

# Аутентификация в приложении

Аутентификация Windows

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.

# Содержание

<b>Аутентификация Windows</b>	<b>4</b>
Как работает аутентификация Windows	4
Настроить аутентификацию Windows в IIS	5
Настроить файл Web.config приложения-загрузчика	6

# Аутентификация Windows

ПРОДУКТЫ: **ВСЕ ПРОДУКТЫ**

## Как работает аутентификация Windows

Аутентификации Windows (NTLM) и LDAP могут работать независимо друг от друга. Аутентификация Windows требует ввода учетных данных пользователя в окне авторизации браузера. А аутентификация LDAP использует проверку пароля пользователя на сервере Active Directory. Аутентификации Windows (NTLM) и LDAP работают вместе, когда пользователь нажимает ссылку “Войти под доменным пользователем”, и его аккаунт синхронизирован с LDAP.

**На заметку.** Аутентификация Windows доступна только для on-site приложений в связи с особенностями cloud-архитектуры.

При попытке пользователя войти в систему, используя доменные учетные данные, выполняется следующий алгоритм аутентификации:

1. Выполняется проверка авторизации пользователя в домене.
2. Имя и пароль текущего доменного пользователя считываются из cookie-файла, если эти данные записаны в cookie. В противном случае отображается браузерное окно ввода учетных данных.  
Дальнейшие шаги зависят от того, синхронизирован ли пользователь с каталогом LDAP.

1. Если пользователь не синхронизирован с LDAP:
  - Выполняется проверка подлинности пользователя путем сравнения логина и пароля, записанных в cookie-файл, с учетными данными соответствующей записи Creatio. Таким образом, для возможности Windows-аутентификации пользователя, не синхронизированного с LDAP, необходимо, чтобы при регистрации данного пользователя в Creatio были указаны те же логин и пароль, которые используются им в домене.
  - Если по результатам проверки данные совпадают и учетная запись пользователя [лицензирована](#), осуществляется авторизация в приложении.
  - Если пользователь синхронизирован с LDAP:
  - Браузер посылает запрос в службу Active Directory для проверки подлинности пользователя.
  - Запрос возвращает учетные данные текущего доменного пользователя, которые сравниваются с логином и паролем, записанными в cookie-файл.
  - Если данные совпадают и учетная запись пользователя [лицензирована](#), то осуществляется авторизация в приложении.

**На заметку.** Проверка подлинности выполняется как среди пользователей основного приложения, так и среди пользователей портала самообслуживания. Порядок проверки настраивается в файле Web.config приложения-загрузчика. Подробнее: [Настроить файл Web.config приложения-загрузчика](#).

Для использования функциональности аутентификации Windows по протоколу NTLM необходимо зарегистрировать пользователей в системе вручную или импортировать из LDAP и предоставить им лицензии. Также необходимо, чтобы у пользователей в настройках браузера была разрешена запись локальных данных в cookie-файлы.

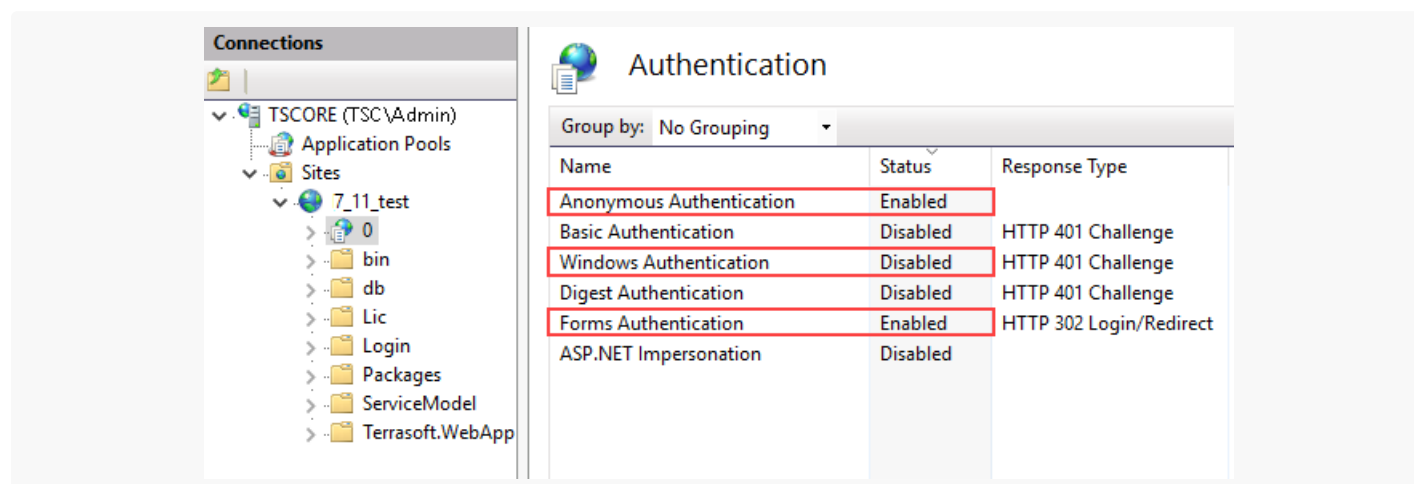
Настройка выполняется на сервере, где развернуто приложение, и включает в себя:

- Настройку сервера IIS, которая активирует аутентификацию по протоколу NTLM. Подробнее: [Настроить аутентификацию Windows в IIS](#).
- Настройку файла Web.config приложения-загрузчика, которая определяет провайдеров аутентификации и порядок проверки наличия пользователей среди зарегистрированных в Creatio. Подробнее: [Настроить файл Web.config приложения-загрузчика](#).

## Настроить аутентификацию Windows в IIS

Для приложения-загрузчика и веб-приложения включите анонимную аутентификацию и аутентификацию форм (Рис. 1).

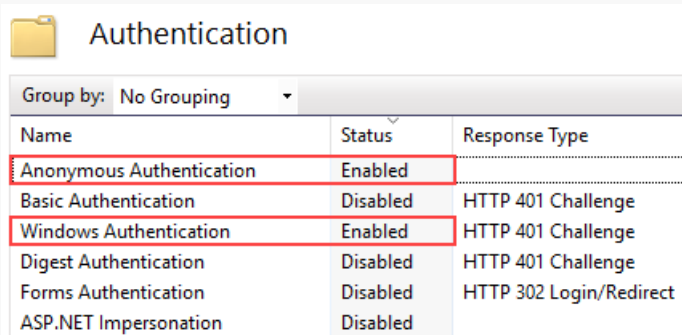
Рис. 1 — Настройки для приложения-загрузчика в настройках IIS



**На заметку.** Обратите внимание, что необходимо выключить настройку “Windows Authentication”, которая в IIS включена по умолчанию.

Для директории Login внутри приложения-загрузчика отключите аутентификацию форм и включите анонимную аутентификацию и аутентификацию Windows (Рис. 2).

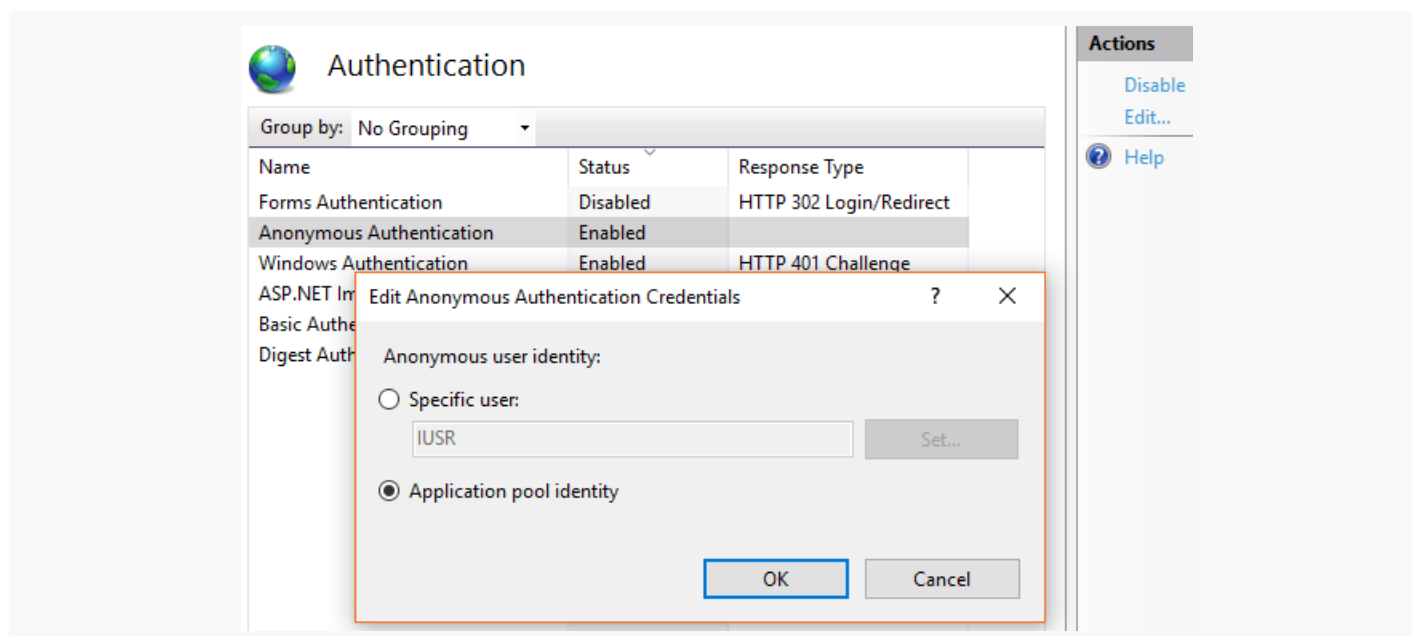
Рис. 2 — Настройки для директории Login



Name	Status	Response Type
Anonymous Authentication	Enabled	
Basic Authentication	Disabled	HTTP 401 Challenge
Windows Authentication	Enabled	HTTP 401 Challenge
Digest Authentication	Disabled	HTTP 401 Challenge
Forms Authentication	Disabled	HTTP 302 Login/Redirect
ASP.NET Impersonation	Disabled	

Обратите внимание, что анонимная аутентификация приложения-загрузчика и рабочих приложений должна выполняться под пользователем Application Pool Identity. Для этого перейдите в окно редактирования данных входа настроек Authentication по кнопке [ *Edit* ] в боковом меню [ *Actions* ] менеджера IIS, и выберите пользователя “Application Pool Identity” (Рис. 3).

Рис. 3 — Указание пользователя для анонимной аутентификации в настройках IIS



**На заметку.** Подробнее о настройке аутентификации Windows читайте в [справочной документации Microsoft](#).

## Настроить файл Web.config приложения-загрузчика

[ *InternalUserPassword* ] — провайдер, указанный в файле Web.config по умолчанию. Если вы хотите предоставить возможность аутентификации по NTLM-протоколу только пользователям, которые не синхронизированы с LDAP, 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.

[ *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* ].

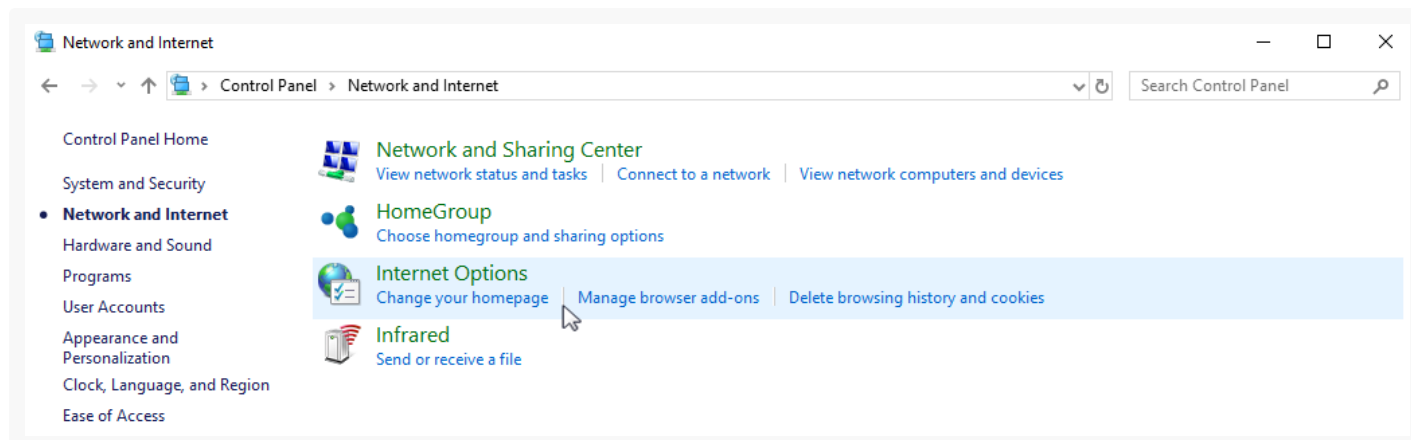
Для отображения страницы входа в систему с доступной ссылкой [ *Войти под доменным пользователем* ] укажите значение “false” для параметра [ *UsePathThroughAuthentication* ]. При этом сквозная аутентификация будет выполняться лишь при переходе на главную страницу приложения. Чтобы отобразить страницу 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:

В меню “Start” → “Settings” → “Control Panel” → “Network and Internet” выберите пункт “Internet options” (Рис. 4).

Рис. 4 — Настройка свойств обозревателя



1. Откройте для редактирования файл Web.config приложения-загрузчика.

2. Укажите в файле провайдеры аутентификации Windows:

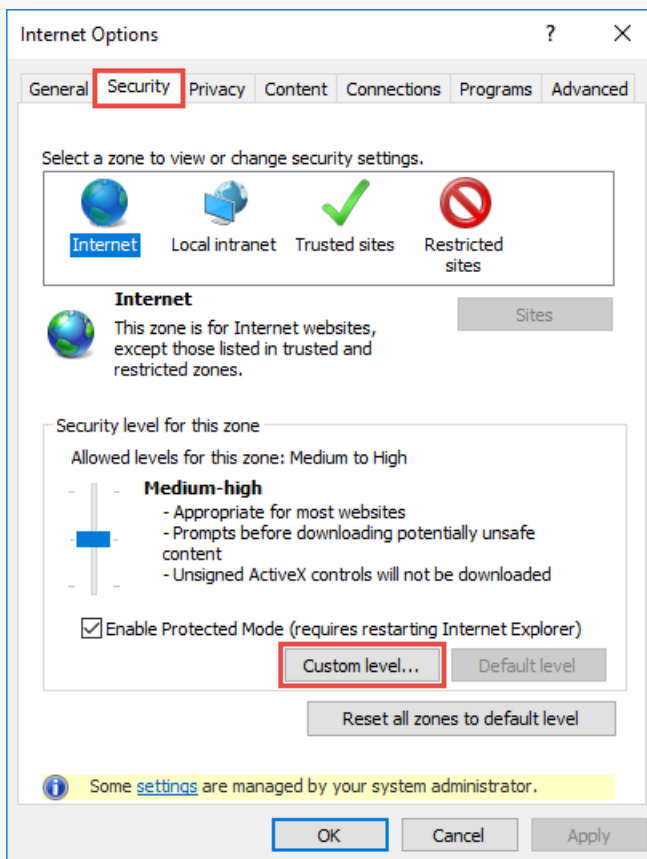
```
auth providerNames="InternalUserPassword,SSPLdapProvider,Ldap"
autoLoginProviderNames="NtlmUser,SSPNtlmUser"
```

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

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

4. В открывшемся окне перейдите на вкладку “Security” и по кнопке “Custom level” перейдите к настройкам безопасности (Рис. 5).

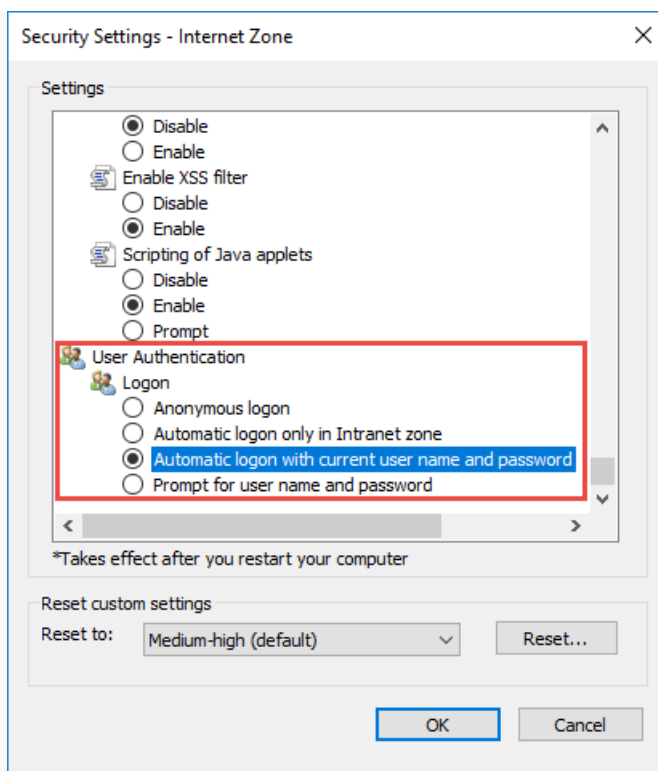
Рис. 5 — Настройки безопасности



5. В группе настроек “User Authentication” выберите способ авторизации “Automatic logon with current user name and password” (Рис. 6).

Рис. 6 — Выбор способа авторизации





6. Нажмите “OK”.

В результате пользователи, которые уже прошли аутентификацию в домене, смогут войти в Creatio по ссылке “Войти как доменный пользователь”, и им не придется повторно вводить учетные данные домена каждый раз для получения доступа к Creatio.