все права защищены.

Для 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))" />
    <!--При “Kerberos” аутентификации-->
    <add name="KeyDistributionCenter" value="ctl.com" />
</parameters>
```

- **ServerPath** — доменное имя (URL-адрес) LDAP сервера, но не IP-адрес.
- **KeyDistributionCenter** — доменное имя (URL-адрес), но не IP-адрес.

На заметку. Если вы выберете тип аутентификации “Kerberos”, то сервер приложений Creatio должен быть включен в домен, в котором находится LDAP-сервер и центр распределения ключей.

3. Укажите IP или адрес сервера, а также параметры домена для портальных пользователей в секции “SspLdapProvider”. Шаг выполняется одинаково для Active Directory и 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. Сохраните изменения в файле Web.config.
5. **Шаг только для настройки OpenLDAP**: перед синхронизацией с OpenLDAP-сервером укажите в файле Web.config в Terrasoft.WebApp значение для “UseLoginUserLDAPEntryDN”.

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

© 2022 Terrasoft. Все права защищены.

Без данной настройки пользователи будут синхронизироваться без значений в поле [*LDAPEntryDN*] таблицы [*SysAdminUnit*], что приведет к проблемам с авторизацией.

Настроить аутентификацию пользователей через LDAP на .NET Core

Для включения возможности авторизации пользователей с помощью LDAP внесите изменения в файл Terrasoft.WebHost.dll.config в корневой папке приложения. Настройки для Active Directory и OpenLDAP одинаковы.

1. Укажите “Ldap” в списке доступных провайдеров авторизации. Чтобы портальные пользователи могли войти в систему, добавьте провайдер “SspLdapProvider”:

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

Важно. Необходимо соблюдать регистр согласно примеру. Также обратите внимание, что названия провайдеров должны быть приведены через запятую и без пробелов.

2. Укажите настройки провайдера аутентификации “Ldap”:

```
<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))" />
    <!--При “Kerberos” аутентификации-->
    <add name="KeyDistributionCenter" value="ctl.com" />
    <!--При использовании LDAPS-->
    <add name="SecureSocketLayer" value="false" />
    <add name="CertificateFileName" value="" />
</parameters></provider>
```

- **ServerPath** — доменное имя (URL-адрес) LDAP сервера, но не IP-адрес.
- **KeyDistributionCenter** — доменное имя (URL-адрес), но не IP-адрес.

На заметку. Если вы выберете тип аутентификации “Kerberos”, то сервер приложений Creatio должен быть включен в домен, в котором находится LDAP-сервер и центр распределения ключей.

© 2022 Terrasoft. Все права защищены.

Чтобы использовать **защищенный протокол LDAPS**, в настройках провайдера аутентификации укажите следующие параметры:

- **SecureSocketLayer** — флаг для использования LDAPS.
- **CertificateFileName** — имя сгенерированного SSL-сертификата для валидации LDAPS-подключения. Данный сертификат должен находиться в корне приложения. Этот параметр обязательный для заполнения при SecureSocketLayer=true, например:

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

3. Укажите IP или адрес сервера, а также параметры домена для портальных пользователей в секции “SspLdapProvider”:

```
<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. Сохраните изменения в файле Terrasoft.WebHost.dll.config.

Настроить провайдеры аутентификации

Настройка провайдеров аутентификации осуществляется одинаково для приложений на **.NET Framework** и **.NET Core**. Настройки вносятся в следующих файлах, которые находятся в корневой директории приложения:

- **Web.config** для приложения на **.NET Framework**.
- **Terrasoft.WebHost.dll.config** для приложения на **.NET Core**.

Для настройки откройте файл в текстовом редакторе и укажите провайдеров аутентификации:

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

- **InternalUserPassword** — провайдер, указанный по умолчанию. Если вы хотите предоставить возможность аутентификации по NTLM-протоколу только пользователям, которые не синхронизированы с LDAP, то не указывайте для параметра [*providerNames*] дополнительные значения.
- **Ldap** — добавьте к значениям параметра [*providerNames*] данный провайдер, чтобы предоставить возможность аутентификации по NTLM-протоколу пользователям приложения, которые синхронизированы с LDAP.

© 2022 Terrasoft. Все права защищены.

- **SSPLdapProvider** — добавьте к значениям параметра [*providerNames*] данный провайдер, чтобы предоставить возможность аутентификации по NTLM-протоколу пользователям портала самообслуживания, которые синхронизированы с LDAP.
- **NtlmUser** — добавьте к значениям параметра [*autoLoginProviderNames*] данный провайдер, чтобы предоставить возможность аутентификации по NTLM-протоколу пользователям приложения, независимо от того, синхронизированы ли они с LDAP и какой тип аутентификации установлен для данных пользователей в Creatio.
- **SSPNtlmUser** — добавьте к значениям параметра [*autoLoginProviderNames*] данный провайдер, чтобы предоставить возможность аутентификации по NTLM-протоколу пользователям портала самообслуживания, независимо от того, синхронизированы ли они с LDAP и какой тип аутентификации установлен для данных пользователей в Creatio.
- Порядок записи провайдеров параметра [*autoLoginProviderNames*] определяет, в каком порядке выполняется проверка наличия пользователя системы среди пользователей приложения (NtlmUser) или среди пользователей портала (SSPNtlmUser). Например, чтобы проверка осуществлялась в первую очередь среди пользователей основного приложения, укажите провайдер **NtlmUser** первым в списке значений параметра [*autoLoginProviderNames*].

Важно. Вы можете указать в качестве значения параметра [*autoLoginProviderNames*] провайдер **SSPNtlmUser**, только если указан дополнительно провайдер **NtlmUser**. Существует возможность использовать отдельно только провайдер **NtlmUser**.

Настроить доменную авторизацию

Если вы хотите активировать **сквозную аутентификацию**, чтобы пользователь имел возможность авторизоваться в Creatio, минуя страницу входа, то укажите значение “true” для параметра [*UsePathThroughAuthentication*] элемента <appSettings>:

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

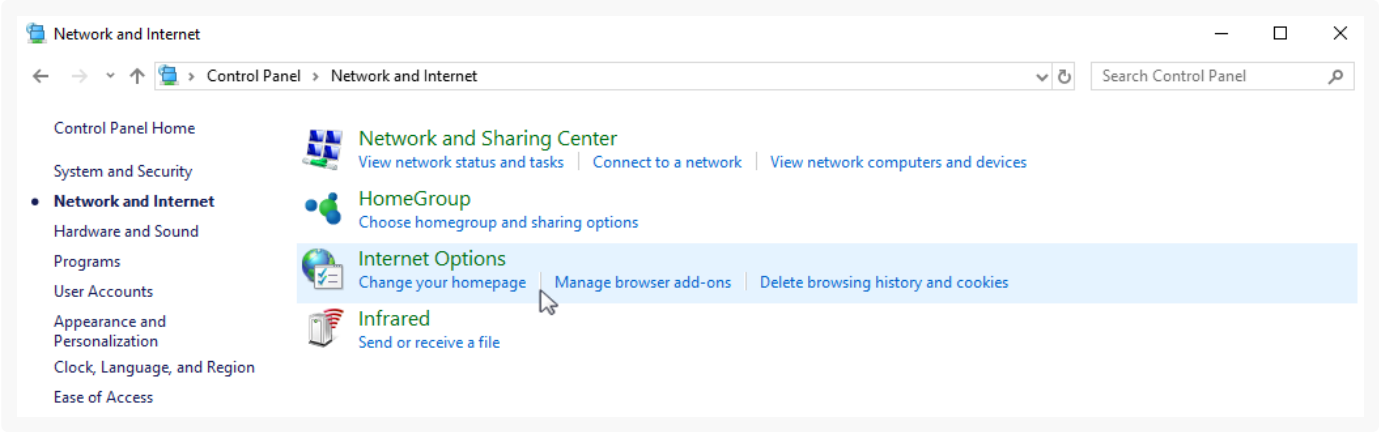
Для **отображения страницы входа** в систему с доступной ссылкой [*Войти под доменным пользователем*] укажите значение “false” для параметра [*UsePathThroughAuthentication*]. При этом сквозная аутентификация будет выполняться лишь при переходе на главную страницу приложения. Чтобы отобразить страницу входа, добавьте запись /Login/NuiLogin.aspx к адресу сайта.

Если после выполнения описанных действий при первой попытке входа в систему отображается окно доменной авторизации, то необходимо дополнительно настроить свойства обозревателя Windows. Чтобы в дальнейшем окно доменной авторизации не отображалось:

1. В меню “Пуск” (“Start”) → “Параметры” (“Settings”) → “Control Panel” (“Панель управления”) → “Сеть и Интернет” (“Network and Internet”) выберите пункт “Свойства обозревателя” (“Internet options”) (Рис. 1).

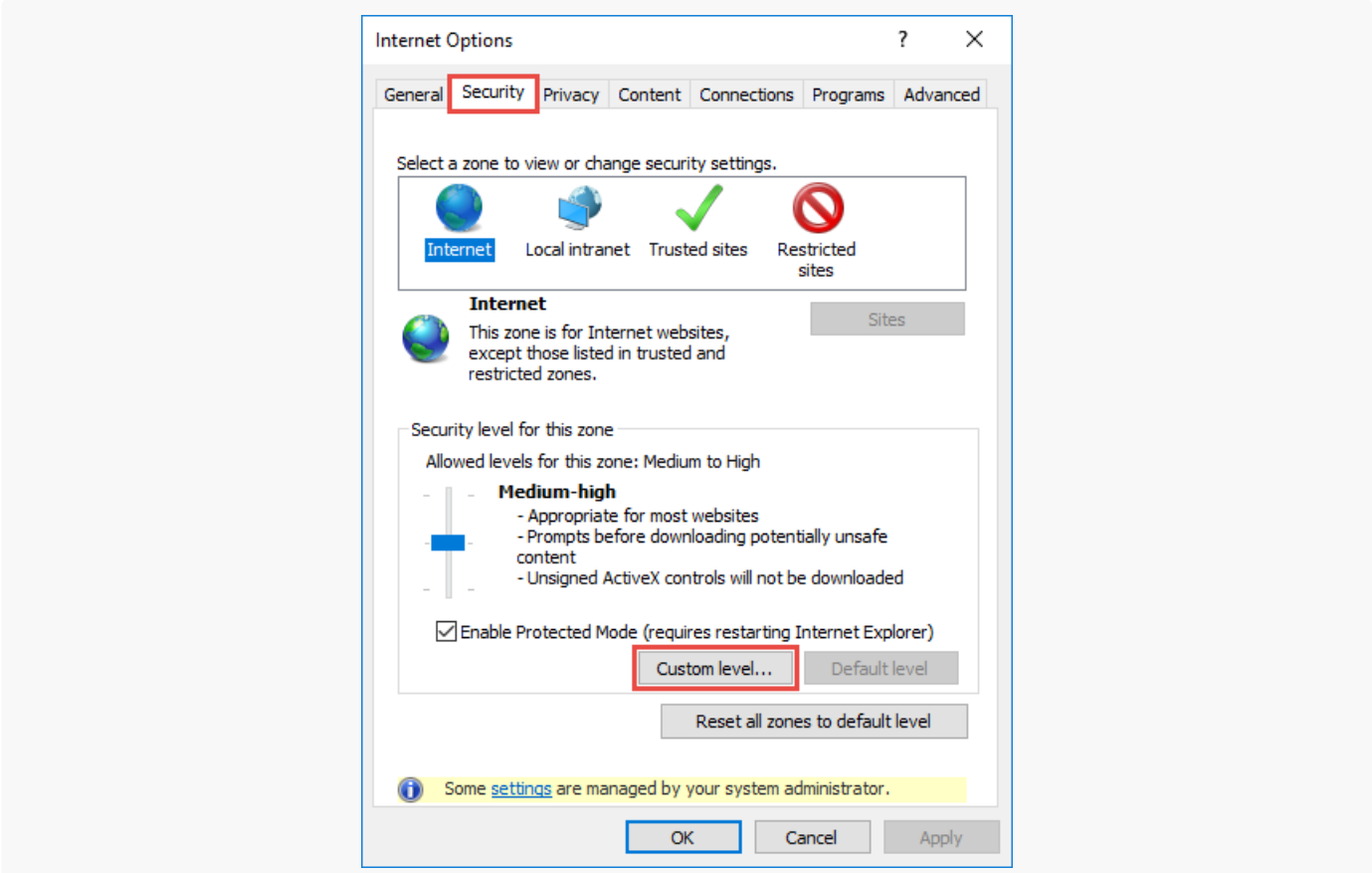
Рис. 1 — Настройка свойств обозревателя

© 2022 Terrasoft. Все права защищены.



2. В открывшемся окне перейдите на вкладку “Безопасность” (“Security”) и по кнопке “Другой” (“Custom level”) перейдите к настройкам безопасности (Рис. 2).

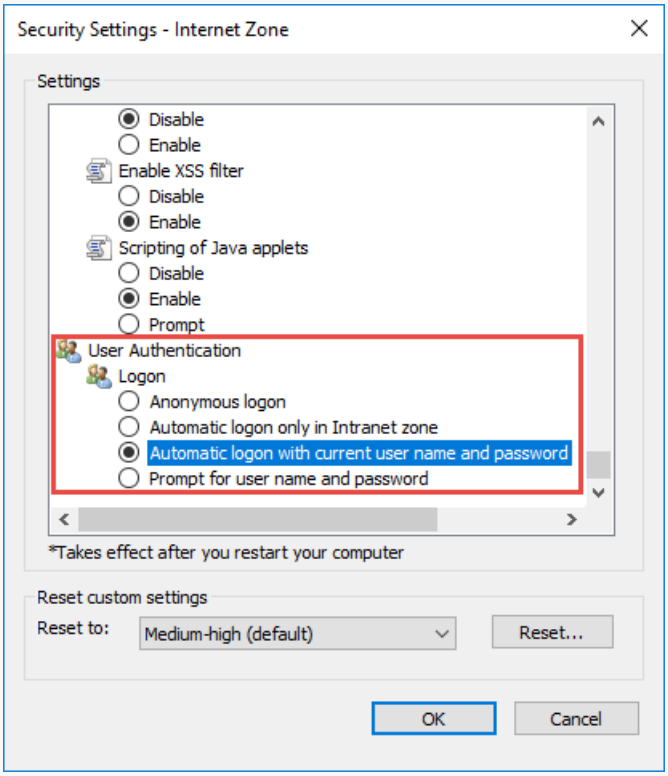
Рис. 2 — Настройки безопасности



3. В группе настроек “Проверка подлинности пользователя” (“User Authentication”) выберите способ авторизации “Автоматический вход с текущим именем пользователя и паролем” (“Automatic logon with current user name and password”) (Рис. 3).

Рис. 3 — Выбор способа авторизации

© 2022 Terrasoft. Все права защищены.



4. Нажмите “OK”.

В результате выполненных настроек окно доменной авторизации не будет отображаться при входе в систему.

© 2022 Terrasoft. Все права защищены.