

# Настройка OAuth-аутентификации

Настроить OAuth-аутентификацию для Microsoft 365

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

**Настроить OAuth-аутентификацию для Microsoft 365**

4

# Настроить OAuth-аутентификацию для Microsoft 365

ПРОДУКТЫ: [ВСЕ ПРОДУКТЫ](#)

OAuth — открытый стандарт аутентификации для делегирования ограниченного доступа. OAuth позволяет предоставить третьей стороне ограниченный доступ к защищенным ресурсам пользователя без необходимости использования логина и пароля. Вы можете настроить OAuth-авторизацию для учетных записей почтового сервиса Microsoft 365, предварительно зарегистрировав OAuth-приложение.

Для этого:

1. Зарегистрируйте приложение в учетной записи администратора службы управления корпоративными удостоверениями Azure Active Directory (Azure AD). Подробно о том, как это сделать, читайте в [документации Microsoft](#).

**На заметку.** В поле [ *Redirect URI* ] задайте параметры переадресации, используя следующий шаблон:

`https://<ваш_сайт>.creatio.com/0/rest/Office365OAuthAuthenticator/ProcessAuthenticationCode.`

После завершения регистрации Azure AD присвоит приложению уникальный идентификатор. Он будет отображаться в поле [ *Идентификатор приложения (клиент)* ] на странице обзора приложения в Azure AD. Данный параметр будет запрашивать Creatio как ключ клиента.

2. Добавьте разрешения, чтобы предоставить пользователям доступ для работы с приложением. Подробнее о добавлении разрешений для доступа к веб-API читайте в [документации Microsoft](#).
  - a. Выберите в перечне поддерживаемых APIs “Office 365 Exchange Online”. Укажите тип разрешений “Делегированные разрешения” и установите признак в поле [ *EWS.AccessAsUser.All* ].
  - b. Выберите в перечне поддерживаемых APIs “Microsoft Graph”. Укажите тип разрешений “Делегированные разрешения” и установите признак в поле [ *User.Read* ].
3. Предоставьте согласие на разрешения, настроенные для приложения, по кнопке [ *Предоставить согласие администратора для клиента* ]. Подробнее о кнопке согласия администратора читайте в [документации Microsoft](#).
4. Создайте секрет клиента, который будет использоваться на стороне Creatio. Как это сделать, описано в [документации Microsoft](#).
5. Скопируйте ключ для дальнейшего использования на стороне Creatio.

В результате вы получите необходимые значения параметров “Идентификатор приложения (клиент)” (“Client ID”) и “Секрет клиента” (“Client Secret”) для продолжения настройки на стороне Creatio, а само приложение Creatio будет указано в параметрах переадресации.