Администрирование серверной версии Р7-Офис. Сервер. Профессиональный

Дата создания: 6 мая 2023г.

Дата последнего изменения: 10 мая 2023г.

Р7-ОФИС

Оглавление

Администрирование серверной версии Р7-Офис. Сервер. Профессиональный

Р7-Офис. Сервер. Профессиональный — это система для совместной работы, централизованного управления документами и электронной перепиской.

Панель управления Р7-Офис

Настройка Р7-Офис SP и AD FS IdP

Введение

Технология единого входа (англ. Single Sign-On или SSO) — технология, которая позволяет пользователям осуществлять вход в систему только один раз, а затем получать доступ ко множеству приложений/сервисов без повторной аутентификации.

Примечание: если на веб-портале существует несколько обширных независимых разделов (форум, чат, блог и т. д.) то, пройдя процедуру аутентификации в одном из сервисов, пользователь автоматически получает доступ ко всем остальным, что избавляет его от многократного ввода данных своей учётной записи.

SSO — это всегда совместная работа двух приложений: поставщика учетных записей (англ. Identity Provider, далее по тексту сокращенно «IdP») и поставщика сервиса (англ. Service Provider, далее по тексту сокращенно «SP»). **Р7-Офис SSO** реализует **только SP**. В качестве IdP может выступать множество различных провайдеров, но в этой статье мы рассмотрим реализацию Active Directory Federation Services (AD FS).

Системные требования

Системные требования включают в себя следующее программное обеспечение, которое было протестировано и корректно работает с **Р7-Офис SSO**:

- Windows Server 2008 R2, Windows Server 2016;

- AD FS версии **3.0** или более поздней версии.

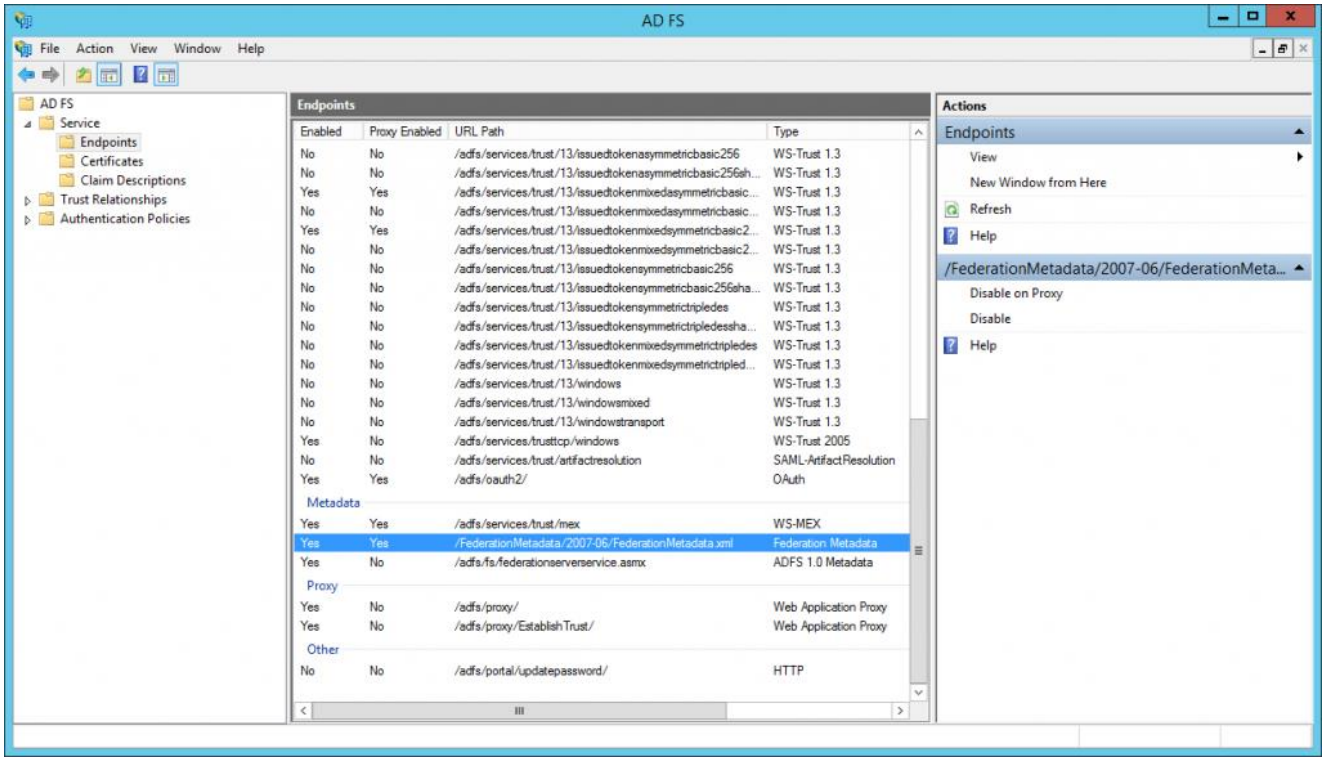
Подготовка Р7-Офис для настройки SSO

1. Установите версию Р7-Офис. Сервер. Профессиональный с поддержкой SSO.
2. Привяжите доменное имя, например, myportal-address.com.
3. На портале перейдите в **Панель управления** -> **HTTPS**, создайте и примените сертификат letsencrypt для шифрования трафика (для включения HTTPS на портале).

Подготовка AD FS для настройки SSO

1. Установите последнюю версию AD DS (Active Directory Domain Service) со всеми официальными обновлениями и исправлениями.
2. Установите последнюю версию AD FS со всеми официальными обновлениями и исправлениями.
3. Проверьте, что ссылка на файл метаданных AD FS доступна публично. Для этого:
   A. В консоли **Диспетчер сервера** откройте **Tools** (Инструменты) -> **AD FS Management** (Управление AD FS),
   B. Перейдите в **AD FS \ Service \ Endpoints** (AD FS \ Служба \ Конечные точки),
   C. Найдите в таблице строку с типом **Federation Metadata** (Метаданные федерации). Ссылка на файл метаданных IdP формируется по следующей схеме:

```
https://{ad-fs-domain}/{path-to-FederationMetadata.xml}
```



Можно также воспользоваться следующей командой **PowerShell**:

```
PS C:\Users\Administrator> (Get-ADFSEndpoint | Where {$_.Protocol -eq "FederationMetadata" -or $_.Protocol -eq "Federation Metadata"}).FullUrl.ToString()
```

В результате вы должны получить ссылку следующего вида:

```
https://r7-officevm.northeurope.cloudapp.azure.com/FederationMetadata/2007-06/FederationMetadata.xml
```

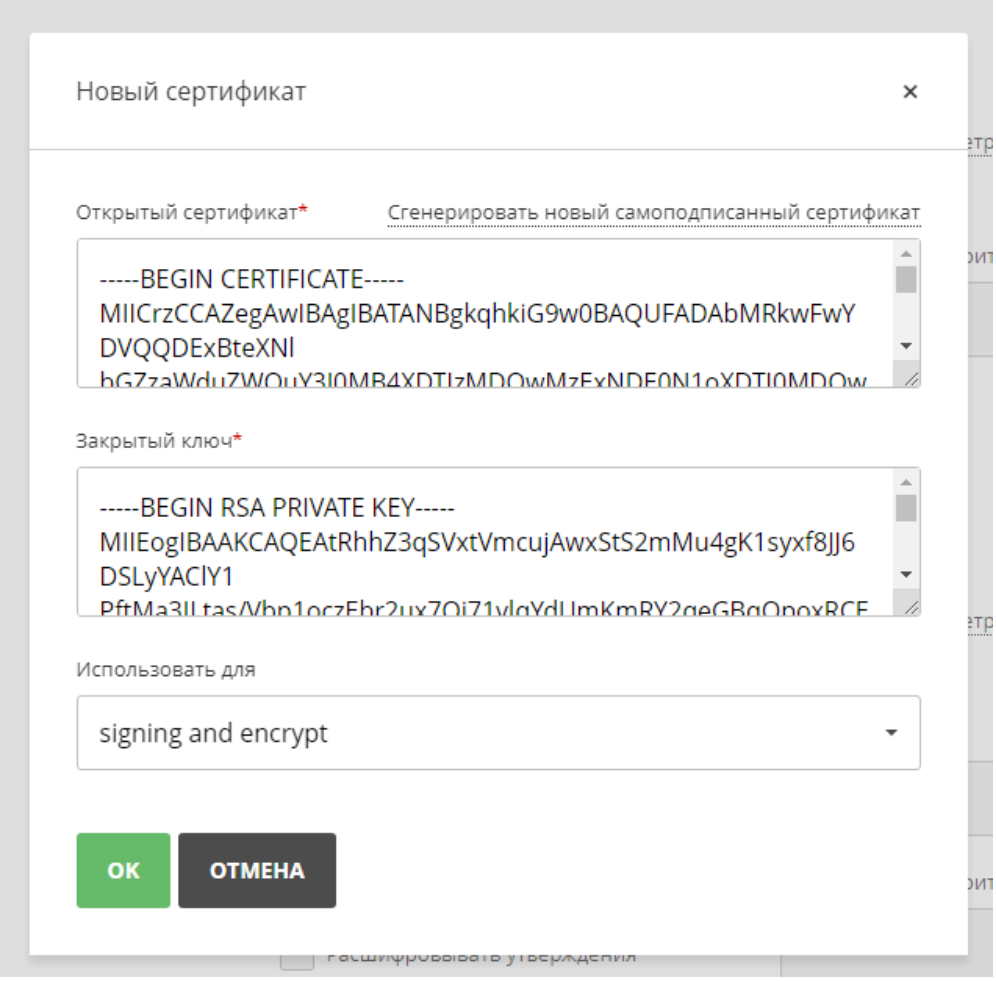
D. Для проверки, что AD FS стартовал корректно, перейдите в браузере по ссылке,
полученной ранее. Должна скачаться/отобразится xml. Скопируйте ссылку на xml-файл метаданных: она потребуется на следующем шаге.

Настройка Р7-Офис SP

1. Убедитесь, что вы зашли в качестве администратора в **Панель управления** Р7-Офис, и щелкните вкладку **SSO**.
   Примечание: Вы можете зарегистрировать только одного корпоративного поставщика учетных записей для вашей организации на портале Р7-Офис.
2. Включите SSO, используя переключатель. **Включить аутентификацию с помощью технологии единого входа**. Ссылку, скопированную из AD FS,

вставьте в поле **URL-адрес XML-файла метаданных IdP**.Нажмите кнопку со стрелкой вверх, чтобы загрузить метаданные IdP. Форма **Настройки поставщика сервиса Р7-Офис** будет автоматически заполнена данными из AD FS IdP.

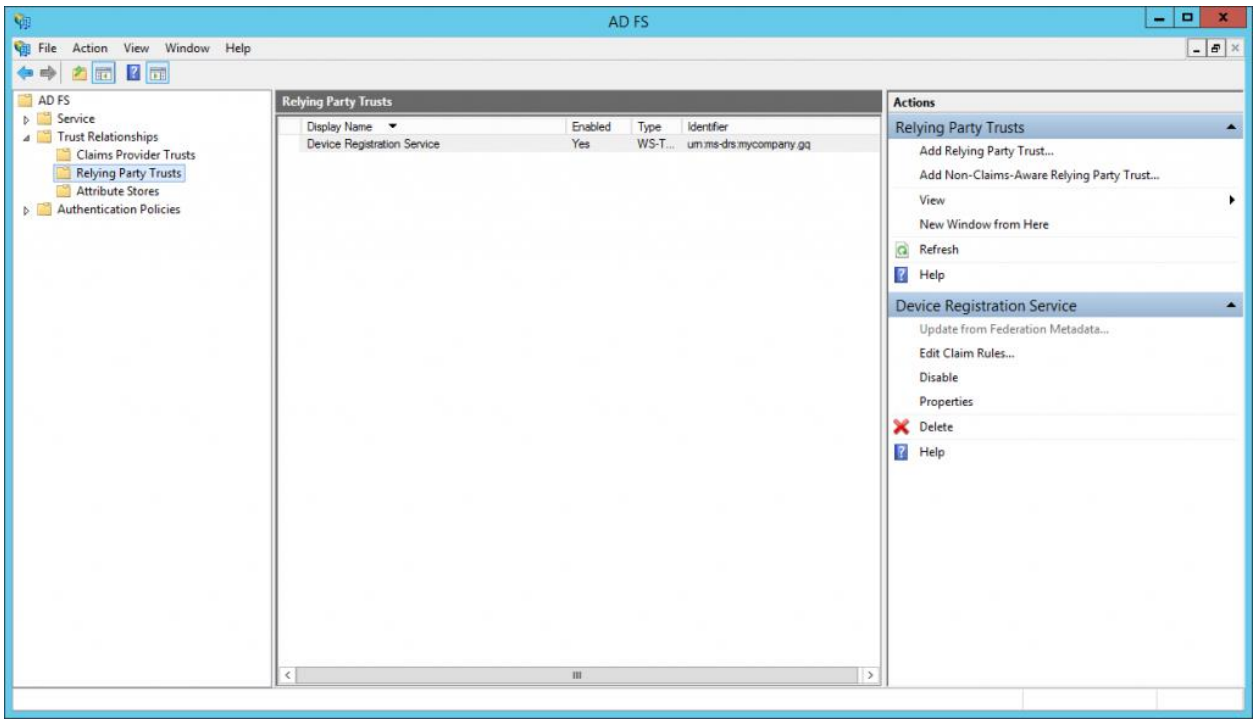
3. В поле **Пользовательская надпись для кнопки входа** вы можете ввести любой текст вместо стандартного «*Single Sign-on*«. Этот текст будет отображаться на кнопке для входа с помощью сервиса Single Sign-on на странице аутентификации портала Р7-Офис.
4. В селекторе **Формат NameID** выберите следующее значение: **urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress**.
5. В разделе **Открытые сертификаты поставщика учетных записей \ Дополнительные параметры** уберите галочку **Проверять подпись ответов выхода**, так как AD FS не требует этого по умолчанию.
6. Теперь необходимо добавить сертификаты в раздел **Сертификаты поставщика сервиса**. Можно сгенерировать самоподписанные сертификаты или добавить любые другие.
   Примечание: в окне **Новый сертификат** переключите селектор **Использовать для** на **signing and encrypt**, так как AD FS IdP автоматически настроен на проверку цифровой подписи и шифрование данных.
   Должно получиться примерно так:



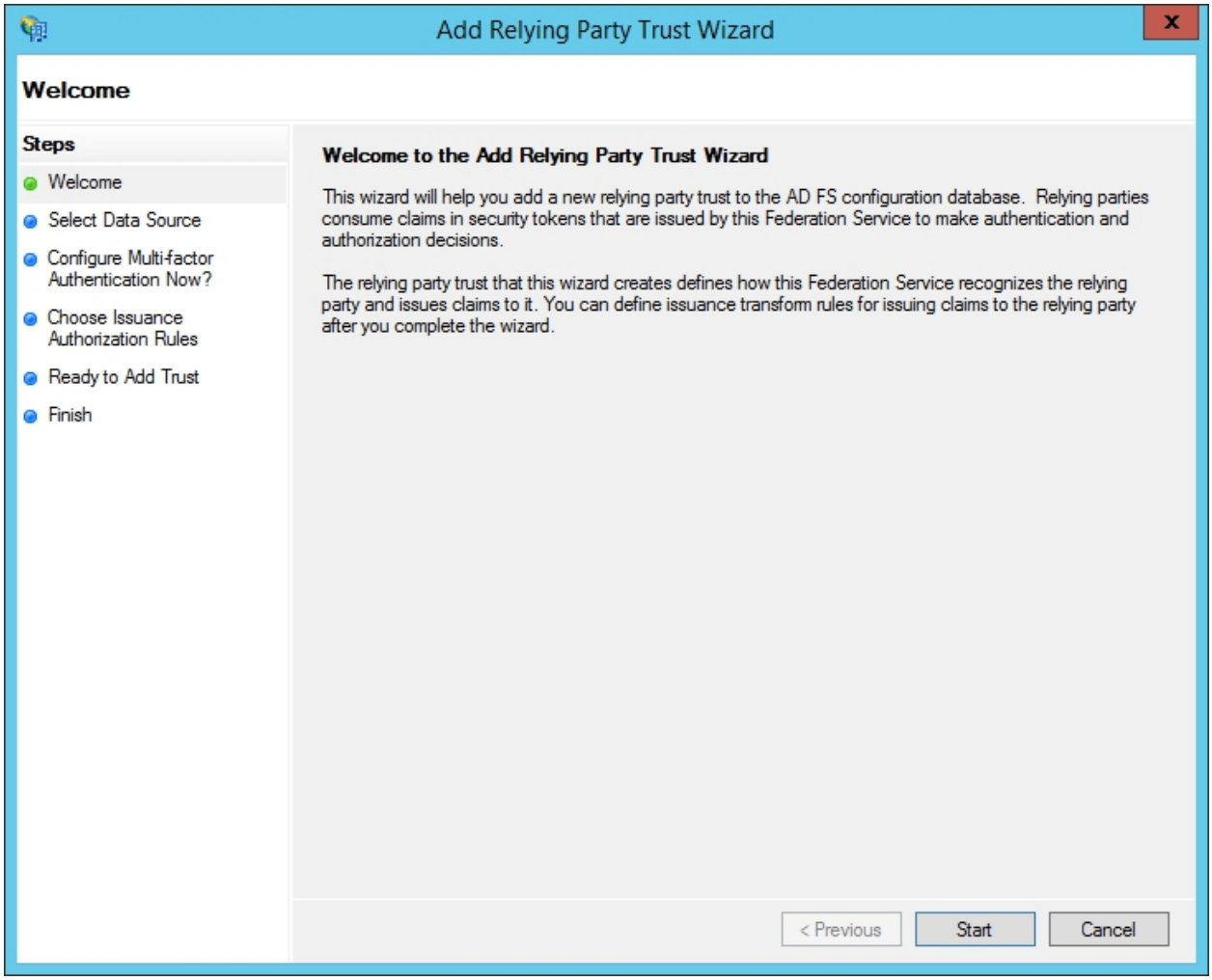
7. В разделе **Сертификаты поставщика сервиса \ Дополнительные параметры**, уберите галочку **Подписывать ответы выхода**, так как AD FS не требует этого по умолчанию.
   Примечание: Форму с заголовком **Сопоставление атрибутов** настраивать не нужно, так как эти параметры мы настоим в AD FS IdP позже.
8. Нажмите кнопку **Сохранить**. Должен открыться раздел **Метаданные поставщика сервиса Р7-Офис**. Проверьте, что настройки доступны публично, кликнув по кнопке **СКАЧАТЬ XML-ФАЙЛ МЕТАДАННЫХ ПОСТАВЩИКА СЕРВИСА**. Должно отобразиться содержимое XML-файла.
9. Скопируйте ссылку на файл метаданных Р7-Офис SP из поля **Идентификатор сущности поставщика сервиса (ссылка на XML-файл метаданных)** и перейдите на машину, где установлен AD FS.

Настройка AD FS IdP

1. В консоли **Диспетчер сервера** откройте **Tools** (Инструменты) -> **AD FS Management** (Управление AD FS),



2. В панели управления **AD FS** выберите **Trust Relationships > Relying Party Trusts** (Отношения доверия -> Отношения доверия проверяющей стороны). Выберите команду **Add Relying Party Trust...** (Добавить отношение доверия проверяющей стороны...) справа. Откроется **Мастер добавления отношений доверия проверяющей стороны**,



Для того чтобы добавить AD FS в IdP в Microsoft Active Directory Federation Service на сервере Microsoft Windows Server 2012 R2 или ниже необходимо включить поддержку протокола TLS 1.2

Для этого воспользуйтесь инструкцией:

Пререквизиты:

- Версия .NET Framework, установленная на сервере ADFS, должна быть выше 4.6.2:
  - Проверка версии .NET Framework
  - Загрузки .NET Framework
- Версия Windows Server 2012 Hardware Abstraction Layer (HAL) должна быть не ниже 6.3.9600.17031.

Инструкция

A. Запустите Windows PowerShell с параметром «Запуск от имени администратора».

B. Выполните следующие команды, чтобы включить TLS2 на клиенте ADFS:

```
New-Item
'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS
1.2\Client' -Force

New-ItemProperty -Path
'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS
1.2\Client' -name 'Enabled' -value '1' –PropertyType 'DWORD'

New-ItemProperty -Path
'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS
1.2\Client' -name 'DisabledByDefault' -value '0' –PropertyType 'DWORD'
```

Информационное сообщение Write-Host «TLS 1.2 включен».

C. Затем выполните следующую команду, чтобы включить строгую аутентификацию:

```
New-ItemProperty -path 'HKLM:\SOFTWARE\Microsoft\.NetFramework\v4.0.30319' -name
'SchUseStrongCrypto' -value '1' -PropertyType 'DWord'
```

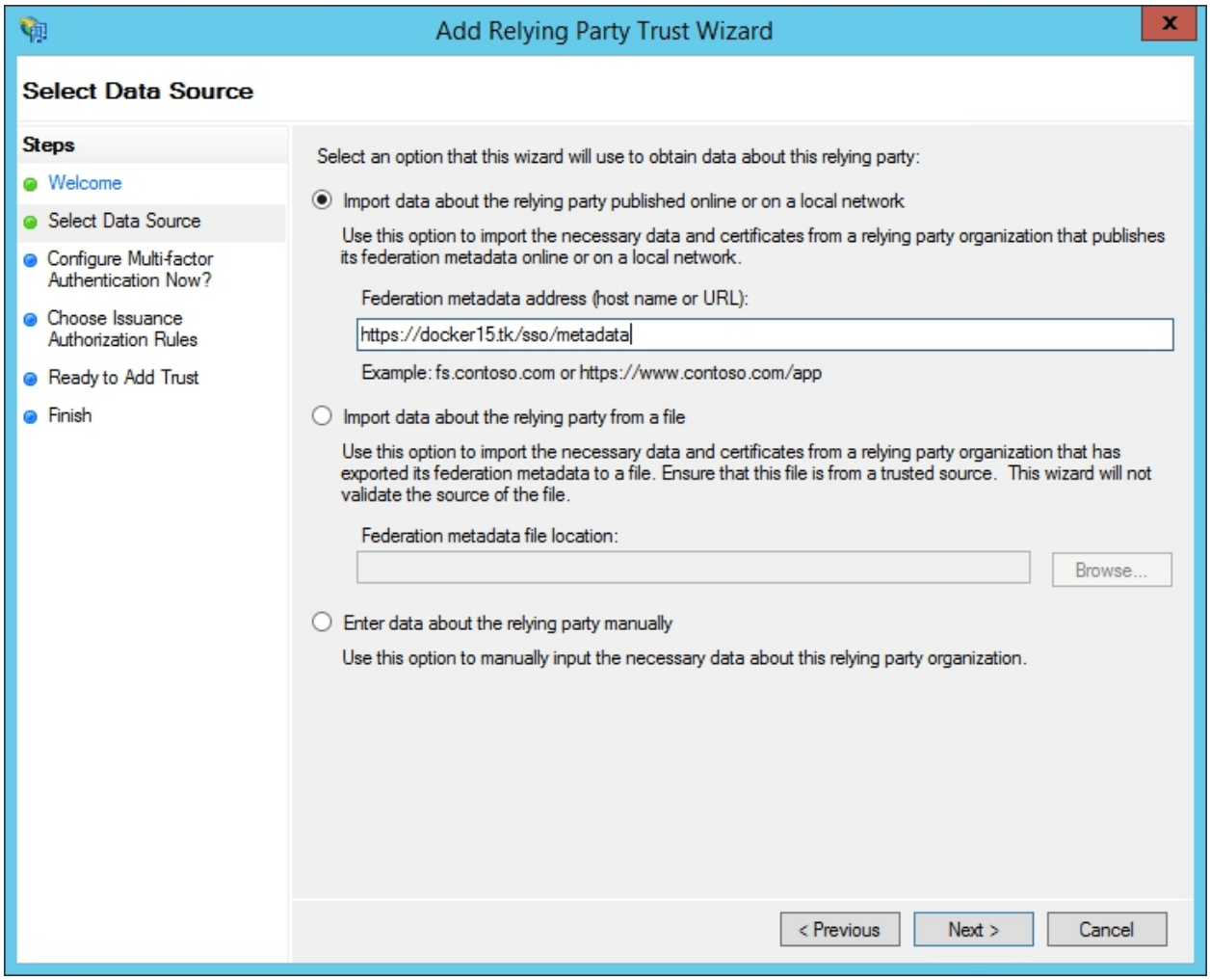
D. (Необязательно) Выполните следующие команды, чтобы отключить SSL0 на клиенте ADFS:

```
New-Item
'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL
3.0\Client' -Force | Out-Null

New-ItemProperty -path
'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\ Protocols\SSL
3.0\Client' -name 'Enabled' -value '0' -PropertyType 'DWord' -Force | Out-Null

New-ItemProperty -path
'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\ Protocols\SSL
3.0\Client' -name 'DisabledByDefault' -value 1 -PropertyType 'DWord' -Force | Out-Null
```

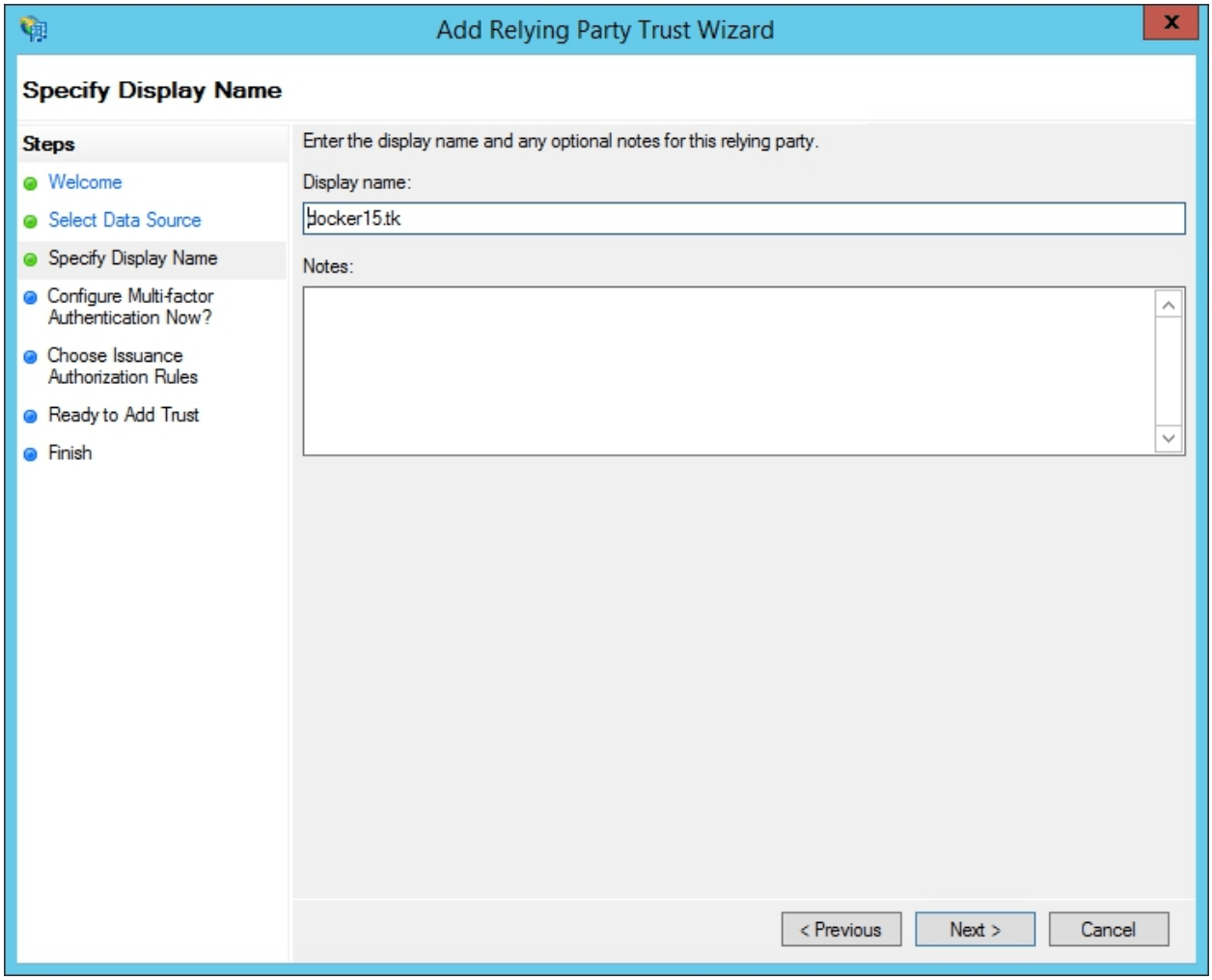
Информационное сообщение Write-Host «SSL 3.0 отключен».

1. Закройте все окна управления сервером ADFS.

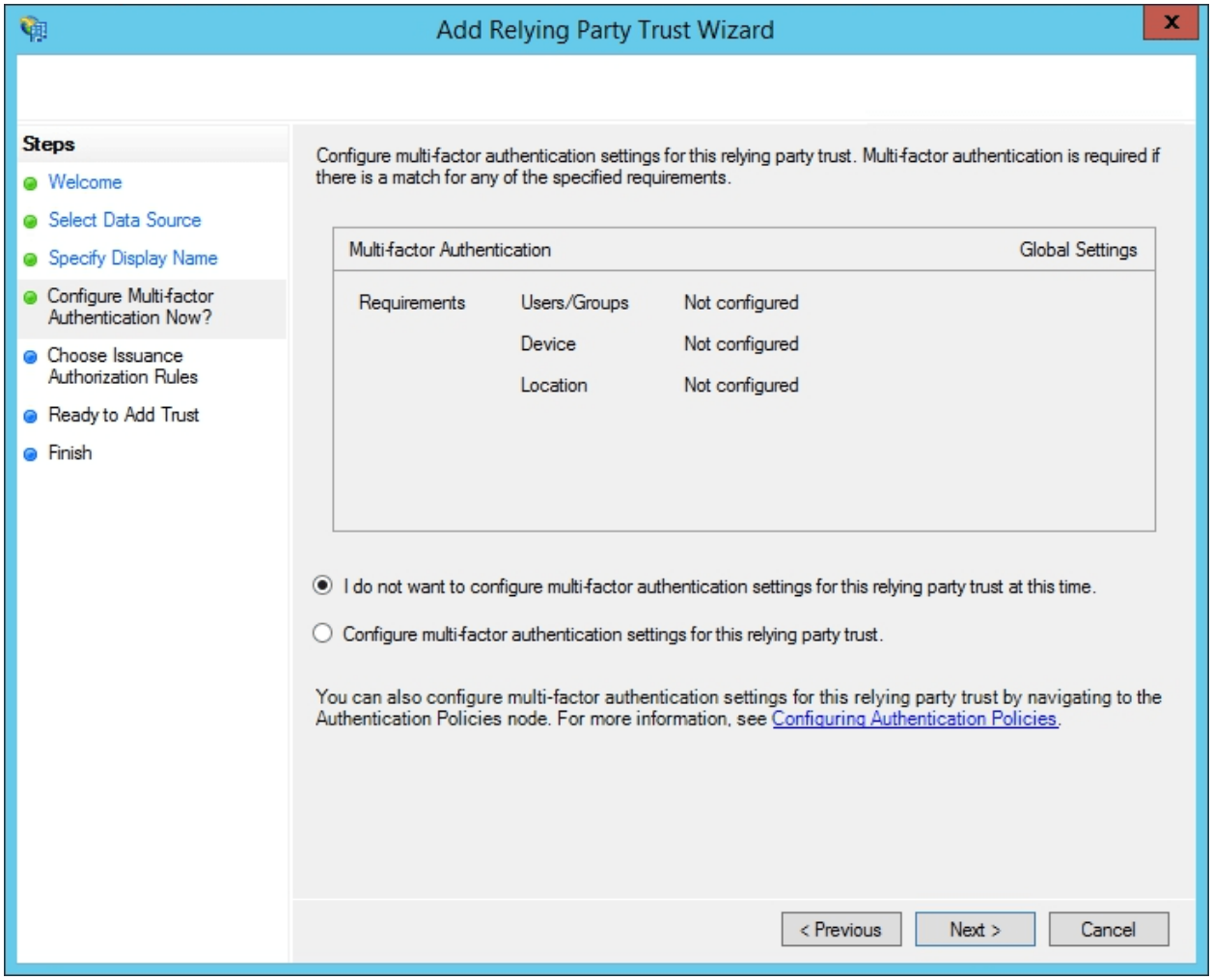
3. В окне мастера выберите переключатель **Import data about the relying party published online or on a local network** (Импорт данных о проверяющей стороне, опубликованных в Интернете или локальной сети), вставьте скопированную ранее ссылку на файл метаданных Р7-Офис SP в поле **Federation metadata address (host name or URL)** (Адрес метаданных федерации (имя узла или URL-адрес)) и нажмите кнопку **Next** (Далее)



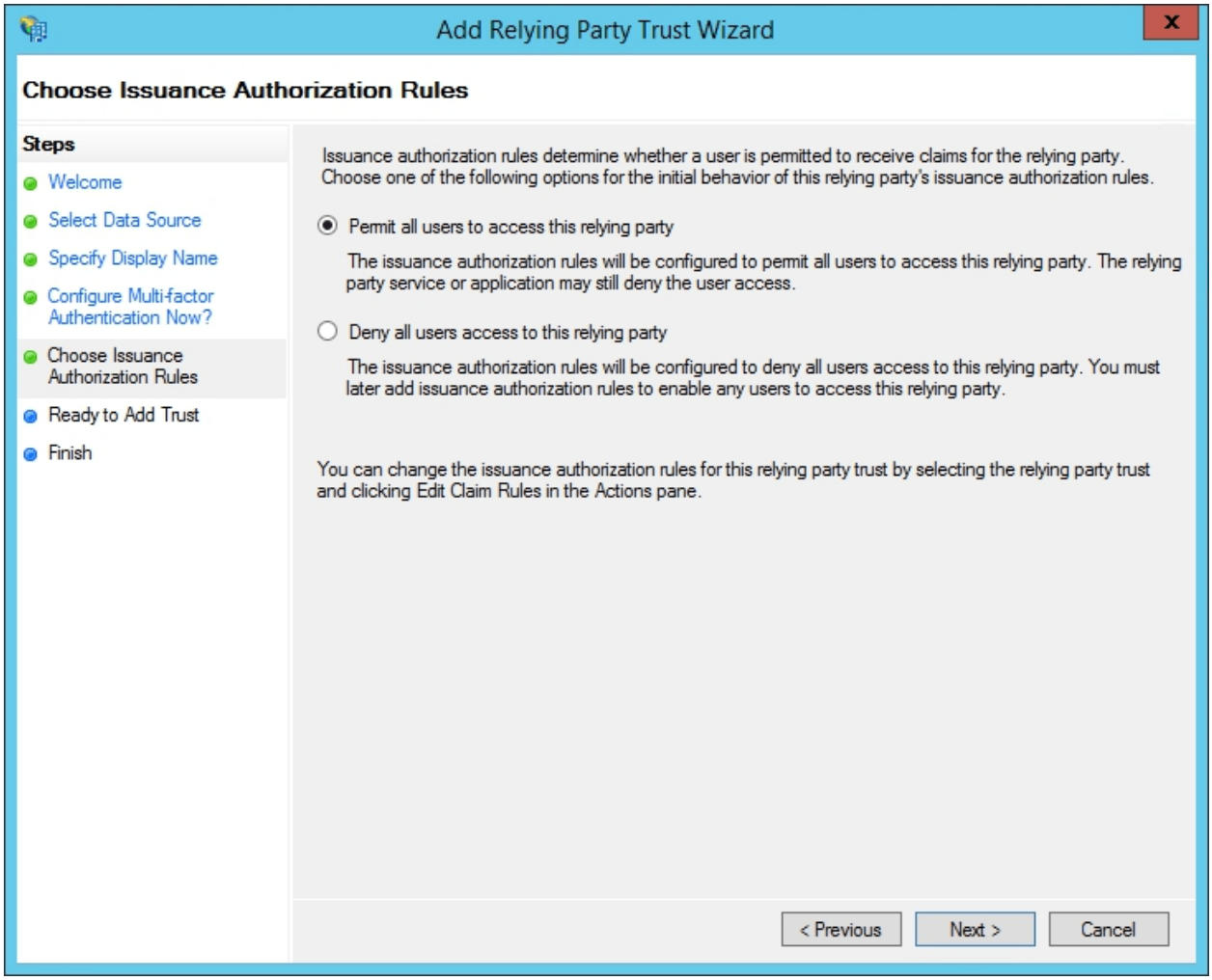
4. В поле **Display name** (Отображаемое имя) укажите любое имя и нажмите кнопку **Next** (Далее)



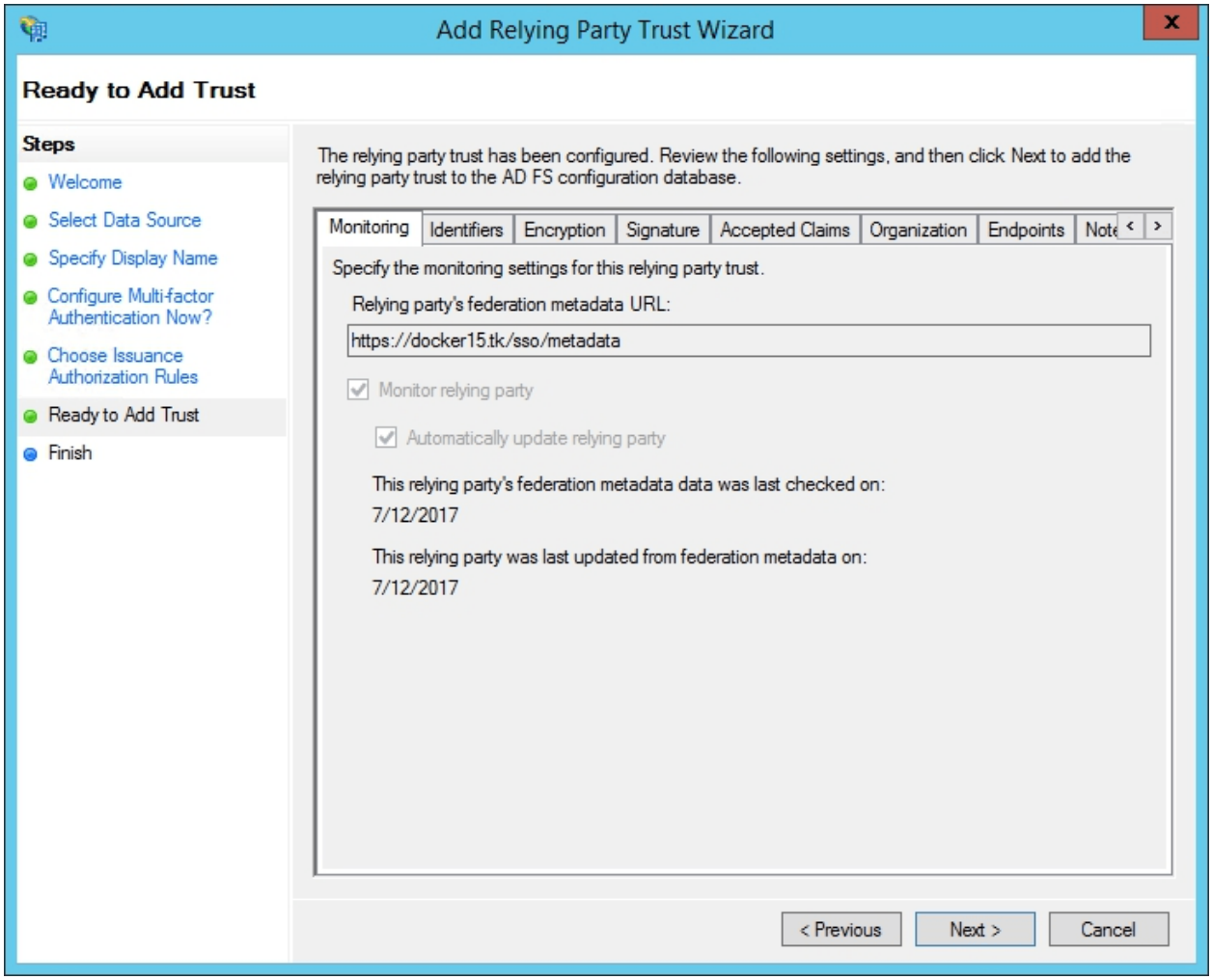
5. Выберите опцию **I do not want to configure multi-factor authentication settings for this relying party trust at this time** (Сейчас не настраивать параметры для этого отношения доверия с проверяющей стороной) и нажмите кнопку **Next** (Далее)



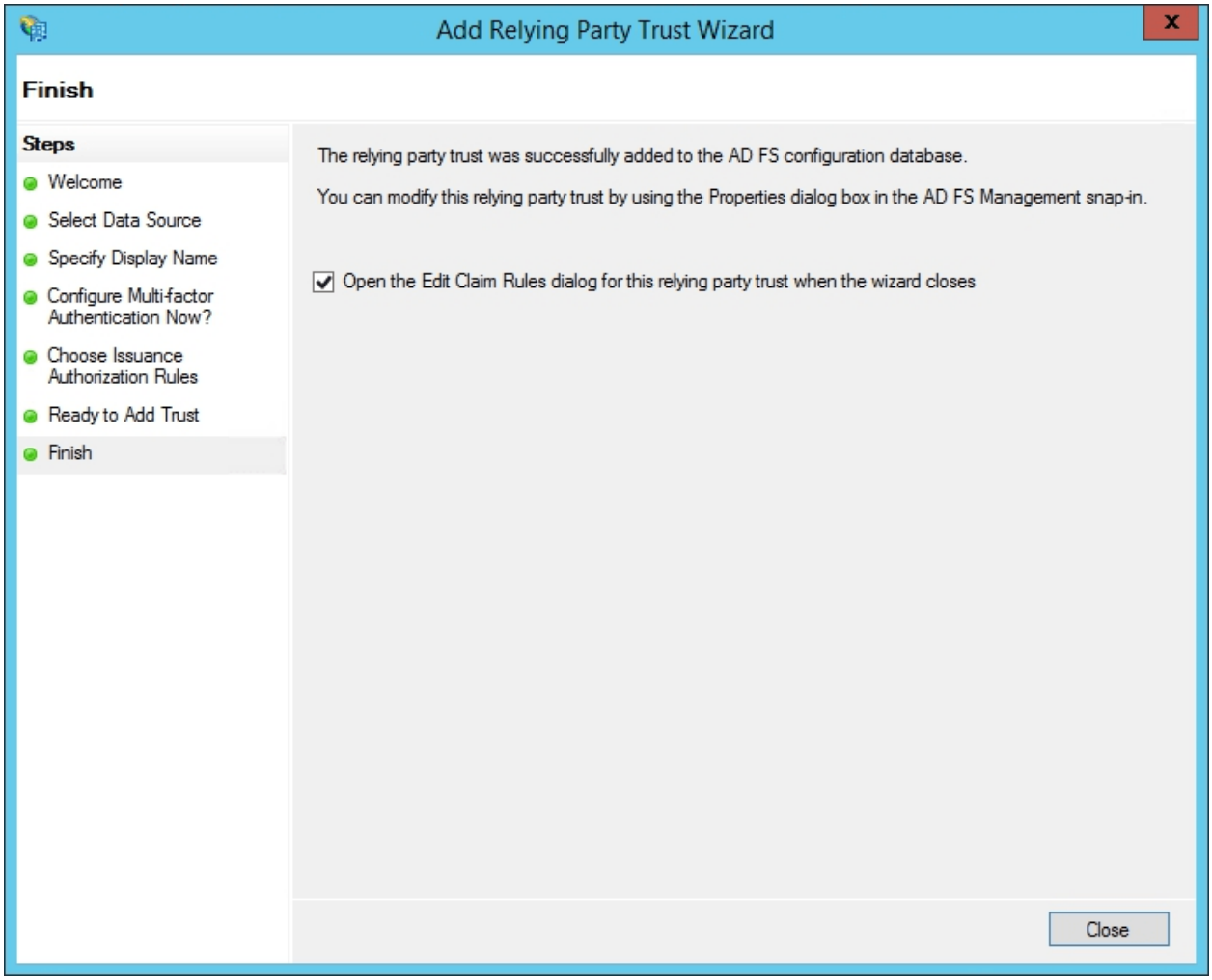
6. Выберите опцию **Permit all users to access this relying party** (Разрешить доступ к этой проверяющей стороне всем пользователям) и нажмите кнопку **Next** (Далее)



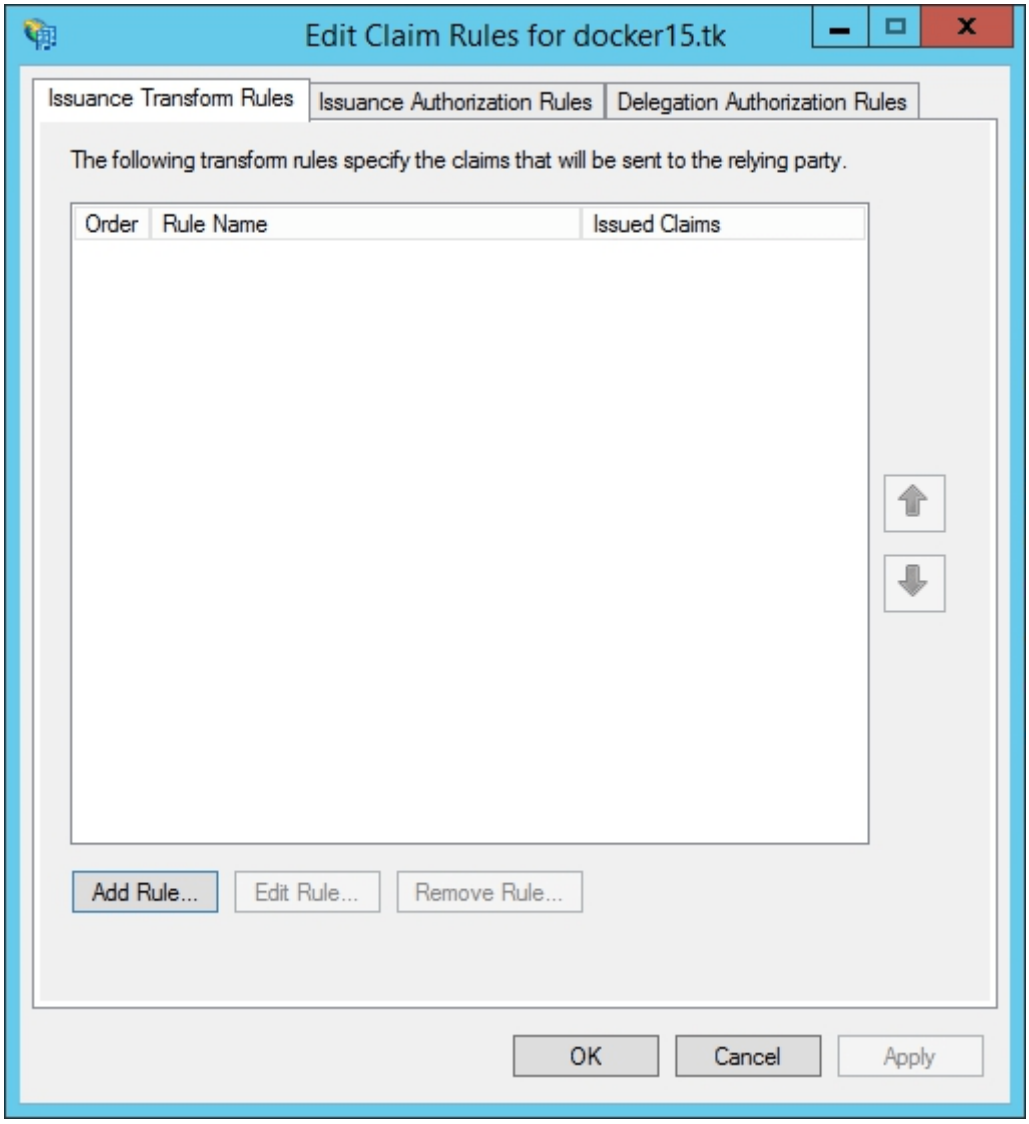
7. Проверьте полученные настройки и нажмите кнопку **Next** (Далее)



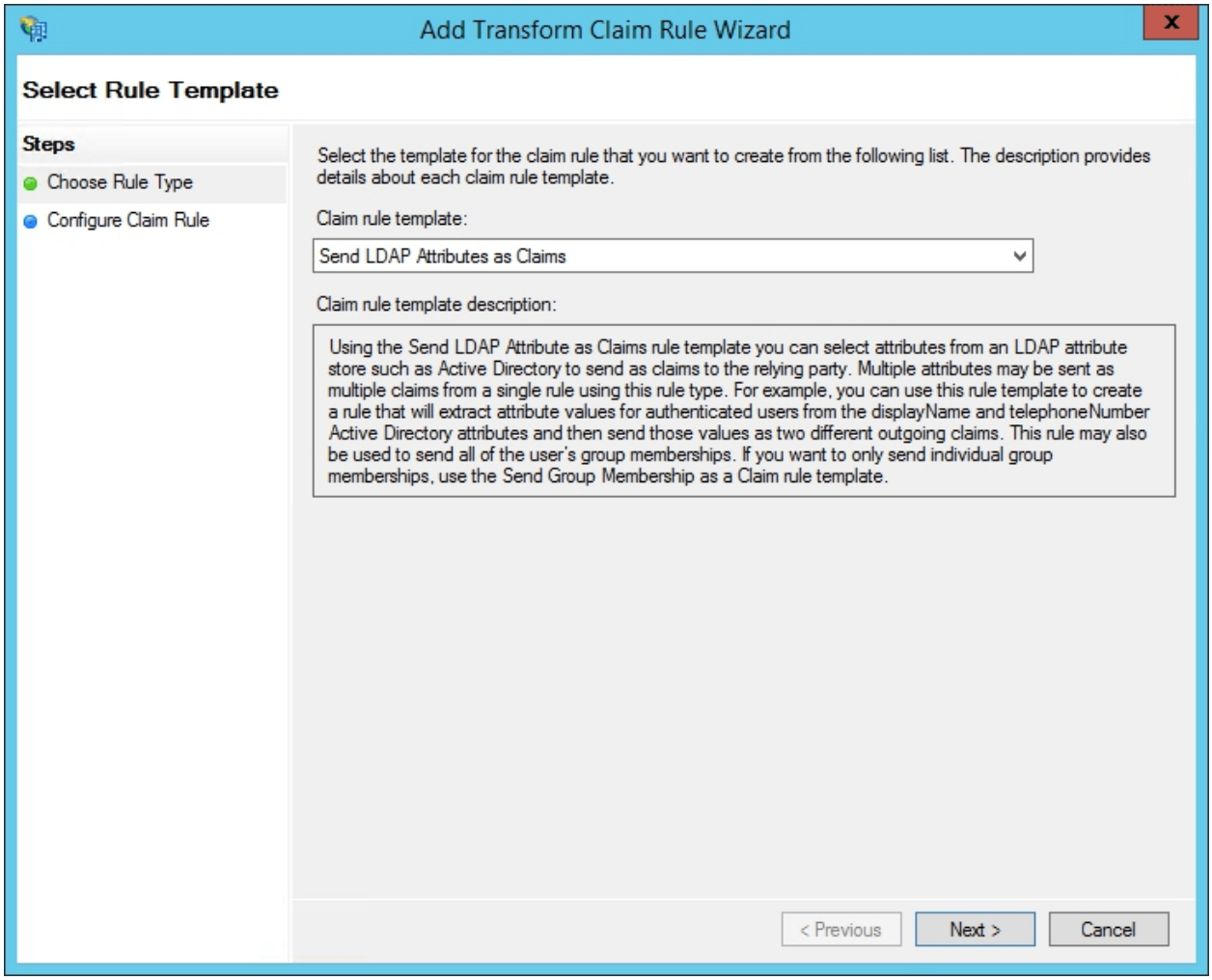
8. Оставьте опцию, выбранную по умолчанию, без изменений и нажмите кнопку **Close** (Закрыть)



9. Откроется новое окно. На вкладке **Issuance Transform Rules** (Правила преобразования выдачи) нажмите кнопку **Add Rule...** (Добавить правило...)

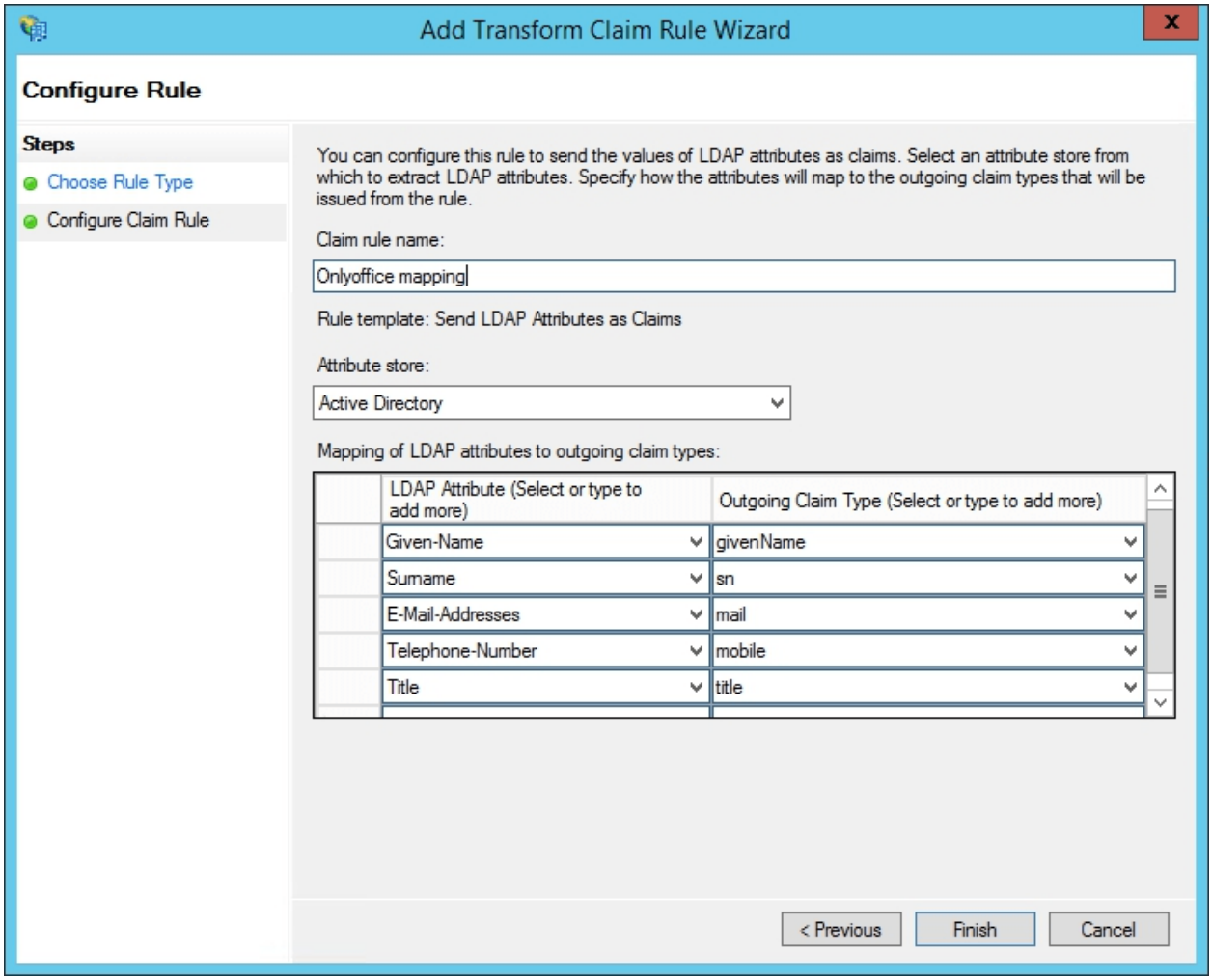


10. Выберите опцию **Send LDAP Attributes as Claims** (Отправка атрибутов LDAP как утверждений) из списка **Claim rule template** (Шаблон правила утверждения) и нажмите кнопку **Next** (Далее)

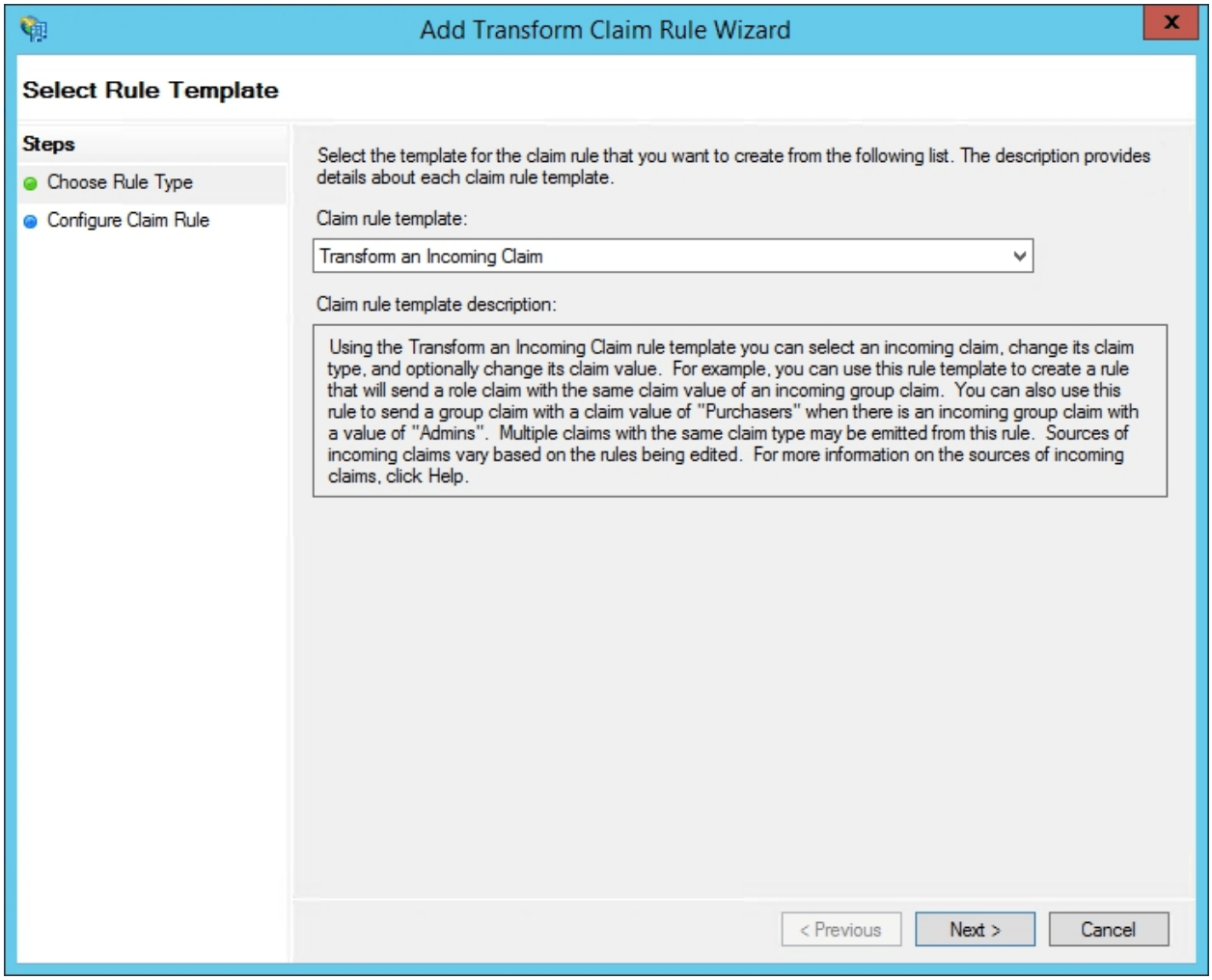


11. Напишите любое имя в поле **Claim rule name** (Имя правила утверждения). Выберите опцию **Active Directory** из списка **Attribute store** (Хранилище атрибутов) и заполните форму **Mapping of LDAP attributes to outgoing claim types** (Сопоставление атрибутов LDAP типам исходящих утверждений) согласно приведенной ниже таблице. Когда все будет готово, нажмите кнопку **Finish** (Завершить).

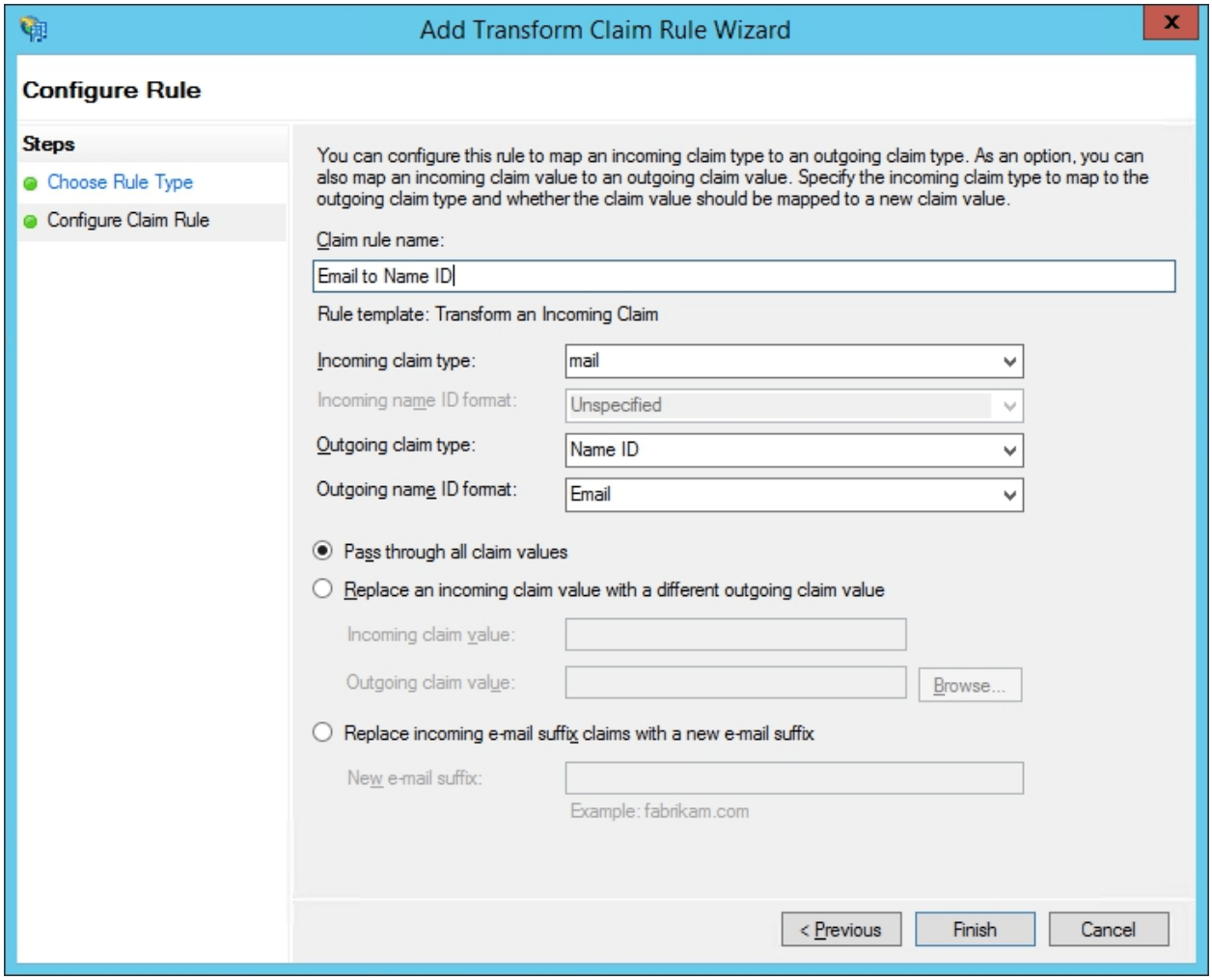
LDAP ATTRIBUTE (АТРИБУТ LDAP)	OUTGOING CLAIM TYPE (ТИП ИСХОДЯЩЕГО УТВЕРЖДЕНИЯ)
Given-Name	givenName
Surname	sn
E-Mail-Addresses	mail
Telephone-Number	mobile
Title	title
physicalDeliveryOfficeName	l



12. В окне **Edit Claim Rules** (Изменить правила утверждений) снова нажимите кнопку **Add Rule...** (Добавить правило...), выберите опцию **Transform an Incoming Claim** (Преобразование входящего утверждения) из списка **Claim rule template** (Шаблон правила утверждения) и нажмите кнопку **Next** (Далее)

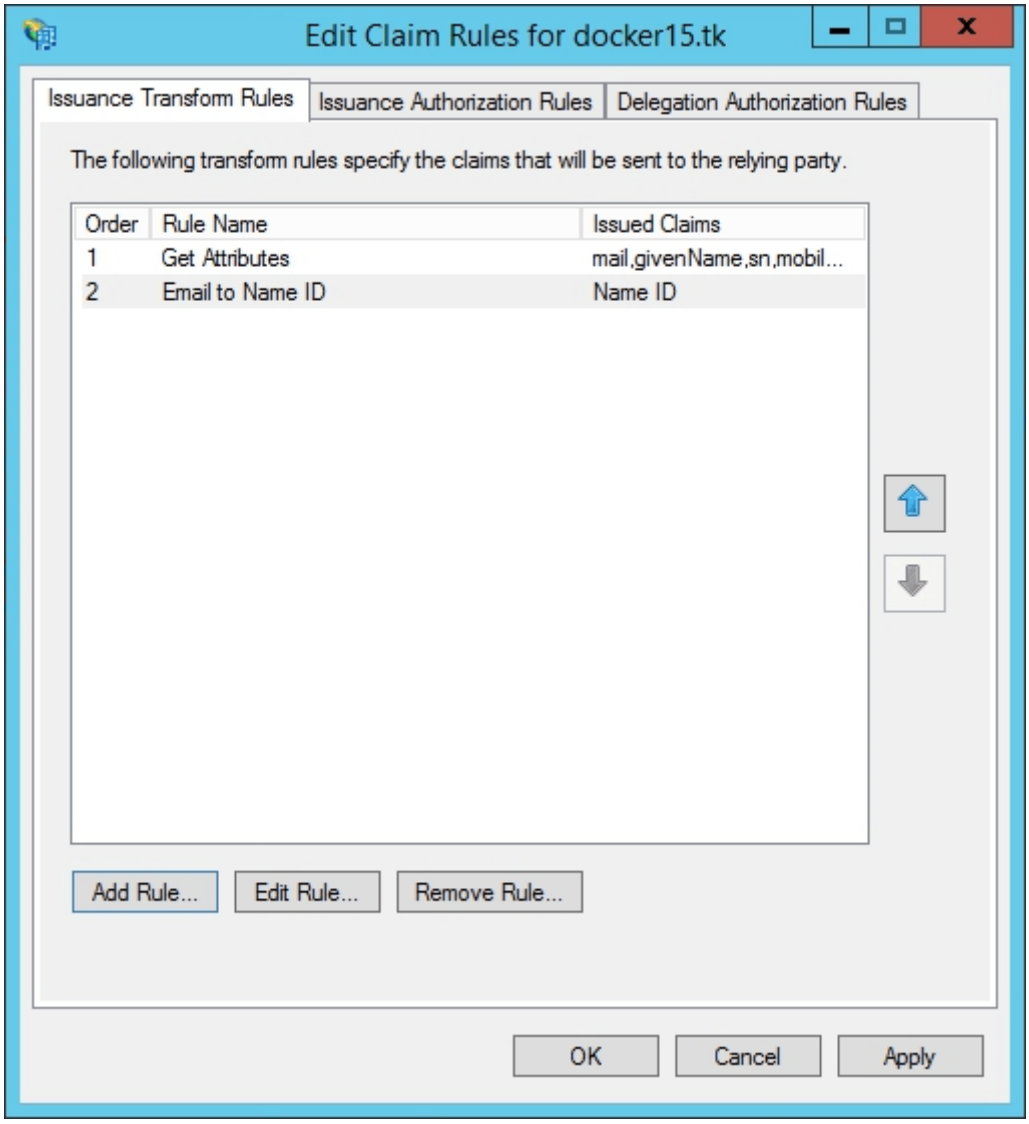


13. Напишите любое имя в поле **Claim rule name** (Имя правила утверждения) и выберите следующие параметры из списков:
    - **Incoming claim type** (Тип входящего утверждения): mail,
    - **Outgoing claim type** (Тип исходящего утверждения): Name ID,
    - **Outgoing name ID format** (Формат ИД исходящего имени): Email



Когда все будет готово, нажмите кнопку **Finish** (Завершить).

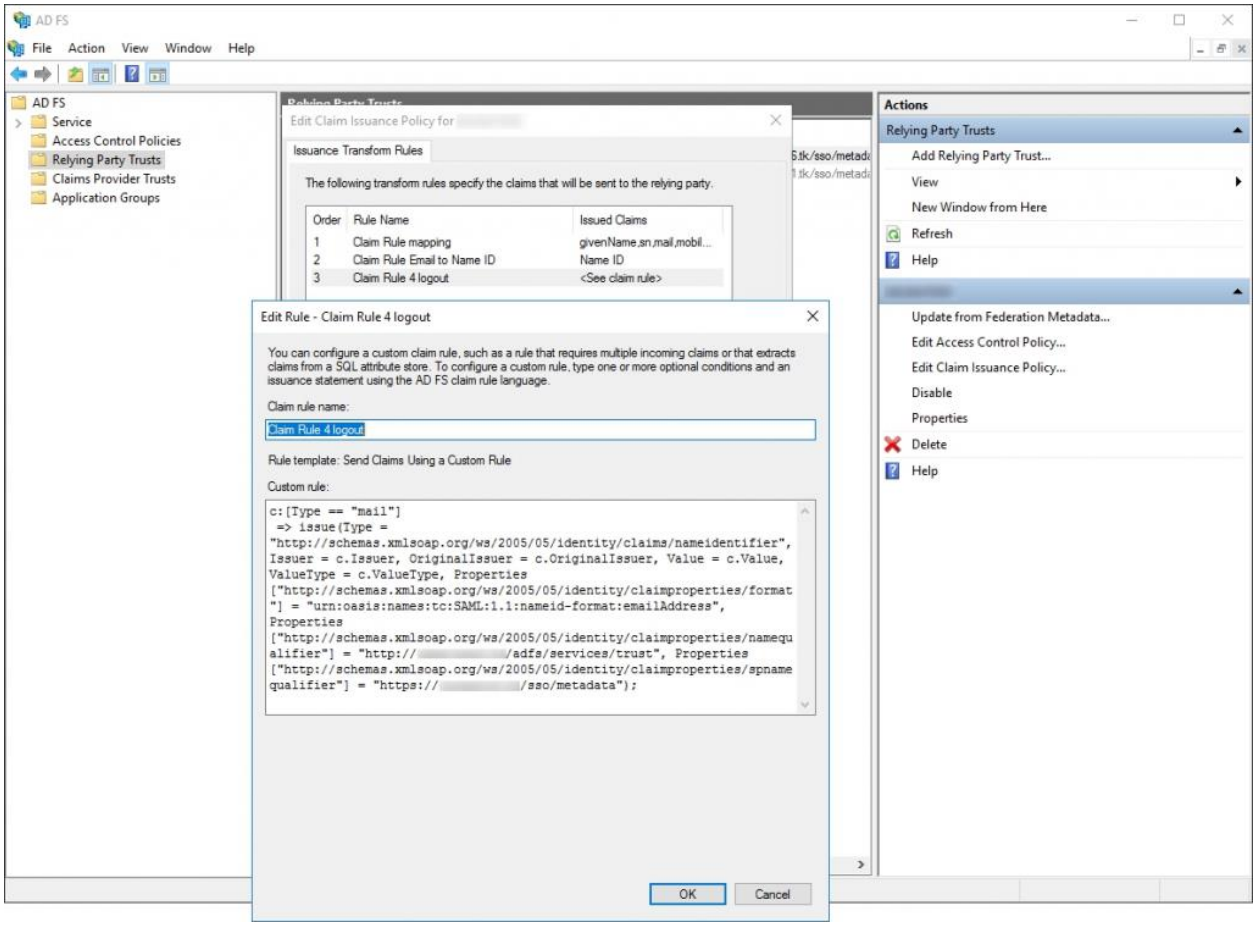
Должно получиться примерно так:



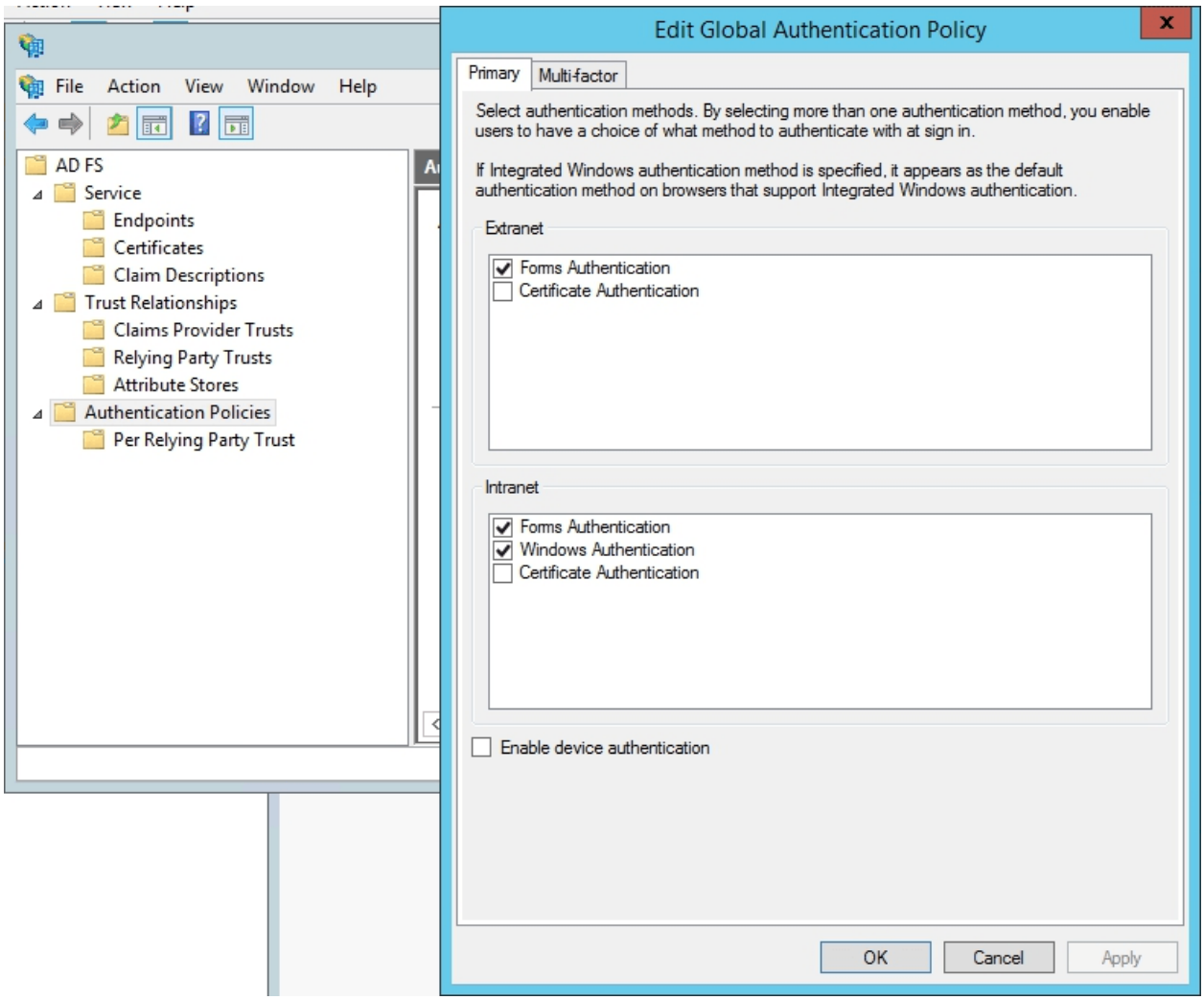
Если не будет работать logout из AD FS, то стоит добавить Custom Claim Rule (настраиваемое правило утверждения), где {portal-domain} нужно заменить на домен своего SP, а {ad-fs-domain} заменить на домен IdP:

```
c:[Type == "mail"]

 => issue(Type =
"http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier", Issuer =
c.Issuer, OriginalIssuer = c.OriginalIssuer, Value = c.Value, ValueType = c.ValueType,
Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/format"] =
"urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress",
Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/namequalif
ier"] = "http://{ad-fs-domain}/adfs/services/trust",
```

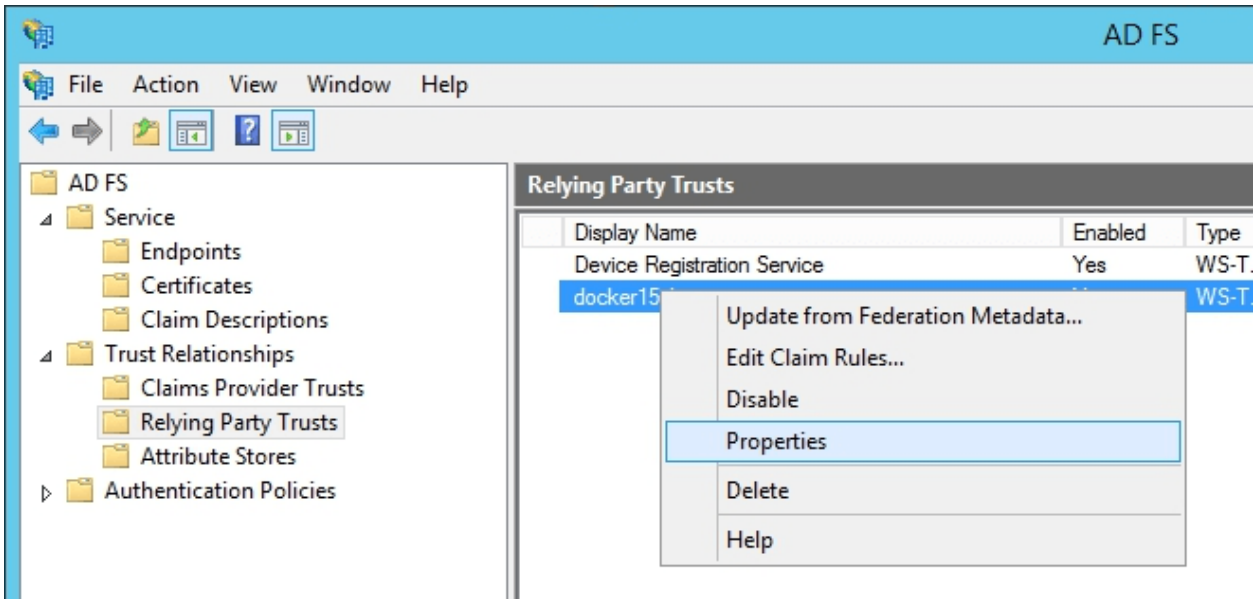
Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/spnamequalifier"] = "https://{portal-domain}/sso/metadata");



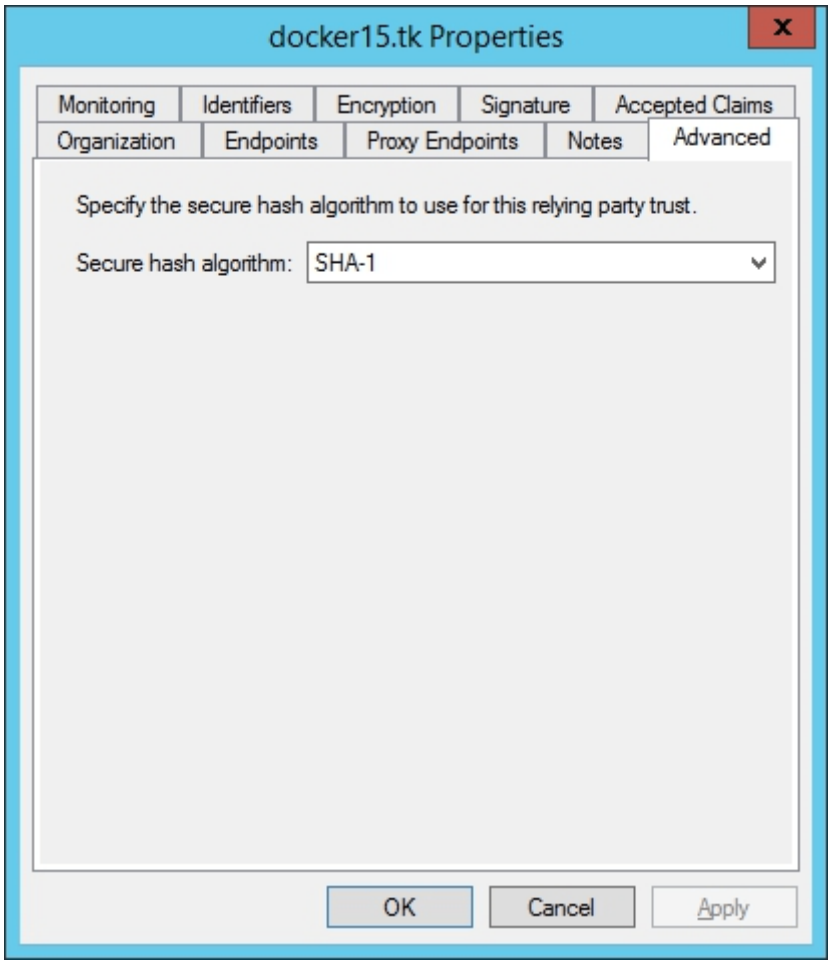
14. Нажмите кнопку **OK**,
15. Для работы SSO из интранета потребуется включить опцию **Forms Authentication** (Проверка подлинности с помощью форм) в окне **Edit Global Authentication** Policy (Изменить глобальную политику проверки подлинности), вызываемом через контекстное меню **AD FS / Authentication Policies** (AD FS / Политики проверки подлинности)



16. Откройте свойства созданной проверяющей стороны и перейдите на вкладку **Advanced** (Дополнительные параметры)



Выберите опцию **SHA-1** в списке **Secure hash algorithm** (Алгоритм SHA).



Проверка работы Р7-Офис SP и AD FS IdP

Вход в Р7-Офис на стороне SP

1. Перейдите на страницу аутентификации Р7-Офис (например, https://myportal-address.com/auth.aspx).
2. Нажмите на кнопку **Single sign-on** (название кнопки может отличаться, если вы указали свой вариант при настройке Р7-Офис SP). Если этой кнопки нет, то SSO не включен.
3. Если всё настроено верно в SP и IdP, мы будем перенаправлены на форму логина в AD FS IdP.
4. Введите логин и пароль учетной записи в AD FS IdP и нажмите кнопку **Sign in**.
5. Если учетные данные указаны правильно, мы будем перенаправлены на главную страницу портала (если такого пользователя нет на портале, он будет создан автоматически, а если данные были изменены в IdP, они будут обновлены).

Профили пользователей, добавленных с помощью SSO-аутентификации

Возможность редактирования профилей пользователей, созданных с помощью SSO-аутентификации, ограничена. Поля профиля пользователя, полученные из IdP, заблокированы для редактирования (а именно: Имя, Фамилия, Email, Позиция и Местоположение). Эти поля можно отредактировать только из вашей учетной записи в IdP.

Пользователи, созданные с помощью SSO-аутентификации, отмечены в списке пользователей значком SSO для администраторов портала.

Настройка Р7-Офис SP и OneLogin IdP

Введение

Технология единого входа (англ. Single Sign-On или SSO) — технология, которая позволяет пользователям осуществлять вход в систему только один раз, а затем получать доступ ко множеству приложений/сервисов без повторной аутентификации. Если на веб-портале существует несколько обширных независимых разделов (форум, чат, блог и т. д.) то, пройдя процедуру аутентификации в одном из сервисов, пользователь автоматически получает доступ ко всем остальным, что избавляет его от многократного ввода данных своей учётной записи.

SSO — это всегда совместная работа двух приложений: поставщика учетных записей (англ. Identity Provider, далее по тексту сокращенно «IdP») и поставщика сервиса (англ. Service Provider, далее по тексту сокращенно «SP»). **Р7-Офис SSO** реализует **только SP**. В качестве IdP может выступать множество различных провайдеров, но в этой статье мы рассмотрим реализацию OneLogin.

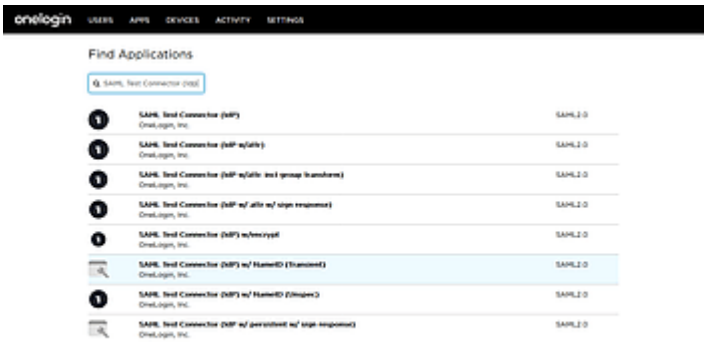
Подготовка Р7-Офис для настройки SSO

1. Установите версию Р7-Офис. Сервер. Профессиональный для Docker с поддержкой SSO.
2. Привяжите доменное имя, например, myportal-address.com.
3. На портале перейдите в **Панель управления -> HTTPS**, создайте и примените сертификат letsencrypt для шифрования трафика (для включения HTTPS на портале).
4. Перейдите на хостовую машину, скопируйте значения закрытого ключа и открытого сертификата, которые вы использовали для включения HTTPS, и сохраните их в любом текстовом редакторе, например, в Блокноте (эти значения потребуются позже для настройки SSO).

Примечание: не требуется выполнять **Пункт 4**, если есть уже готовые действующие сертификаты или вы хотите проверить самоподписанные сертификаты.

Создание IdP в OneLogin

1. Зарегистрируйтесь в OneLogin, если ещё не зарегистрировались.
2. Войдите в OneLogin под учетной записью администратора.
3. Перейдите в меню **APPS -> Add Apps**.
4. В строке для поиска **Find Application** введите следующий текст: SAML Test Connector (Idp:



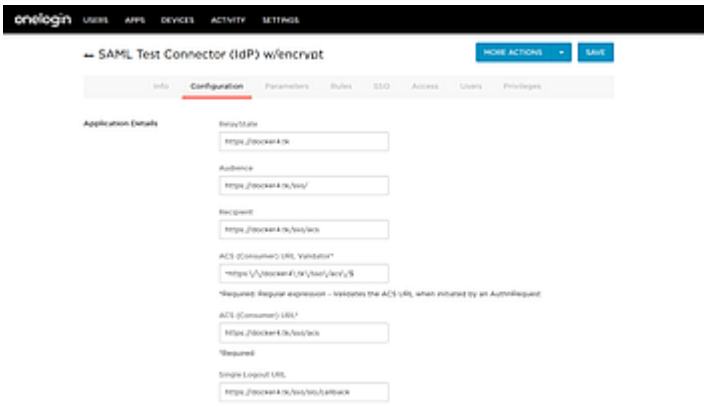
5. Среди полученных вариантов выберите подходящий, например, **SAML Test Connector (IdP) w/encrypt.**
6. В новом открывшемся окне напишите любое имя в поле **Display Name**, чтобы отличать это приложение от других, смените иконки на собственные и нажмите кнопку **Save**.

7. Примечание: Перейдите в подменю **Configuration** и заполните поля в соответствии с приведенной ниже таблицей: вместо myportal-address.com укажите собственное доменное имя или публичный IP-адрес, на котором располагается Р7-Офис SP.

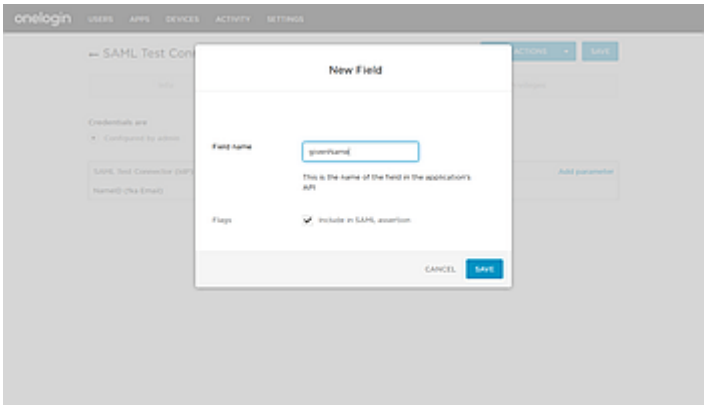
APPLICATION DETAILS	
RELAYSTATE	https://myportal-address.com
AUDIENCE	https://myportal-address.com/sso/

RECIPIENT	https://myportal-address.com/sso/acs
ACS (CONSUMER) URL VALIDATOR	^https:\/\/myportal-address\.com\/sso\/acs\/$
ACS (CONSUMER) URL	https://myportal-address.com/sso/acs
SINGLE LOGOUT URL	https://myportal-address.com/sso/slo/callback
SAML ENCRYPTION	
PUBLIC KEY *	-----BEGIN CERTIFICATE----- MIIE9zCCA9+gAwIBAgISA5VHo5m3/9NM1/gv8SDlE7vxMA0GCSqGSIb3DQEBCwUA MEoxCzAJBgNVBAYTAlVTMRYwFAYDVQQKEw1MZXQncyBFbmNyeXB0MSMwIQYDVQQD ExpMZXQncyBFbmNyeXB0IEF1dGhvcml0eSBYMzAeFw0xNzA1MzExNTEzMDBaFw0x NzA4MjkxNTEzMDBaMBUxEzARBgNVBAMTCmRvY2tlcjQudGswggEiMA0GCSqGSIb3 DQEBAQUAA4IBDwAwggEKAoIBAQC/LuH8Hcu0DUz2b8lFiUYHK1l2R55m/3ap9DsA /BbOJdbnFm/v5dTgUL4Vx73aX8vl2I5ePh5siNrhEuc7d8VfQ62WqLHM/3jz0wVi vFJN4rRVZAOK/S7zfTGf6HUloi0Jg+Rol2zh0IfWUN+UczClJ0b0zewYEF8ZLhNY W65X2fx6BahK6zbRotNj3tJy0zib6znqBOPhT999pnk5L0S+CfzNhVHH/V+IPVtX Tu9tSILnFQpVAsv3oKo/7n/N/F9t5bI/kMllXQFReq1a+9KTOv0OlZgEd7xMu8ht 707IdILRBAW3f1iMMT43DpmjkcST7NnNEbsLXSlBIwKz8GENAgMBAAGjggIKMIIC BjAOBgNVHQ8BAf8EBAMCBaAwHQYDVR0lBBYwFAYIKwYBBQUHAwEGCCsGAQUFBwMC MAwGA1UdEwEB/wQCMAAwHQYDVR0OBBYEFOqivMdw2WduQJmO1lXsq9E3zEvmMB8G A1UdIwQYMBaAFKhKamMEfd265tE5t6ZFZe/zqOyhMG8GCCsGAQUFBwEBBGMwYTAu BggrBgEFBQcwAYYiaHR0cDovL29jc3AuaW50LXgzLmxldHNlbmNyeXB0Lm9yZzAv BggrBgEFBQcwAoYjaHR0cDovL2NlcnQuaW50LXgzLmxldHNlbmNyeXB0Lm9yZy8w FQYDVR0RBA4wDIIKZG9ja2VyNC50azCB/gYDVR0gBIH2MIHzMAgGBmeBDAECATCB 5gYLKwYBBAGC3xMBAQEwgdYwJgYIKwYBBQUHAgEWGmh0dHA6Ly9jcHMubGV0c2Vu Y3J5cHQub3JnMIGrBggrBgEFBQcCAjCBngyBm1RoaXMgQ2VydGlmaWNhdGUgbWF5 IG9ubHkgYmUgcmVsaWVkIHVwb24gYnkgUmVseWluZyBQYXJ0aWVzIGFuZCBvbmx5 IGluIGFjY29yZGFuY2Ugd2l0aCB0aGUgQ2VydGlmaWNhdGUgUG9saWN5IGZvdW5k IGF0IGh0dHBzOi8vbGV0c2VuY3J5cHQub3JnL3JlcG9zaXRvcnkvMA0GCSqGSIb3 DQEBCwUAA4IBAQBltwpwwcQGMvap2hGhBQnZoS8bJ5iuq24KmEl3TrLdtLyklPy2 oR1HXgfW5fpTCGP744pVBwGXO2A8+2J6/wcNybo/odoB9dSzAMfRtXQR83XN4F8l 6E5zShBZ1kkzJayk4RytSzBR+uyTR1J7erK1MxlmOgQfLp2JqQsdEO6qpycER5pY mK77eWGrEE2+tOwgY4amlnLgBSif+nieUgQiSRboHGSF6nizES2pBKTk595P4pzK 9W5ax4zjqwQnMQujcjrHm7kbny2gFLH1wl0MY0yRlBytaFOhSWvr2g5JDFjgoFtd xEe8PMKA+cfU+0SznX/ynMgrz4MqSRRtQChx -----END CERTIFICATE-----

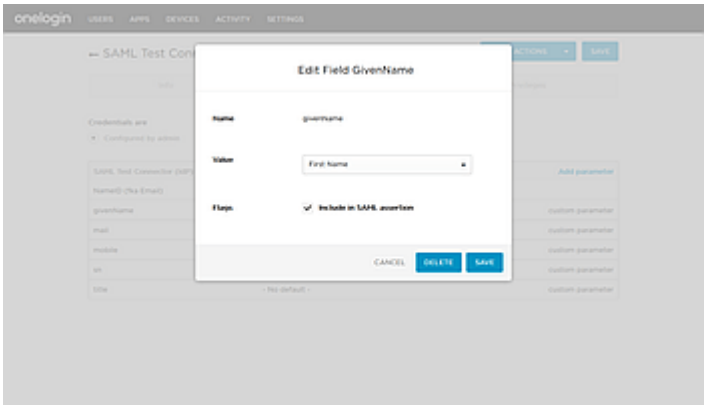
Примечание: * Здесь представлен пример сертификата HTTPS для доменного имени myportal-address.com, созданный с помощью сервиса letsencrypt.



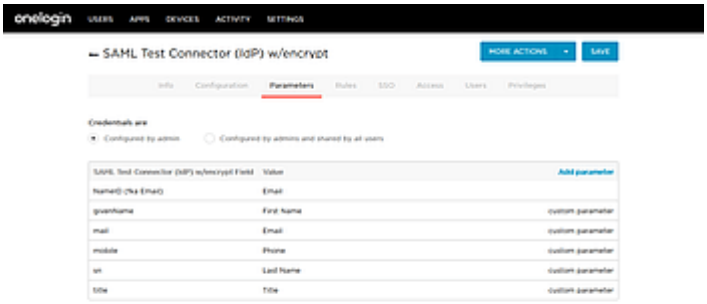
8. Нажмите кнопку **Save** и перейдите в подменю **Parameters**. Используйте ссылку **Add parameter**, чтобы создать 5 параметров (`givenName`, `sn`, `mail`, `title`, `mobile`), для каждого из них отметив опцию **Include in SAML assertion**:



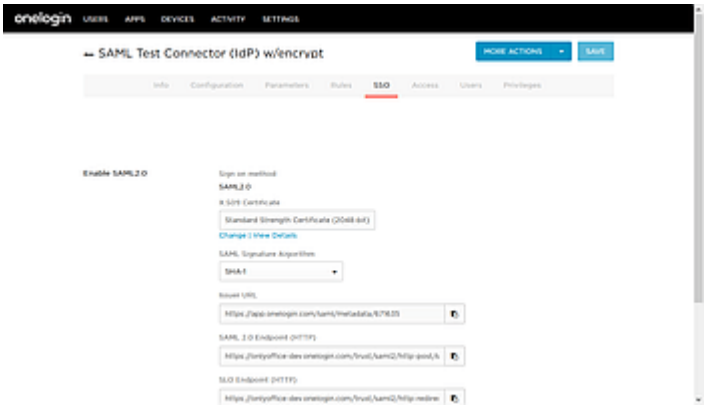
9. Отредактируйте значение каждого параметра, выбирая подходящее значение из списка:



10. Когда все нужные поля для атрибутов в утверждениях SAML будут заполнены в IdP, получится примерно такой же результат, как на следующем изображении. Нажмите кнопку **Save**.



11. Перейдите в подменю **SSO**:



Скопируйте ссылку из поля **Issuer URL** (например, https://app.onelogin.com/saml/metadata/666179) и перейдите на портал Р7-Офис под учетной записью администратора. Откройте страницу **Панель управления -> SSO**.

Настройка Р7-Офис SP

1. Убедитесь, что вы зашли в качестве администратора в **Панель управления** Р7-Офис, и щелкните вкладку **SSO**.
   Примечание: Вы можете зарегистрировать только одного корпоративного поставщика учетных записей для вашей организации на портале Р7-Офис.
2. Включите SSO, используя переключатель **Включить аутентификацию с помощью технологии единого входа**. Ссылку, скопированную из поля **Issuer URL** в OneLogin, вставьте в поле **URL-адрес XML-файла метаданных** IdP.Нажмите кнопку со стрелкой вверх, чтобы загрузить метаданные IdP. Форма **Настройки поставщика сервиса Р7-Офис** будет автоматически заполнена данными из OneLogin IdP.
3. В поле **Пользовательская надпись для кнопки входа** вы можете ввести любой текст вместо стандартного «Single Sign-on«. Этот текст будет отображаться на кнопке для входа с помощью сервиса Single Sign-on на странице аутентификации портала Р7-Офис.
4. Теперь необходимо добавить сертификаты в раздел **Сертификаты поставщика сервиса**. Можно добавить сертификаты, взятые ранее при настройке HTTPS, или любые другие.
   Примечание: открытый сертификат в OneLogin должен быть тем же, что и сертификат, загруженный в разделе Сертификаты поставщика сервиса, и закрытый ключ должен к нему подходить.

   Примечание: Форму с заголовком **Сопоставление атрибутов** настраивать не нужно, так как мы указали эти же параметры при создании OneLogin IdP.
5. Нажмите кнопку **Сохранить**. Должен открыться раздел **Метаданные поставщика сервиса Р7-Офис**. Проверьте, что настройки доступны публично,

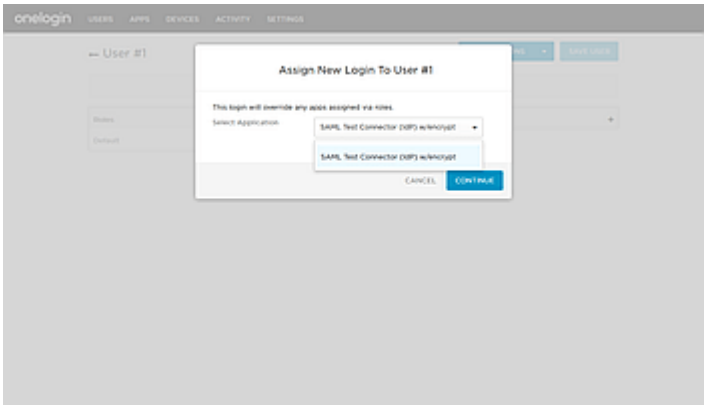
кликнув по кнопке **СКАЧАТЬ XML-ФАЙЛ МЕТАДАННЫХ ПОСТАВЩИКА СЕРВИСА**. Должно отобразиться содержимое XML-файла.

Создание пользователей в OneLogin и предоставление им доступа к Р7-Офис

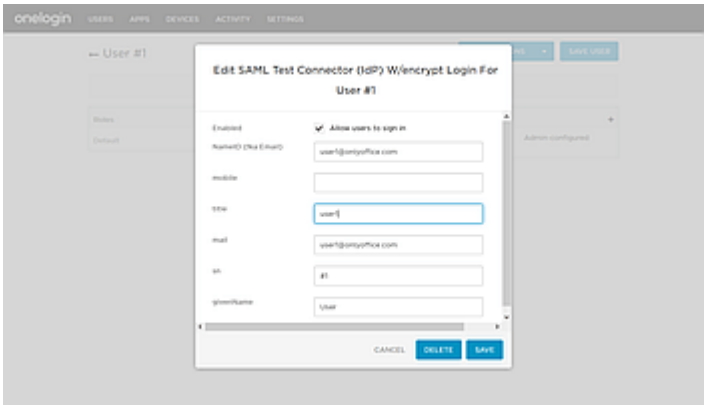
Чтобы создать пользователей в OneLogin и предоставить им доступ к Р7-Офис SP, выполните следующие действия:

1. перейдите на страницу **All Users** в OneLogin под учетной записью администратора

2. создайте нового пользователя или отредактируйте уже существующего,
3. перейдите в подменю **Applications**,
4. выберите наше новое созданное приложение из списка и нажмите **CONTINUE**,



5. в новом открывшемся окне добавьте недостающие данные, если это необходимо, или просто закройте его

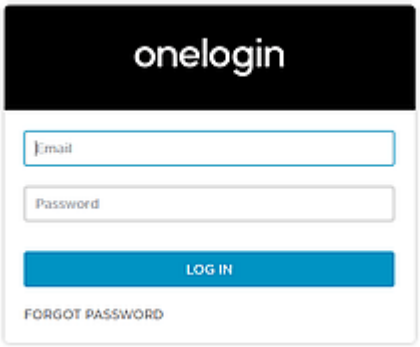


6. нажмите кнопку SAVE USER,
7. теперь пользователь может работать в Р7-Офис SP.

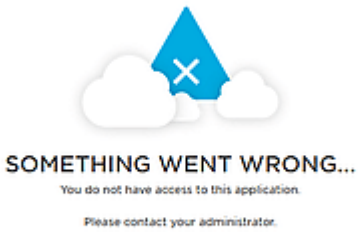
Проверка работы Р7-Офис SP и OneLogin IdP

Вход в Р7-Офис на стороне SP

1. Перейдите на страницу аутентификации Р7-Офис (например, https://myportal-address.com/auth.aspx).
2. Нажмите на кнопку Single sign-on (название кнопки может отличаться, если вы указали свой вариант при настройке Р7-Офис SP). Если этой кнопки нет, то SSO не включен.
3. Если всё настроено верно в SP и IdP, мы будем перенаправлены на форму логина в OneLogin IdP



4. Введите логин и пароль пользователя, которому дан доступ к Р7-Офис SP, и нажмите кнопку LOG IN.
5. Если выдаётся такая страница, то пользователю не предоставлен доступ к Р7-Офис SP



В этом случае нужно выйти из OneLogin и повторить шаги 1—4, но используя учетные данные другого пользователя.

6. Если учетные данные указаны правильно, мы будем перенаправлены на главную страницу портала (если такого пользователя нет на портале, он будет создан автоматически, а если данные были изменены в IdP, они будут обновлены).

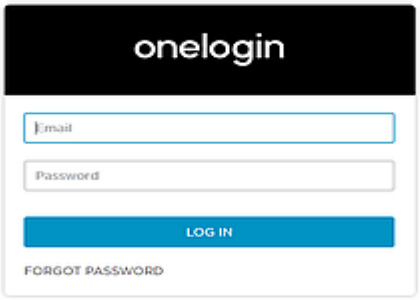
Профили пользователей, добавленных с помощью SSO-аутентификации

Возможность редактирования профилей пользователей, созданных с помощью SSO-аутентификации, ограничена. Поля профиля пользователя, полученные из IdP, заблокированы для редактирования (а именно: Имя, Фамилия, Email, Позиция и Местоположение). Эти поля можно отредактировать только из вашей учетной записи в IdP.

Пользователи, созданные с помощью SSO-аутентификации, отмечены в списке пользователей значком SSO для администраторов портала:

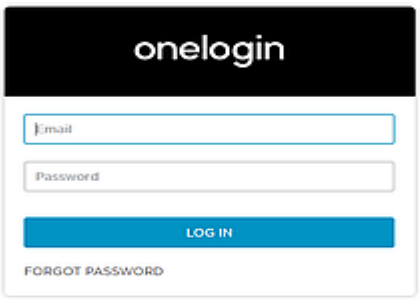
Выход из Р7-Офис SP

1. Выход можно осуществить с портала, используя пункт меню Выйти. Пользователь также должен автоматически выйти из OneLogin IdP, если он вышел из всех других приложений, к которым ему дали доступ в OneLogin и куда он произвёл вход до этого.
2. При удачном выходе вы будете перенаправлены страницу аутентификации портала.
3. Если перейти на страницу с приложением (например, https://companypage.onelogin.com/login), вы увидите форму логина

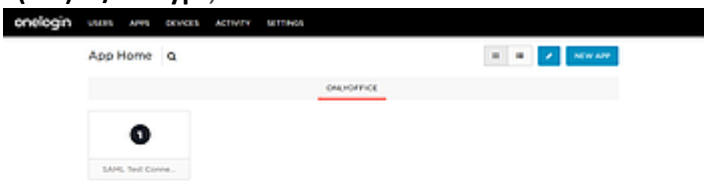


Вход в Р7-Офис на стороне Onlogin IdP

1. Перейдите на страницу вашей компании в OneLogin (например, https://companypage.onelogin.com/login).
2. Войдите, используя ваши учетные данные в OnleLogin.



3. Если учетные данные указаны правильно, вы будете перенаправлены на страницу с приложениями, доступ к которым предоставил вам администратор вашей компании в OneLogin. Нажмите на нужное приложение (например, **SAML Test Connector (IdP) w/encrypt**).



4. Если всё настроено верно, вы будете перенаправлены на портал myportal-address.com.

Выход из OneLogin IdP

1. Перейдите на страницу вашей компании в OneLogin (например, https://companypage.onelogin.com/) и нажмите на пункт меню **Выход**.
2. Если всё пройдёт правильно, вы выйдете из портала и будете перенаправлены на страницу логина в OneLogin.

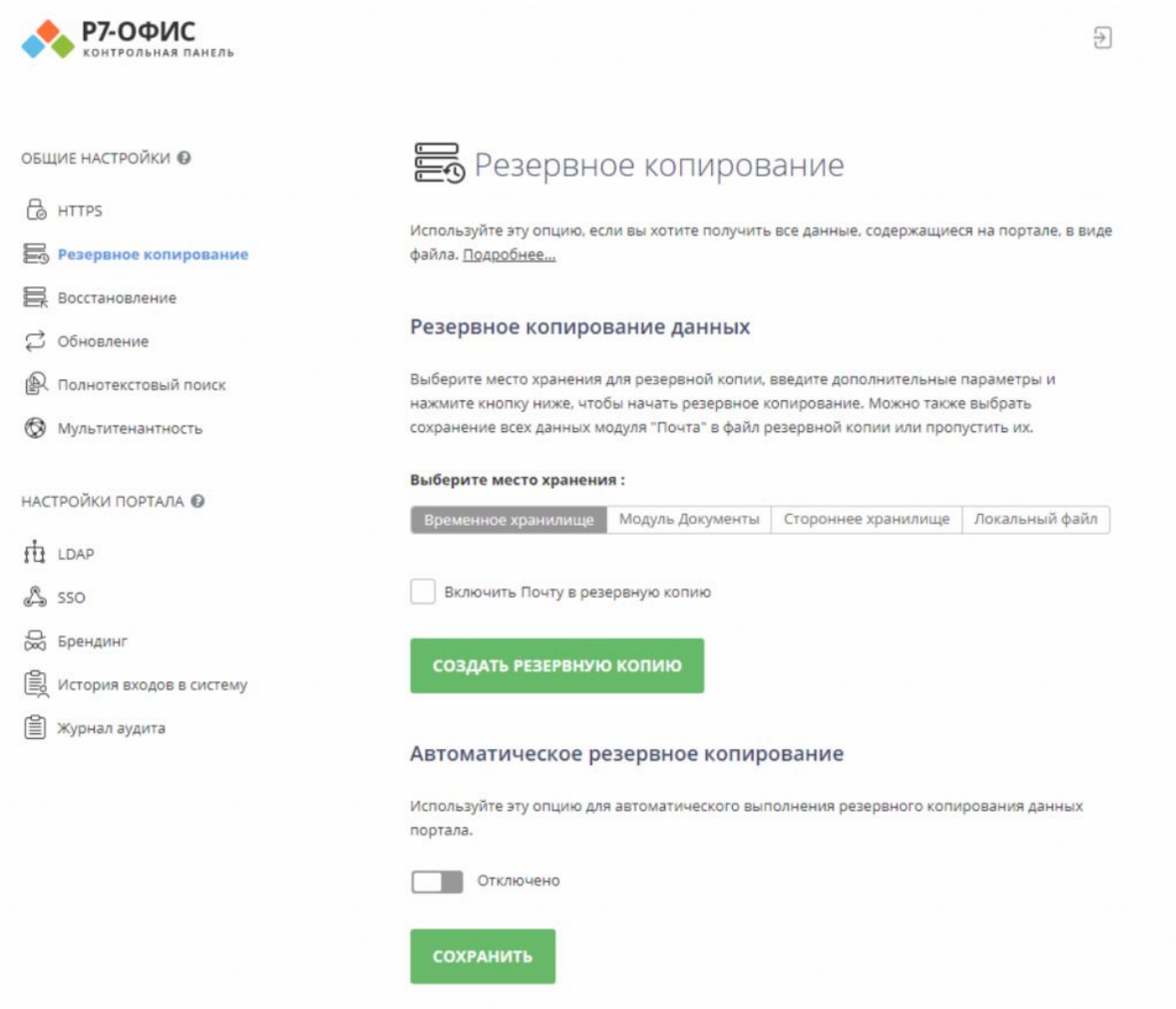
Использование функции резервного копирования и восстановления данных в Панели управления Р7-Офис

Введение

В Панели управления доступна возможность резервного копирования и восстановления, которая позволяет выполнять резервное копирование данных портала и восстанавливать их в серверной версии Р7-Офис. Чтобы открыть Панель управления, войдите на портал и нажмите на ссылку «Панель управления» на Стартовой странице. Можно также перейти в «Настройки» портала и нажать на ссылку ‘Панель управления’ на левой боковой панели.

Резервное копирование данных

Чтобы вручную создать резервную копию данных портала, перейдите на страницу **Резервное копирование** в **Панели управления** и используйте раздел **Резервное копирование данных**:

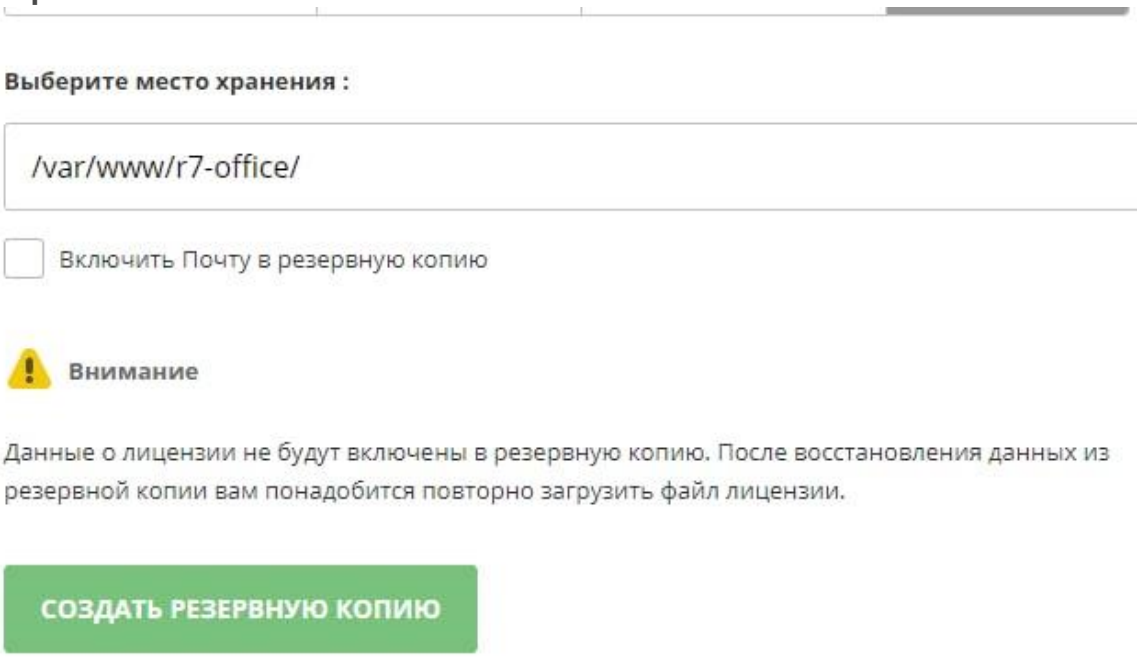


1. выберите требуемое **Хранилище** для файлов резервных копий:
   - отметьте переключатель **Временное хранилище**, если по завершении резервного копирования вы хотите скачать резервную копию на локальный диск. Это можно будет сделать с помощью ссылки, появившейся ниже.
   - отметьте переключатель **Модуль Документы** и нажмите кнопку **Плюс** рядом с полем, появившимся ниже. Откроется окно **Выбрать папку**. Укажите папку в разделе **Общие документы**, в которой надо сохранить резервную копию, и нажмите кнопку **ОК**.
   - отметьте переключатель **Стороннее хранилище**, если вы хотите сохранить резервную копию на облачное хранилище. В появившемся ниже поле место куда вы хотите сохранить резервную копию. На данный момент поддерживается хранилище Яндекс.Диск (прочитать о

том как подключить Яндекс.Диск, а так же хранилища по WebDAV можно тут)

- отметьте переключатель **Локальный файл** если вы хотите сохранить резервную копию на локальном диске. В появившемся ниже поле **Выберите место хранения** укажите путь к папке, в которой вы хотите сохранить резервную копию.

Например:



Обратите внимание на **права доступа к каталогу** для пользователя от которого делается резервная копия.

Примечание: При выборе опции **Модуль Документы** размер файла резервной копии влияет на общее занятое дисковое пространство на портале.

2. установите флажок **Включить Почту в резервную копию**, если вы хотите также выполнить резервное копирование данных **Почты**. Это увеличит время выполнения резервного копирования и размер файла резервной копии, но, если эта опция отключена, данные модуля **Почта** будут потеряны после восстановления, и учетные записи придется подключать заново.

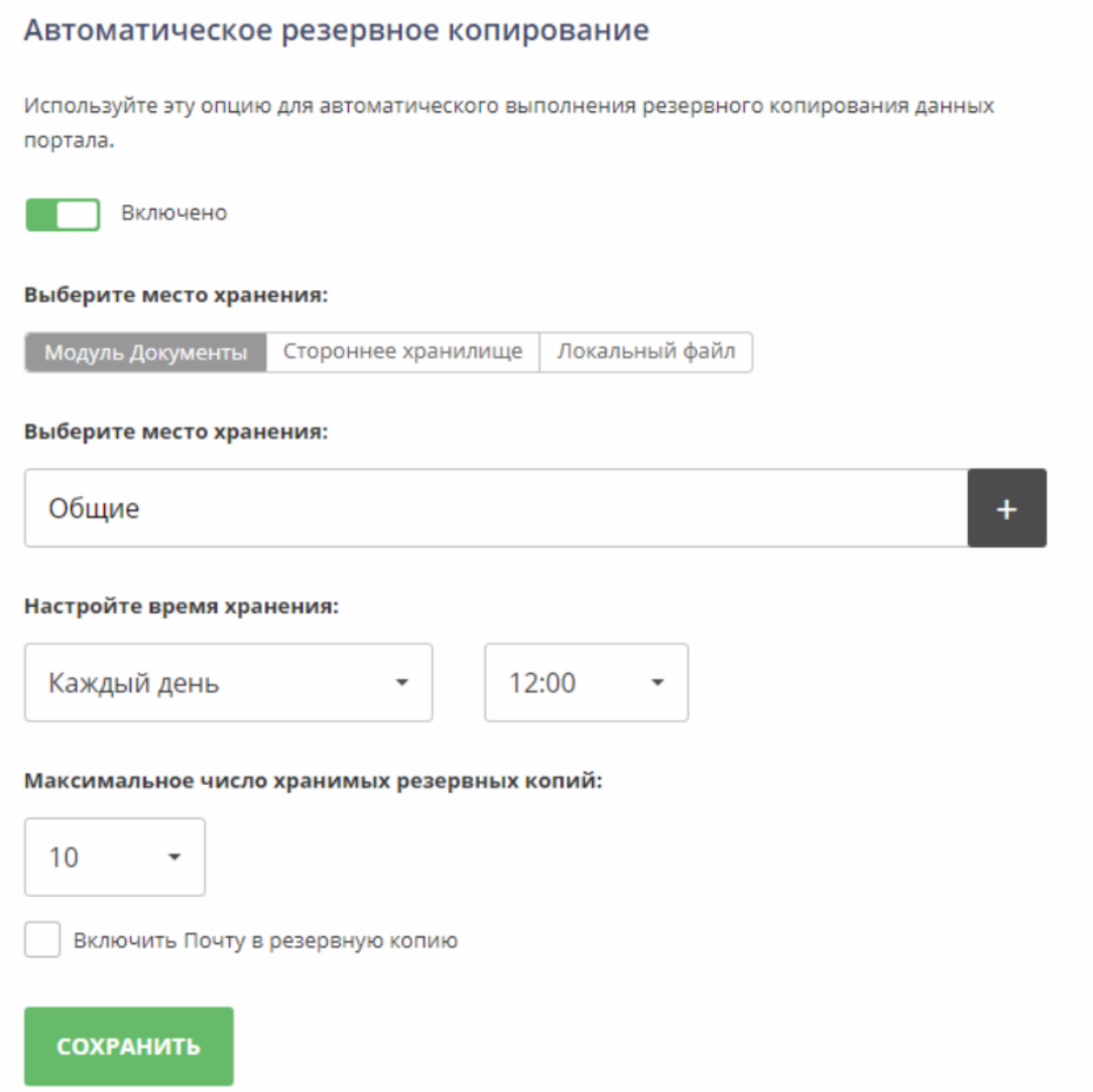
Примечание: Данные о лицензии не будут включены в резервную копию. После восстановления данных из резервной копии вам понадобится повторно загрузить файл лицензии.

3. нажмите на кнопку **СОЗДАТЬ РЕЗЕРВНУЮ КОПИЮ**.

Когда резервное копирование завершится, вы найдете файл резервной копии в формате **.tar.gz** (имя-портала_дата_время.tar.gz) в указанной папке. Если вы выбрали **Временное хранилище**, ссылка для скачивания созданной резервной копии будет доступна в течение 24 часов.

Автоматическое резервное копирование

Для автоматизации процесса резервного копирования используйте раздел **Автоматическое резервное копирование** на странице **Резервное копирование** в **Панели управления**:



1. нажмите на переключатель **Отключено**, чтобы разрешить использование этой возможности.
2. выберите требуемое **Хранилище** для файлов резервных копий (доступны те же опции, что указаны выше, кроме Временного хранилища, которое доступно только в разделе **Резервное копирование данных**).
3. укажите промежуток времени, через который необходимо создавать резервные копии: **Каждый день** с указанием нужного времени суток, **Каждую**

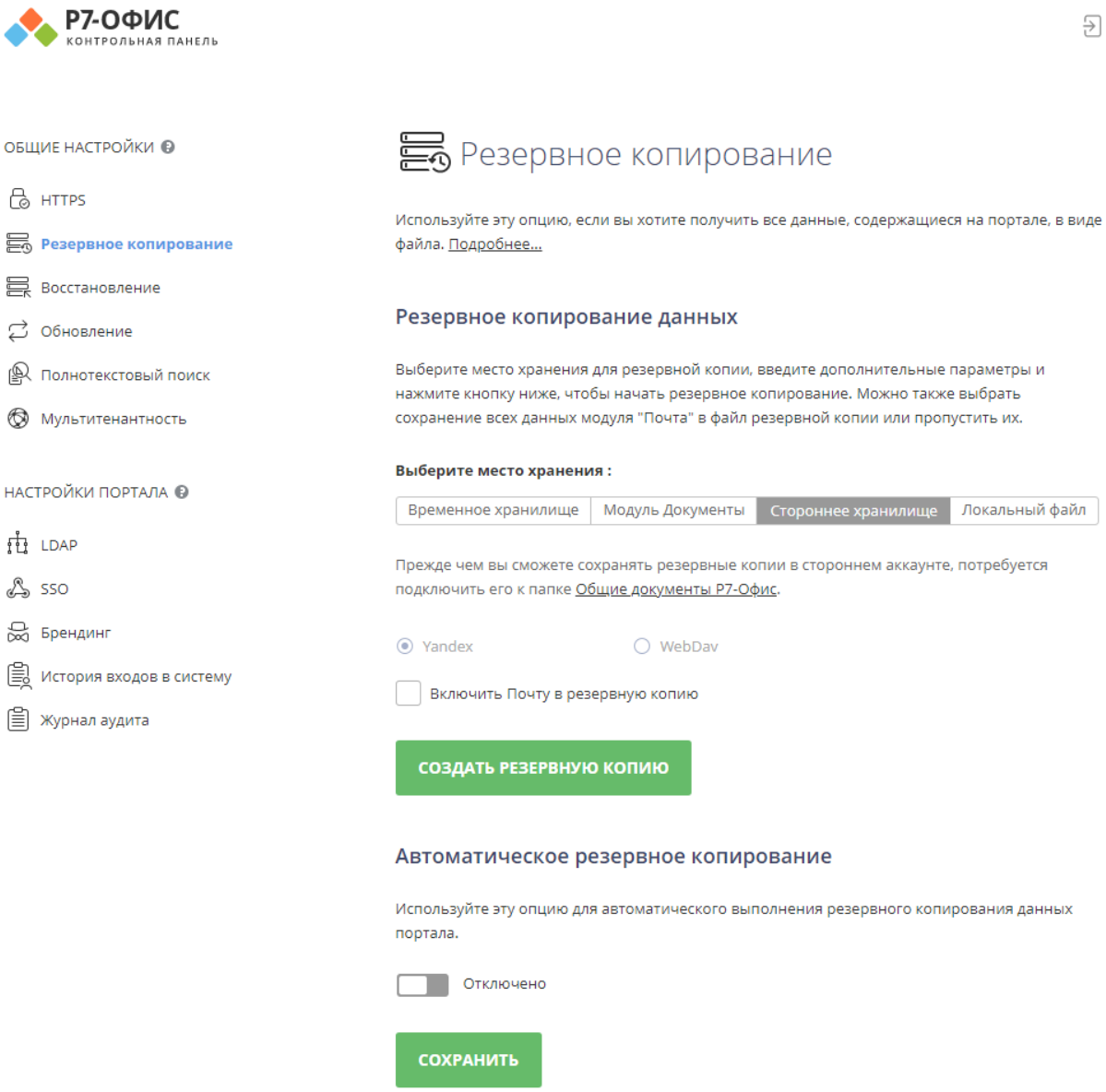
неделю с указанием нужного дня недели и времени суток или **Каждый месяц** с указанием нужной даты и времени суток.

4. задайте **Максимальное число хранимых резервных копий**, выбрав нужное значение (от 1 до 30) из выпадающего списка.
5. установите флажок **Включить Почту в резервную копию**, если вы хотите также выполнять резервное копирование данных **Почты**.
6. нажмите кнопку **СОХРАНИТЬ**.

Резервные копии будут создаваться автоматически с заданной периодичностью.

Восстановление данных из Сторонних хранилищ

Для восстановления данных портала из предварительно созданного файла резервной копии перейдите на страницу **Восстановление** в **Панели управления**.

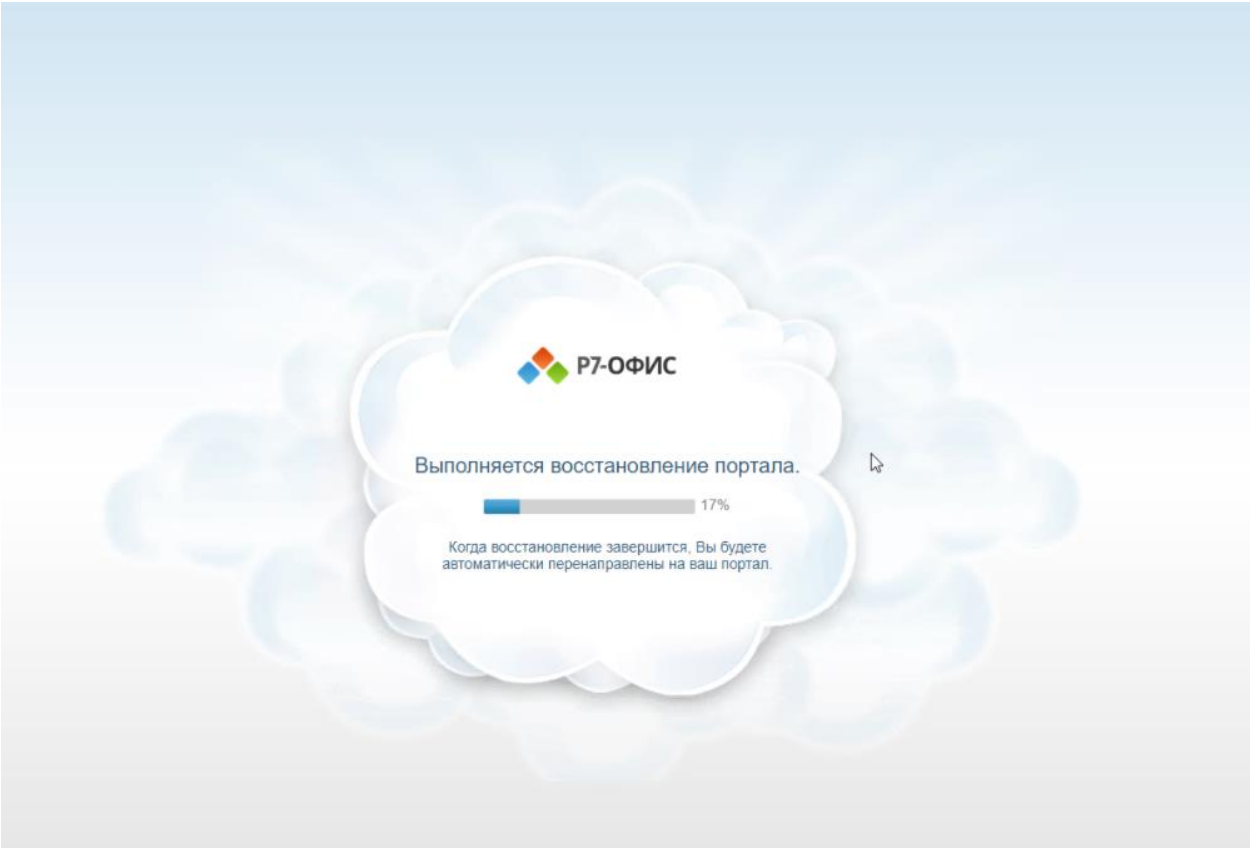


1. выберите **Источник**, где сохранены файлы резервных копий:

- отметьте переключатель **Стороннее хранилище**, выберите хранилище откуда требуется загрузить файл резервной копии. Далее выберите папку, где расположена резервная копия и нажмите кнопку **ОК**.
- отметьте переключатель **Локальный файл**, нажмите кнопку **Плюс** рядом с полем **Выберите место хранения** и найдите нужный файл резервной копии, сохраненный на локальном диске.

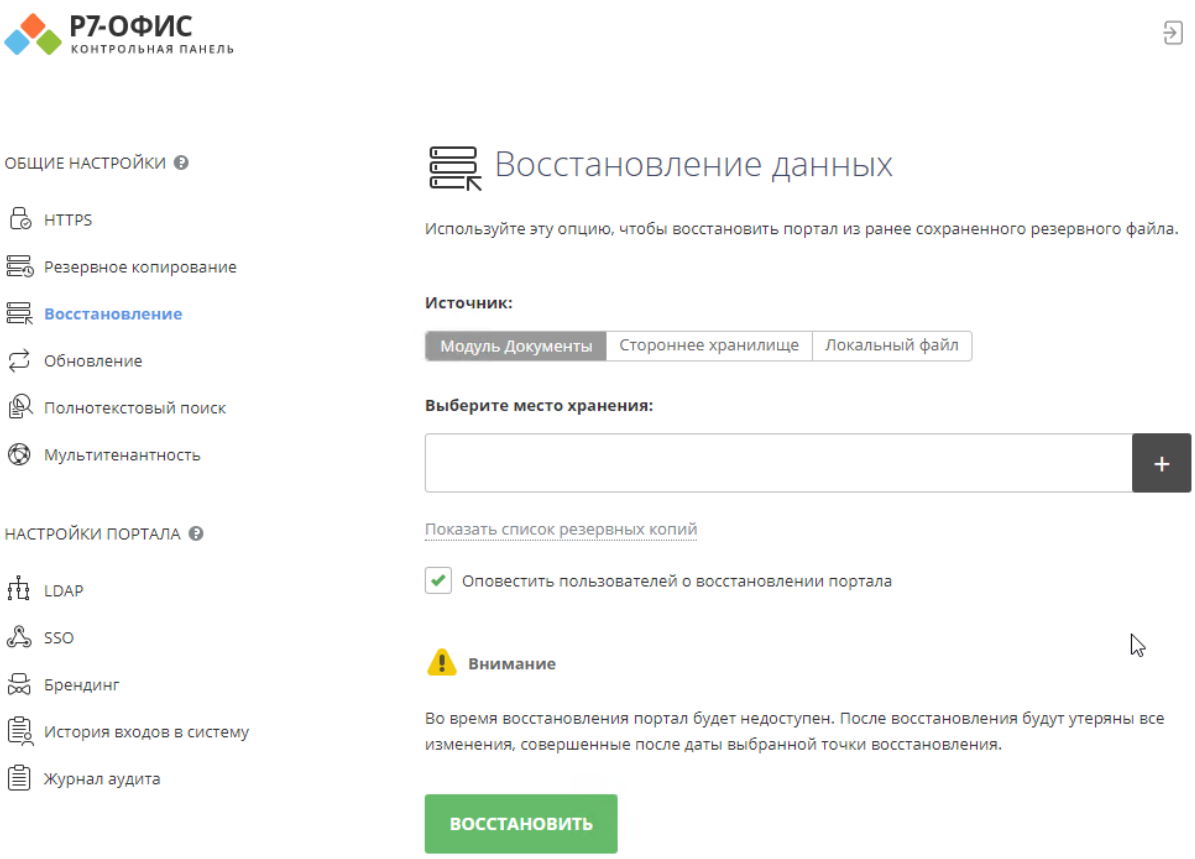
Примечание: Вместо того чтобы выбирать файл резервной копии из определенного **Источника**, можно нажать на ссылку **Показать список резервных копий** под переключателями, чтобы выбрать нужный файл из истории резервного копирования (если файл резервной копии был вручную удален из хранилища, он не будет доступен в списке). Нажмите на ссылку **Восстановить** рядом с нужным файлом резервной копии. Чтобы удалить файл резервной копии из этого списка, нажмите на значок **Удалить**.

1. в случае необходимости оставьте установленным флажок **Оповестить пользователей о восстановлении портала**, чтобы оповестить пользователей портала;
2. нажмите кнопку **ВОССТАНОВИТЬ**.
3. во время восстановления портала появится окно с процентом выполненных работ.



Восстановление данных из Модуля Документы

Для восстановления данных портала из предварительно созданного файла резервной копии перейдите на страницу **Восстановление** в **Панели управления**.



1. выберите **Источник**, где сохранены файлы резервных копий:
   - отметьте переключатель **Модуль Документы** и нажмите кнопку **Плюс** ниже. В окне **Выбрать файл** выберите нужный файл резервной копии, сохраненный в разделе **Общие документы**, и нажмите кнопку **ОК**.
   - отметьте переключатель **Локальный файл**, нажмите кнопку **Плюс** рядом с полем **Выберите место хранения** и найдите нужный файл резервной копии, сохраненный на локальном диске.*Примечание:* В случае, если ваша резервная копия более 100гб необходимо поменять значение по умолчанию в базе MySQL

Для Windows:

Пожалуйста, перейдите в меню Пуск — MySQL — Запустите MySQl Command Line Client
Введите пароль **r7-office**
Выберите базу данных **r7-office**:

```
use r7-office;
```

Выполните команду, где max_file_size задает максимальный размер файла в мегабайтах:

```
UPDATE tenants_quota SET `max_file_size`=512000 WHERE `tenant`=-1000;
UPDATE tenants_quota SET max_file_size=512000 WHERE tenant=-1;
```

Выполните выход из MySQL.

```
exit
```

Для применения изменений необходимо перезапустить сайты (Р7-Офис. Совместная работа и Р7-Офис. Совместная работа. Системное API) в IIS или выполнить полную перезагрузку сервера.

Для Linux:

```
mysql -p
```

Введите пароль **r7-office**
Выберите базу данных **r7-office**:

```
use r7-office;
```

Выполните команду, где max_file_size задает максимальный размер файла в мегабайтах:

```
UPDATE tenants_quota SET `max_file_size`=512000 WHERE `tenant`=-1000;
UPDATE tenants_quota SET max_file_size=512000 WHERE tenant=-1;
```

Выполните выход из MySQL.

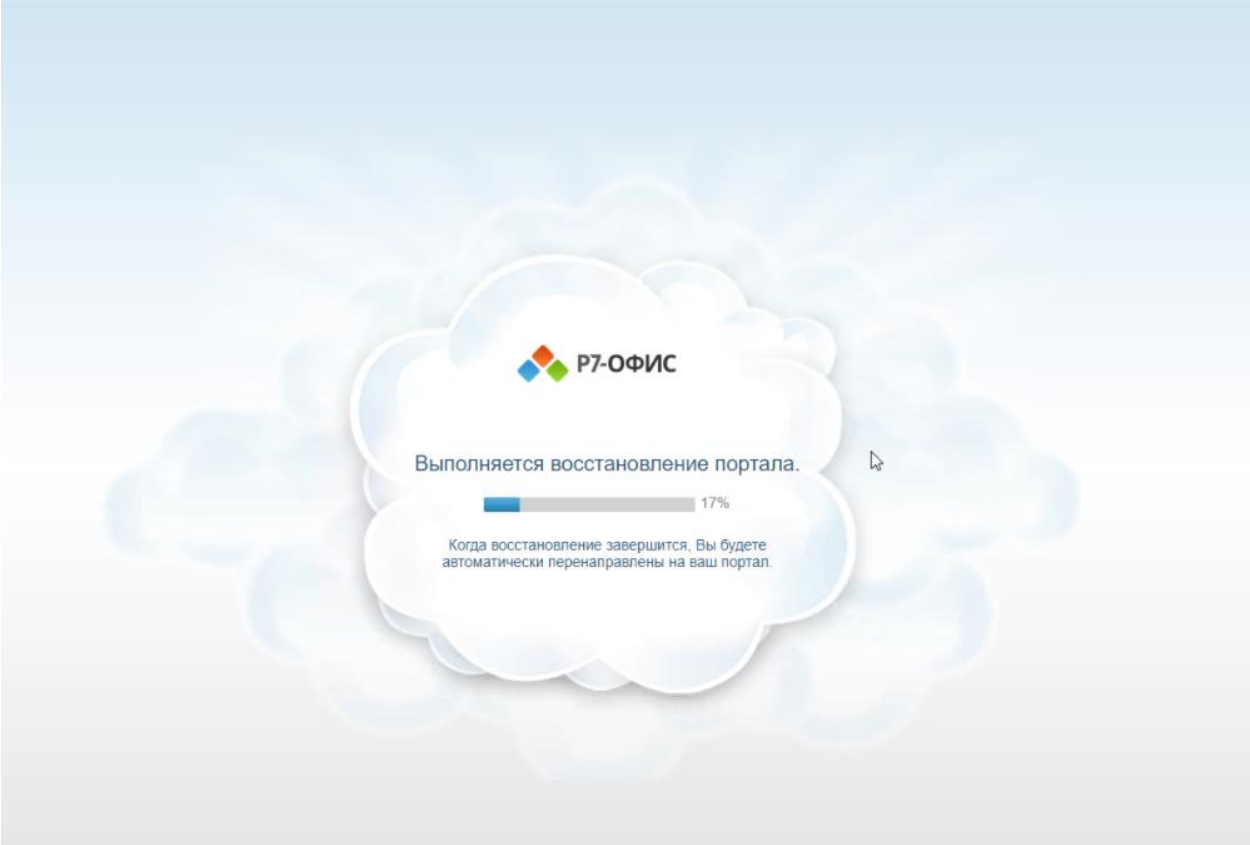
```
exit
```

Для применения изменений необходимо перезапустить сайты (Р7-Офис. Совместная работа и Р7-Офис. Совместная работа. Системное API) в IIS или выполнить полную перезагрузку сервера.

Примечание: Вместо того чтобы выбирать файл резервной копии из определенного **Источника**, можно нажать на ссылку **Показать список резервных копий** под переключателями, чтобы выбрать нужный файл из истории резервного копирования (если файл резервной копии был вручную удален из хранилища, он не будет доступен в списке). Нажмите на ссылку **Восстановить** рядом с нужным файлом

резервной копии. Чтобы удалить файл резервной копии из этого списка, нажмите на значок.

1. в случае необходимости оставьте установленным флажок **Оповестить пользователей о восстановлении портала**, чтобы оповестить пользователей портала;
2. нажмите кнопку **ВОССТАНОВИТЬ**.
3. Во время восстановления портала появится окно с процентом выполненных работ.



Примечание: В случае если восстановление портала происходит не на изначально установленном сервере и переносится на другой сервер, необходимо до момента авторизации на портале после восстановления скопировать значение параметра core.machinekey с сервера откуда переносится резервная копия и заменить на это значение параметр core.machinekey на сервере куда переносится резервная копия в файлах:

Для Windows:

```
C:\Program Files (x86)\R7-OFFICE\CommunityServer\WebStudio\web.appsettings.config
C:\Program Files (x86)\R7-OFFICE\CommunityServer\Services\TeamLabSvc\TeamLabSvc.exe.config
```

```
C:\Program Files (x86)\R7-OFFICE\CommunityServer\ApiSystem\Web.config
C:\Program Files (x86)\R7-OFFICE\CommunityServer\Services\MailAggregator\ASC.Mail.EmlDownloader.exe.config
C:\Program Files (x86)\R7-OFFICE\CommunityServer\Services\MailAggregator\ASC.Mail.Aggregator.CollectionService.exe.config
C:\Program Files (x86)\R7-OFFICE\ControlPanel\www\config\production.json
```

Для Linux:

```
/var/www/r7-office/WebStudio/web.appsettings.config
/var/www/r7-office/Services/TeamLabSvc/TeamLabSvc.exe.config
/var/www/r7-office/ApiSystem/Web.config
/var/www/r7-office/Services/MailAggregator/ASC.Mail.EmlDownloader.exe.config
/var/www/r7-office/Services/MailAggregator/ASC.Mail.Aggregator.CollectionService.exe.config
/var/www/r7-office/controlpanel/www/config/production.json
```

Значение core.machinekey во всех файлах должно быть одинаковое.
После редактирования файлов, для применения изменений необходимо выполнить полную перезагрузку сервера.

Примечание: Не забудьте, что по завершении восстановления потребуется повторно загрузить файл лицензии. Это можно сделать в разделе **Платежи**.

Изменение настроек LDAP

Если вы только что развернули **Р7-Офис. Сервер. Профессиональный** на своем сервере, то первое, что надо сделать, — это создать учетные записи для всех сотрудников компании. Если она насчитывает более 50 человек, создание новых пользователей портала займет много времени. Но теперь в **Панели управления** доступна опция **Поддержка LDAP**, которая позволяет буквально за несколько минут импортировать в онлайн-офис нужных пользователей и группы с сервера LDAP (например, OpenLDAP Server или Microsoft Active Directory). В свою очередь, новым пользователям не придется запоминать новые логины и пароли, поскольку они смогут заходить на портал под своими учетными данными, сохраненными на сервере LDAP.

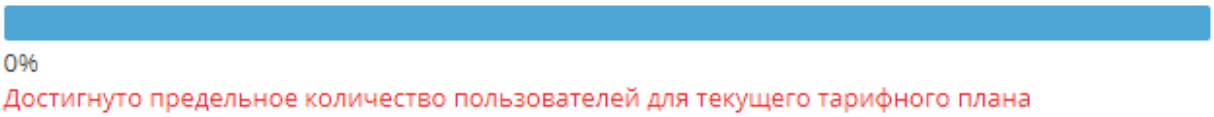
Чтобы открыть **Панель управления**, войдите на портал и нажмите на ссылку ‘Панель управления’ на **Стартовой странице**. Можно также перейти в ‘Настройки’ портала и нажать на ссылку ‘Панель управления’ на левой боковой панели.

Импорт пользователей и групп

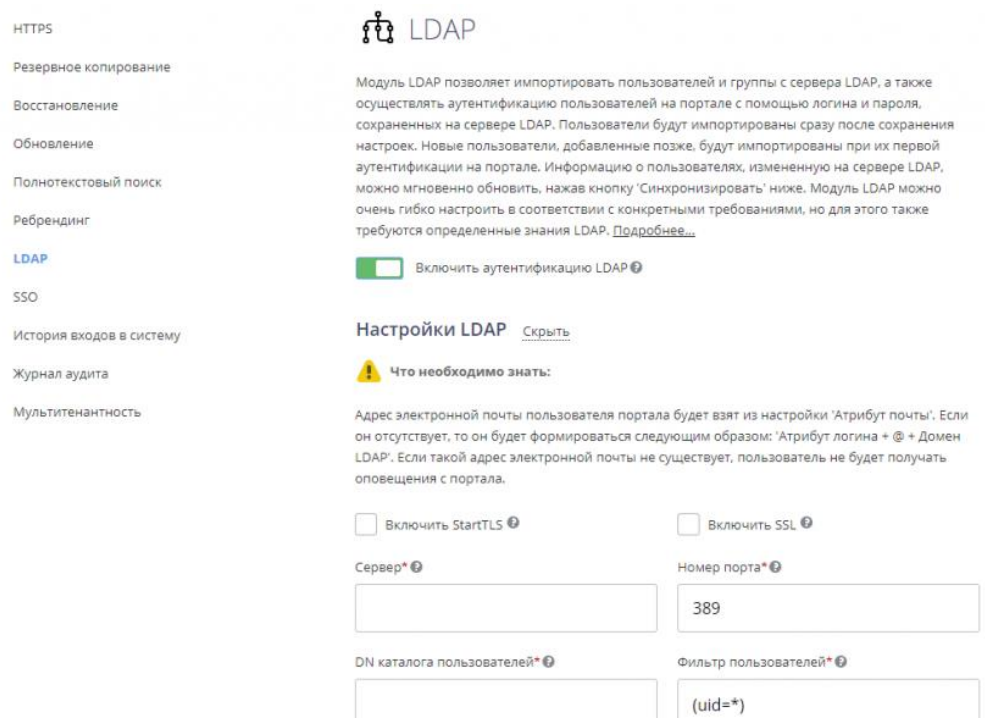
Перед началом импорта: Если вы подключаетесь к базе данных Active Directory, которая содержит более 1000 пользователей, вам потребуется увеличить лимит AD MaxPageSize = 1000 с помощью утилиты **ntdsutil**.

1. В **Панели управления** откройте страницу **LDAP**.
2. Нажмите на переключатель **Включить аутентификацию LDAP** и используйте ссылку **Показать** рядом с заголовком **Настройки LDAP**, чтобы отобразить форму для ввода параметров.
3. Установите флажок **Включить StartTLS**, если вы хотите обеспечить безопасное соединение с помощью технологии **StartTLS** (в этом случае используется стандартный порт 389). Установите флажок **Включить SSL**, если хотите использовать протокол **SSL** (в этом случае номер порта автоматически изменится на 636).
   При импорте пользователей из всего **доменного леса** (при наличии в лесу нескольких доменов) в **«DN каталога пользователей»** — необходимо указать **«DN корневого домена»** и использовать **порт** 3268.

Примечание:
Если вы используете пробную версию, при синхронизации с использованием порта 3268 (будет импортированы пользователи только с родительского домена) и вы получите сообщение:



4. Заполните поля, необходимые для импорта пользователей (обязательные поля помечены звездочкой)



Внимание: Обратите внимание, что в случае, если вы уже импортировали каких-то пользователей и меняете настройки (например, **Сервер**, **Фильтр пользователей**, **DN каталога пользователей**, **Фильтр групп**, **DN каталога групп**), существующие пользователи и все их данные, включая документы, сообщение электронной почты, другие, отсеянные новыми настройками, будут **ОТКЛЮЧЕНЫ**. Мы настоятельно рекомендуем сделать резервное копирование данных, прежде чем вы измените какие-либо настройки.

- в поле **Сервер** введите URL-адрес сервера LDAP в формате protocol://host, например, LDAP://example.com для обычного соединения с сервером LDAP или LDAPS://example.com для безопасного соединения с сервером LDAP по протоколу SSL. Вместо доменного имени можно также указать IP-адрес сервера: LDAP://192.168.3.202. Обратите внимание, что протокол(LDAP) нужно писать заглавными буквами.
- укажите **Номер порта**, используемый для соединения с сервером LDAP. Для обычного соединения с сервером LDAP по умолчанию используется порт 389. Если вы включили опцию StartTLS, также используется стандартный порт 389. Если включена опция SSL, номер порта автоматически изменяется на 636.
  При импорте пользователей из всего **доменного леса** (при наличии в лесу нескольких доменов) в **«DN каталога пользователей»** — необходимо указать **«DN корневого домена»** и использовать **порт** 3268.**Примечание:** Если вы используете пробную версию, при синхронизации с использованием порта 3268 (будет импортированы пользователи только с родительского домена) и вы получите сообщение:

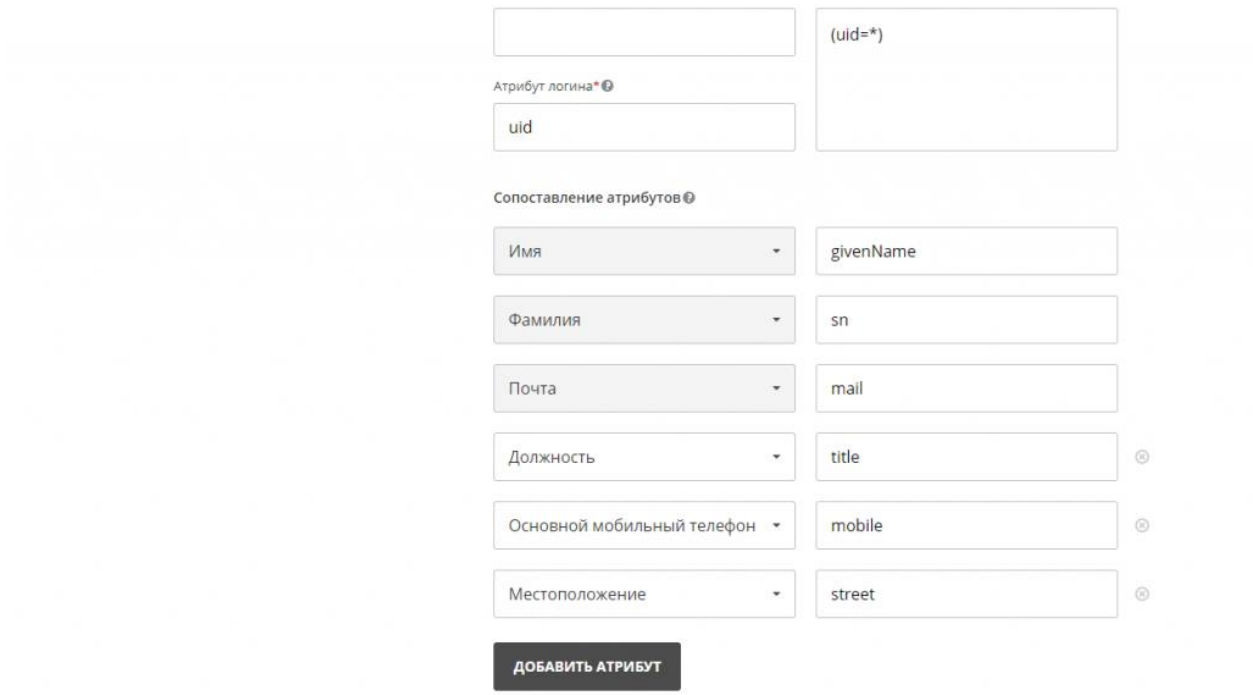
Достигнуто предельное количество пользователей для текущего тарифного плана

- в поле DN каталога пользователей (англ. User Distinguished Name) укажите абсолютный путь к каталогу верхнего уровня, содержащему пользователей, которых требуется импортировать. Этот параметр определяет узел, с которого начинается поиск. Можно указать корневой каталог, например, DC=example,DC=com, чтобы осуществлять поиск пользователей по всему каталогу, или задать определенную область поиска, например, OU=groupname,DC=example,DC=com, чтобы осуществлять поиск пользователей внутри указанной группы.
- заполните поле Фильтр пользователей, если необходимо импортировать пользователей, соответствующих указанным критериям поиска. Значение фильтра, заданное по умолчанию (uid=*), позволяет импортировать всех пользователей.
- Укажите Атрибут логина (атрибут в записи пользователя, соответствующий логину, который пользователи сервера LDAP будут использовать для входа в Р7-Офис).

Примечание: Пожалуйста, обратите внимание: настройки по умолчанию указаны для OpenLDAP Server. Для Active Directory необходимо изменить следующие настройки:

- **Фильтр пользователей** — (userPrincipalName=*)
- **Атрибут логина** — sAMAccountName

1. В разделе **Сопоставление атрибутов** можно установить соответствие между полями с данными пользователя на портале и атрибутами в записи пользователя на сервере LDAP. Нажмите кнопку **Добавить атрибут**, выберите из списка нужное поле данных и укажите атрибут пользователя, используемый на вашем сервере LDAP. Значения следующих параметров заданы по умолчанию, но в случае необходимости их можно изменить:

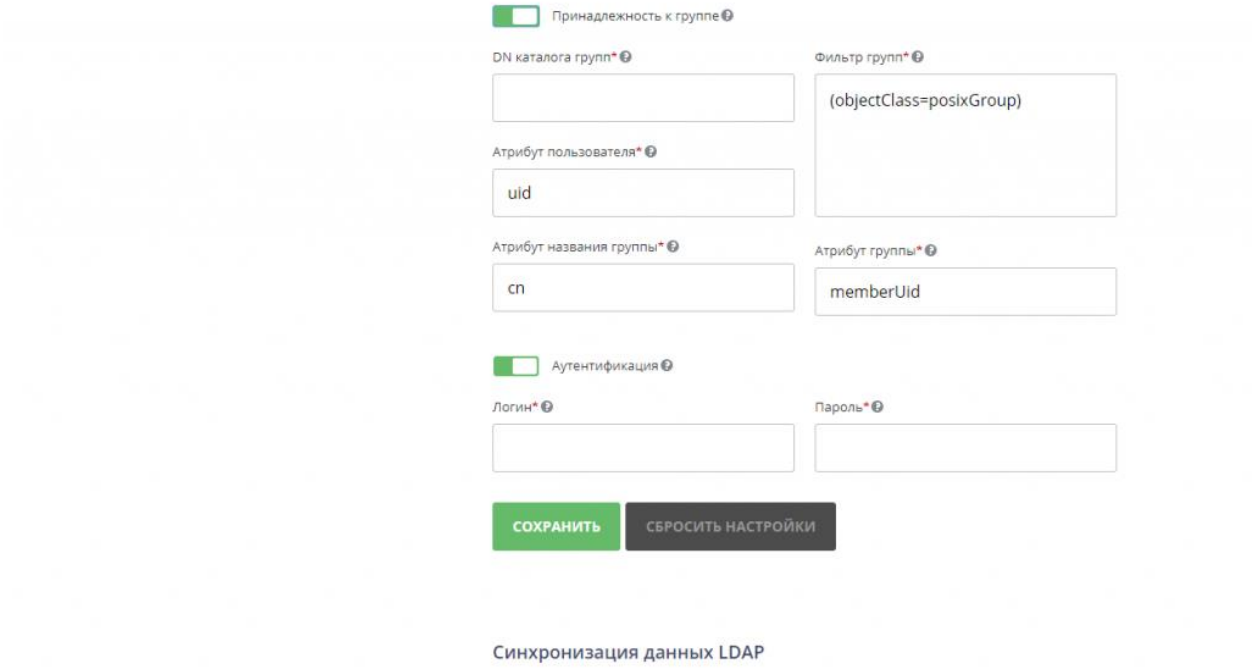


- **Имя** (атрибут в записи пользователя, соответствующий имени пользователя)
- **Фамилия** (атрибут в записи пользователя, соответствующий фамилии пользователя)
- **Почта** (атрибут в записи пользователя, соответствующий адресу электронной почты пользователя)
- **Должность** (атрибут в записи пользователя, соответствующий должности пользователя)
- **Основной мобильный телефон** (атрибут в записи пользователя, соответствующий номеру мобильного телефона пользователя)
- **Местоположение** (атрибут в записи пользователя, соответствующий местоположению пользователя)

Вы также можете добавить следующие атрибуты: **Дополнительная почта**, **Дополнительный мобильный телефон**, **Дополнительный телефон**, **Дата рождения**, **Фото профиля**, **Пол**, **Skype**.

2. Нажмите на переключатель **Принадлежность к группе**, если вы хотите добавить на портал группы с сервера LDAP, и заполните нужные поля:

Примечание: Пожалуйста, обратите внимание: если вы решите добавить группы, будут добавлены только те пользователи, которые состоят хотя бы в одной группе.



Внимание: Обратите внимание, что в случае, если вы уже импортировали каких-то пользователей и меняете настройки (например. **Сервер**, **Фильтр пользователей**, **DN каталога пользователей**, **Фильтр групп**, **DN каталога групп**), существующие пользователи и все их данные, включая документы, сообщение электронной почты, другие, отсеянные новыми настройками, будут **ОТКЛЮЧЕНЫ**. Мы настоятельно рекомендуем сделать резервное копирование данных, прежде чем вы измените какие-либо настройки.

- в поле **DN каталога групп** (англ. Group Distinguished Name) укажите абсолютный путь к каталогу верхнего уровня, содержащему группы, которые требуется импортировать,
  например, OU=Groups,DC=example,DC=com.
- заполните поле **Фильтр групп**, если необходимо импортировать группы, соответствующие указанным критериям поиска. Значение фильтра, заданное по умолчанию (objectClass=posixGroup), позволяет импортировать все группы.
- значения следующих параметров заданы по умолчанию, но в случае необходимости их можно изменить:
  - **Атрибут пользователя** (атрибут, который определяет, состоит ли этот пользователь в группах)
  - **Атрибут названия группы** (атрибут, который соответствует названию группы, в которой состоит пользователь)
  - **Атрибут группы** (атрибут, который указывает, какие пользователи состоят в этой группе)

Примечание: Пожалуйста, обратите внимание: настройки по умолчанию указаны для **OpenLDAP Server**. Для **Active Directory** необходимо изменить следующие настройки:

- **Фильтр групп** — (objectClass=group)
- **Атрибут пользователя** — distinguishedName
- **Атрибут группы** — member

3. Задайте **Настройки прав администратора**: нажмите на соответствующую кнопку, выберите полный доступ и укажите группу, которая должна иметь права администраторов с полным доступом. Выберите из списка какой-либо модуль портала и укажите группу, у которой должны быть права администратора в выбранном модуле.
4. Включите переключатель **Аутентификация**. В полях **Логин** и **Пароль** введите учетные данные пользователя, у которого есть права на чтение данных с сервера LDAP.
5. Нажмите кнопку **СОХРАНИТЬ**.
6. В открывшемся окне 'Подтверждение импорта' нажмите кнопку **ОК**, чтобы начать импорт пользователей.

Импорт займет некоторое время в зависимости от количества пользователей, групп, технических характеристик компьютера и т.д.

Примечание: Пожалуйста, обратите внимание: адрес электронной почты пользователя портала будет взят из настройки **Атрибут почты**. Если он отсутствует, то он будет формироваться следующим образом: Атрибут логина + @ + Домен LDAP.

- Если на портале есть ранее созданный пользователь с таким адресом электронной почты, этот пользователь автоматически будет синхронизирован с LDAP-пользователем.
- Если такой адрес электронной почты не существует, пользователь не будет получать никаких оповещений с портала.

Аутентификация LDAP-пользователей

Каждый импортированный пользователь сможет заходить на портал, используя логин, формируемый по следующим схемам:

- **Атрибут логина**, например Andrew.Stone
- **Атрибут логина + @ + Домен LDAP**, например Andrew.Stone@example.com
- **Домен LDAP + \ + Атрибут логина** (поддерживаются неполные имена доменов), например example\Andrew.Stone

Профили импортированных пользователей в модуле **Люди** будут отмечены значком LDAP для администратора портала. Поля профиля пользователя, импортированные по LDAP, заблокированы для редактирования.

Синхронизация данных LDAP

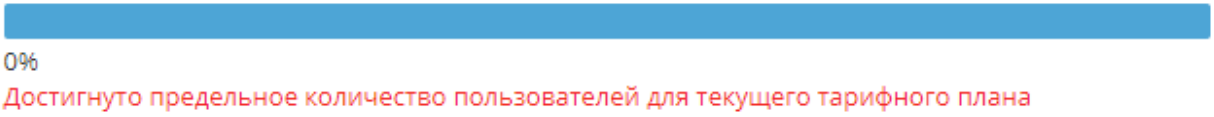
Если вы измените данные на сервере LDAP (например, добавите новых пользователей или группы, переименуете существующие группы или отредактируете какую-то информацию в записи пользователя), данные на портале можно легко синхронизировать с новой информацией с LDAP-сервера.

Чтобы настроить параметры синхронизации, включите переключатель **Автоматическая синхронизация** и задайте нужное время выполнения автоматической синхронизации: данные можно синхронизировать каждый час в указанные минуты, каждый день в указанное время, а также каждую неделю или месяц в указанный день и время. Нажмите кнопку **Сохранить**, чтобы применить настройки. Также можно синхронизировать данные вручную, нажав кнопку **СИНХРОНИЗИРОВАТЬ** внизу страницы **LDAP**. Можно также использовать кнопку **СОХРАНИТЬ** внизу раздела **Настройки LDAP**.

Информация об отдельном пользователе также будет синхронизирована после того, как этот пользователь войдет на портал.

Примечание

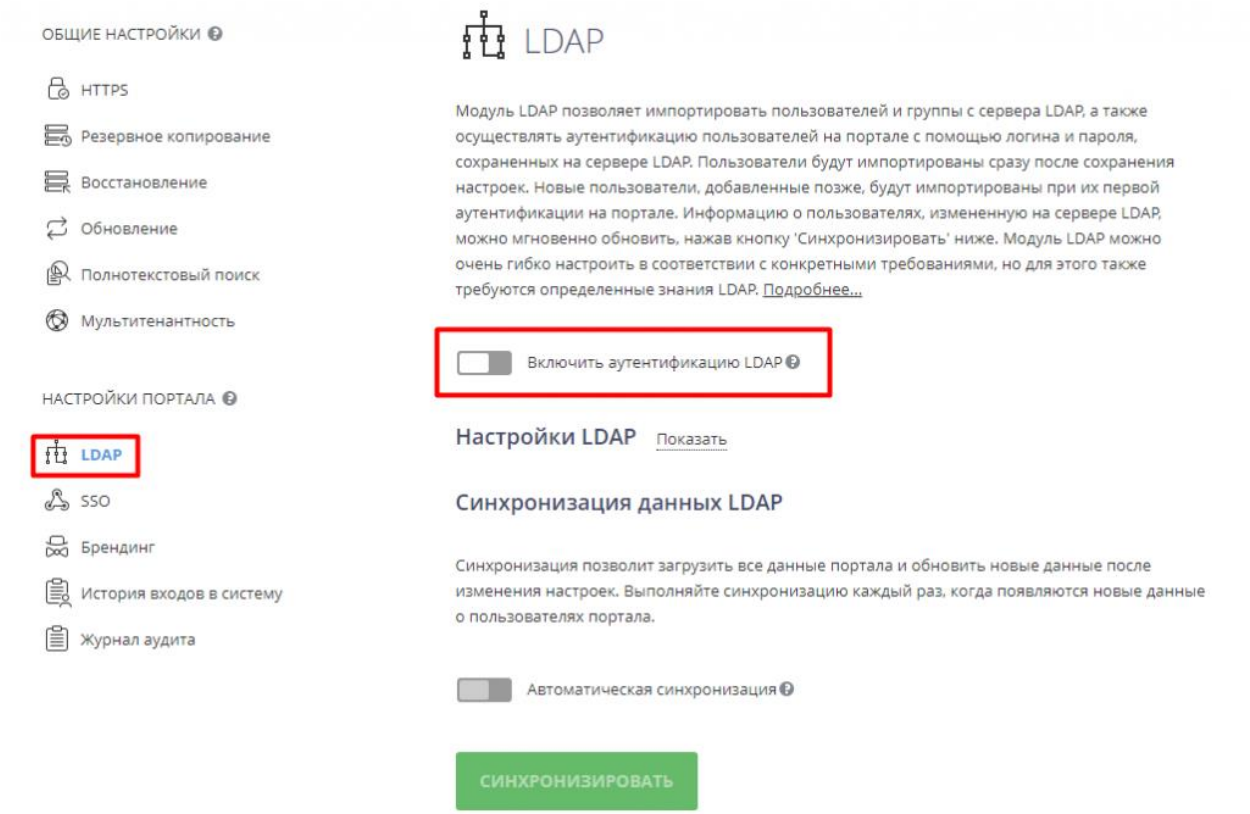
1. Если вы добавили DN каталог, в котором количество пользователей больше, чем указано в лицензии и получаете сообщение:



Необходимо указать в **DN каталоге групп** с меньшим кол-вом пользователей, для перезаписи данных синхронизации.

После удачной синхронизации, отключить **LDAP** и перейти в модуль Люди. Теперь пользователи **LDAP** отличные от вашей новой добавленной группы. Изменив статус пользователя на заблокированный, можно удалить пользователя.

2. Для удаления пользователя, синхронизированного с AD и пометкой LDAP, необходимо в **Панели управления** выключить синхронизацию **LDAP**



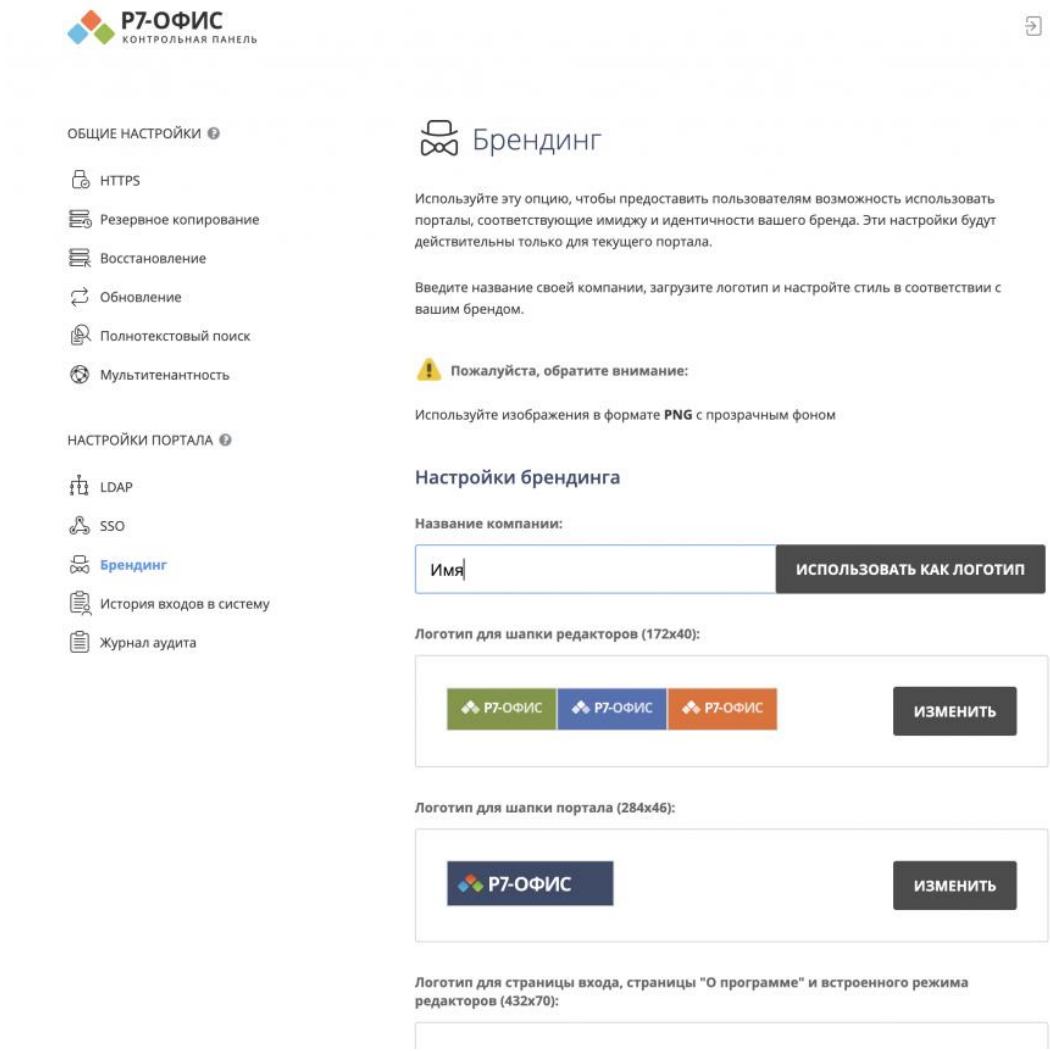
Ребрендинг онлайн-офиса

Если вы хотите использовать Р7-Офис. Сервер. Профессиональный под своим брендом, вы легко можете заменить элементы фирменного стиля, которые используются в интерфейсе онлайн-офиса, на ваши собственные.
Функция **Ребрендинг**, доступная в **Панели управления**, позволяет использовать название вашей компании в текстовых элементах (таких как подсказки, окна сообщений и т.д.), а также заменить используемые по умолчанию логотипы и иконку сайта на свой собственный логотип.

Чтобы открыть **Панель управления**, войдите на портал и нажмите на ссылку «Панель управления» на **Стартовой странице**. Можно также перейти в «Настройки» портала и нажать на ссылку ‘Панель управления’ на левой боковой панели.

Основные инструкции

1. В **Панели управления** откройте страницу **Брендинг**.



2. Введите **Название компании** в текстовом поле ввода, чтобы изменить в интерфейсе онлайн-офиса все надписи и сообщения, в которых использовано значение по умолчанию, заменив его на указанное вами значение. Нажмите кнопку **ИСПОЛЬЗОВАТЬ КАК ЛОГОТИП** справа от поля ввода, если вы хотите использовать название вашей компании в качестве текстового логотипа (вместо графического логотипа) — все представленные ниже логотипы изменятся соответствующим образом.
3. Замените все графические **Логотипы**, которые встречаются в онлайн-офисе:

Примечание: рекомендуется использовать изображения в формате **PNG** с прозрачным фоном. Чтобы улучшить читаемость логотипов и сделать их контур четко различимым, их также необходимо адаптировать под темные или светлые фоны. Размеры изображений должны точно соответствовать размерам, указанным рядом с каждым логотипом.

- **Логотип для шапки редакторов (172×40)** — этот логотип находится в левом верхнем углу запущенных онлайн-редакторов.
- **Логотип для оповещений по почте (432×70)** — этот логотип находится в левом верхнем углу электронных писем с оповещениями о событиях портала.
- **Логотип для шапки портала (284×46)** — этот логотип находится в левом верхнем углу любой страницы портала.
- **Логотип для страницы входа, страницы «О программе» и встроенного режима редакторов (432×70)** — этот логотип находится на странице **Входа** на портал, на странице **О программе** (профиль пользователя -> О программе) и в левом верхнем углу документов портала, встроенных в веб-страницы.
- **Иконка сайта (32×32)** — этот логотип находится в адресной строке или вкладке браузера, когда портал открыт в нем, или на панели закладок, если вы добавили адрес портала в закладки.

Нажмите на кнопку **ИЗМЕНИТЬ** справа от логотипа, который надо заменить. В открывшемся окне выберите нужный графический файл и нажмите кнопку **Открыть**. Изображение будет загружено и отображено в поле соответствующего **Логотипа**.

4. Нажмите кнопку **СОХРАНИТЬ** внизу страницы, чтобы заданные настройки вступили в силу.

Для возврата к настройкам по умолчанию нажмите кнопку **НАСТРОЙКИ ПО УМОЛЧАНИЮ**.

Получение данных журнала аудита

Подраздел **Журнал аудита** позволяет просматривать список последних изменений (создание, модифицирование, удаление и т.д.), внесенных пользователями в элементы (задачи, возможные сделки, файлы и т.д.) на портале.

Примечание: В настоящий момент эта возможность доступна только для модулей **Документы**, **Проекты**, **CRM** и **Люди**, а также для настроек портала.
На этой странице отображается только 20 последних записей. Каждая запись показывает, какое действие произведено, кто его выполнил, и когда произошло это событие. Вы также можете задать период, в течение которого хранятся данные. По умолчанию он составляет 180 дней.

Чтобы просмотреть подробную статистику за последние полгода, нажмите кнопку **Скачать и открыть отчет**. Отчет откроется в таблице в формате .xlsx *(Отчет по журналу аудита Дата начала-Дата окончания.xlsx)*.

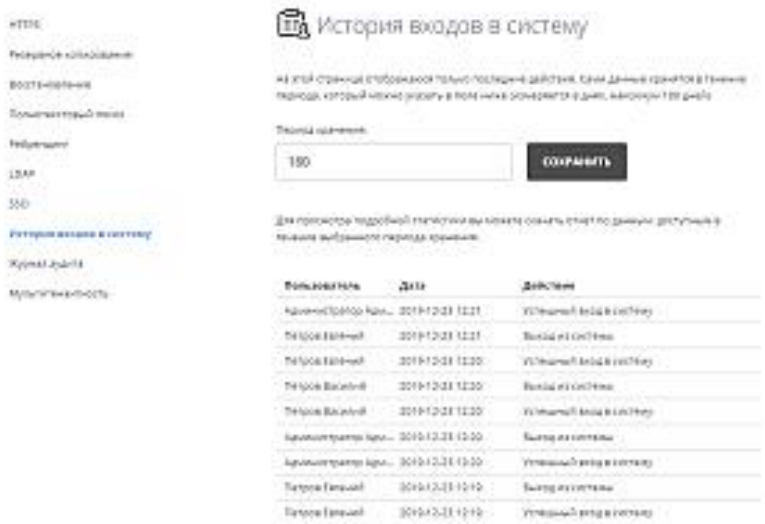
Примечание: Этот файл также будет автоматически сохранен в разделе Мои документы.
Отчет по журналу аудита содержит следующие сведения: **IP**-адрес пользователя, **Браузер** и **Платформа**, которые использовались в момент возникновения зарегистрированного события, **Дата** и время события, имя **Пользователя**, который выполнил эту операцию, **Страница** портала, на которой было выполнено это действие, общий **Тип действия** (например, *загрузка, прикрепление файла, обновление доступа*), конкретное **Действие** (например, *Проекты [Редактор электронных таблиц]. Задачи [Написание документации по редактору таблиц]. Обновлен статус: Закрыта*), **Продукт** и **Модуль**, к которым относится измененный элемент.

Записи отсортированы хронологически в порядке убывания, но вы можете легко сортировать и фильтровать данные по любому параметру или воспользоваться инструментом поиска, чтобы быстро найти определенную запись.

Отслеживание истории входов в систему

Подраздел **История входов в систему** в разделе настроек **Безопасности** используется для отслеживания последних операций входа в систему, выполненных пользователями, включая успешные входы на портал и неудачные попытки входа с указанием причин.

На этой странице отображается только 20 последних записей. Каждая запись показывает, какое действие произведено, кто его выполнил, и когда произошло это событие. Вы также можете задать период, в течение которого хранятся данные. По умолчанию он составляет 180 дней.



Чтобы просмотреть подробную статистику за последние полгода, нажмите кнопку **Скачать и открыть отчет**. Отчет откроется в таблице в формате .xlsx *(Отчет по истории входов в систему Дата начала-Дата окончания.xlsx)*.

Примечание: Этот файл также будет автоматически сохранен в разделе Мои документы.
Отчет по истории входов в систему содержит следующие сведения: **IP**-адрес пользователя, **Браузер** и **Платформа**, которые использовались в момент возникновения зарегистрированного события, **Дата** и время события, имя **Пользователя**, совершившего попытку входа или выхода, **Страница** портала, на которой было выполнено это действие, конкретное **Действие** (например, *Неудачная попытка входа. Не найден связанный аккаунт социальной сети*).

Записи отсортированы хронологически в порядке убывания, но вы можете легко сортировать и фильтровать данные по любому параметру или воспользоваться инструментом поиска, чтобы быстро найти определенную запись.

В разделе **Пользователи в сети** можно также просмотреть список пользователей, которые в данный момент находятся на портале, а также продолжительность сеанса каждого из этих пользователей.

Как переключить Р7-Офис. Сервер. Профессиональный на протокол HTTPS вручную с собственным сертификатом Windows версии?

Введение

В большинстве случаев доступ к порталу по протоколу HTTPS намного безопаснее, чем по протоколу HTTP, который используется по умолчанию. Но для изменения способа доступа к порталу необходимо выполнить определенные действия.

Прежде чем начинать переключение серверной версии **Р7-Офис. Сервер. Профессиональный** на протокол HTTPS, необходимо создать сертификат безопасности в формате .pem.

Примечание: Пожалуйста, убедитесь, что сертификат содержит **закрытый ключ**. Наличие закрытого ключа можно проверить, открыв сертификат в любом текстовом редакторе.

Когда у вас будет сертификат, переходите к описанным ниже действиям.

Переключение серверной версии Р7-Офис. Сервер. Профессиональный на HTTPS с помощью скрипта

Быстрее всего можно переключить **Р7-Офис. Сервер. Профессиональный** на протокол HTTPS с помощью готового скрипта. Пожалуйста, прочитайте эту статью, чтобы узнать, как это можно сделать.

Переключение серверной версии Р7-Офис. Сервер. Профессиональный на HTTPS вручную

Все действия, которые выполняет скрипт, вы можете выполнить вручную. Для этого следуйте инструкциям ниже.

Для текущей версии сервера используются службы IIS 7, у которых есть свои особенности. Сертификат безопасности необходимо привязать к серверной версии **Р7-Офис. Сервер. Профессиональный** с помощью встроенных инструментов служб IIS.

Примечание: Если у вас есть сертификат безопасности (самоподписанный или выданный сторонним центром сертификации), вы можете привязать его к серверной версии **Р7-Офис. Сервер. Профессиональный**:

1. Войдите в **Диспетчер служб IIS**.
2. Выберите сайт, к которому нужно привязать сертификат (портал Р7-Офис. Совместная работа).
3. Используйте опцию **Привязки...** на правой панели, чтобы открыть диалоговое окно **Привязки сайта**.
4. В открывшемся окне нажмите кнопку **Добавить...**.
5. Измените тип на https и выберите из выпадающего меню **SSL-сертификат** предварительно созданный сертификат.
6. Нажмите кнопку **OK**, а затем закройте окно **Привязки сайта**.

После этого ваш сертификат будет привязан к **Р7-Офис. Сервер. Профессиональный**. Если у вас есть еще какие-то вопросы о сертификатах в IIS 7, обратитесь к соответствующим статьям базы знаний Microsoft.

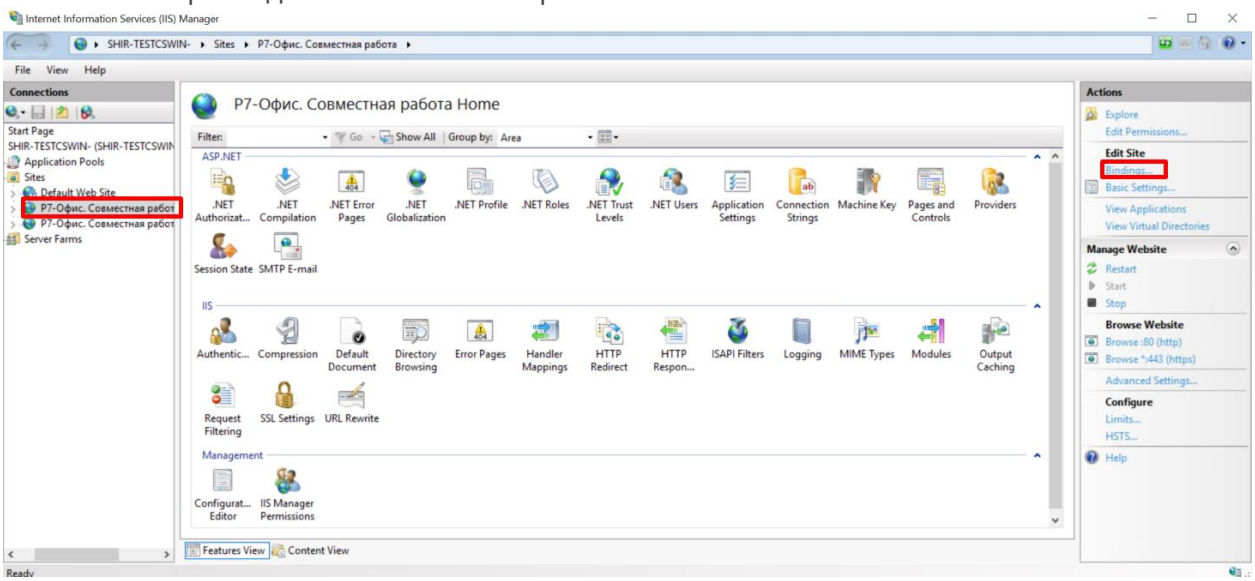
Если у вас нет сертификата, его можно создать с помощью **Диспетчера служб IIS**:

1. Войдите в **Диспетчер служб IIS**.
2. Перейдите к имени сервера, выделите его.
3. Дважды щелкните на опции **Сертификаты сервера** в разделе **IIS**.
4. Используйте опцию **Создать самозаверенный сертификат** на правой панели, чтобы открыть соответствующее диалоговое окно.
5. Введите нужное имя сертификата и нажмите кнопку **OK**.

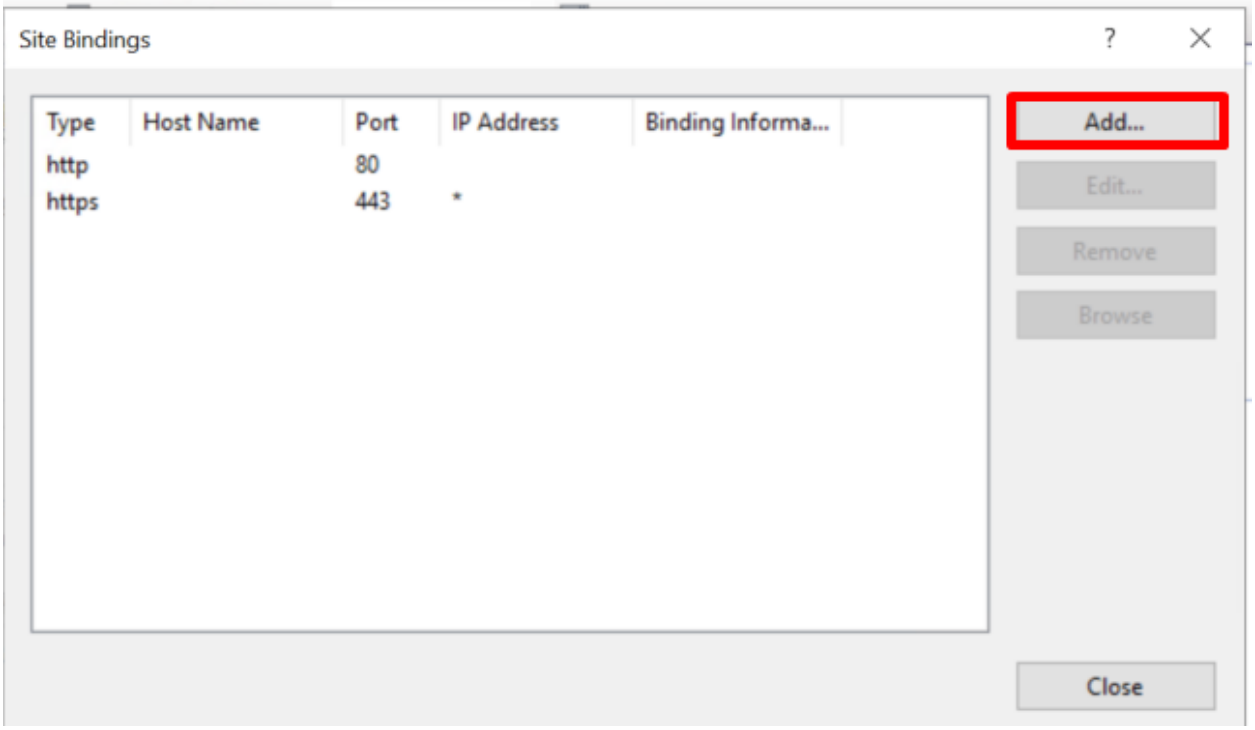
Теперь у вас есть самоподписанный сертификат со сроком действия 1 год.

Теперь надо включить для сервера правила переопределения, чтобы он обрабатывал HTTPS-запросы вместо HTTP. Для этого:

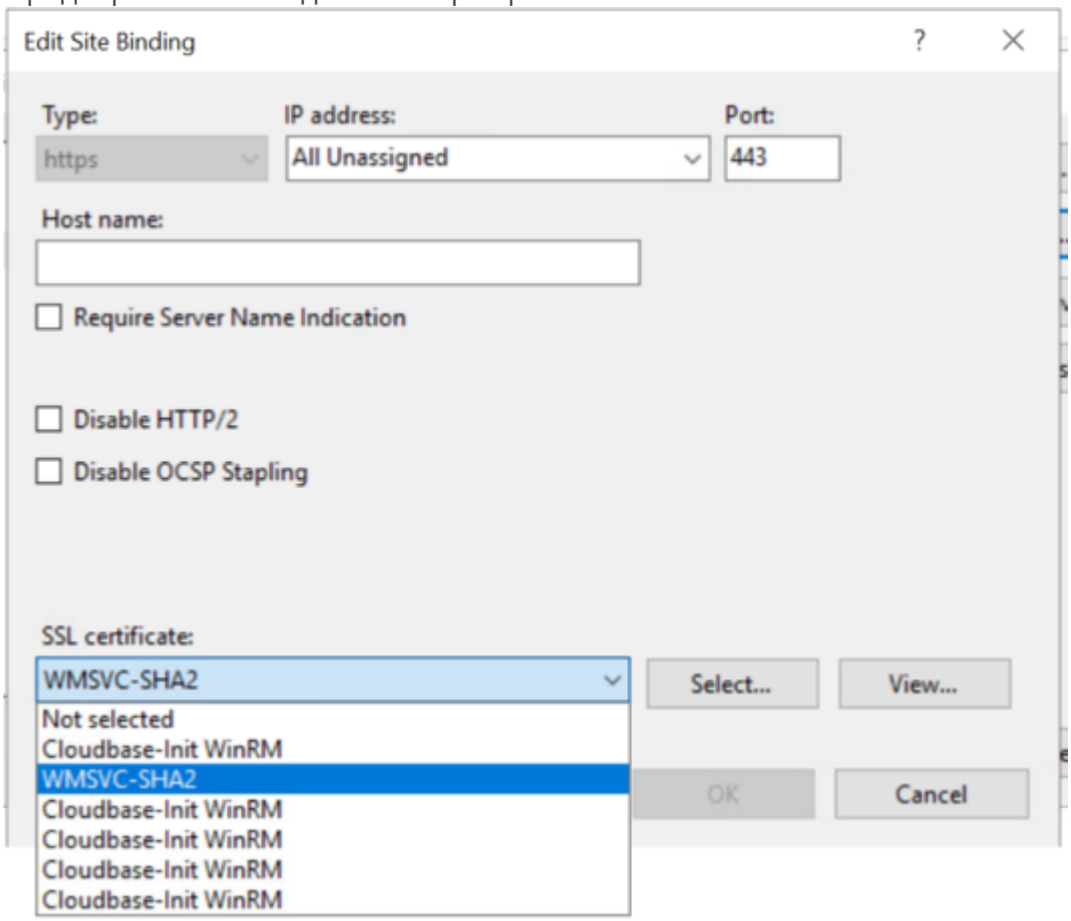
1. Войдите в **Диспетчер служб IIS**.
2. Выберите сайт, для которого надо включить HTTPS. Выберите сайт, к которому нужно привязать сертификат (портал Р7-Офис. Совместная работа). Используйте опцию Привязки (bindigs) на правой панели, чтобы открыть диалоговое окно Привязки сайта.



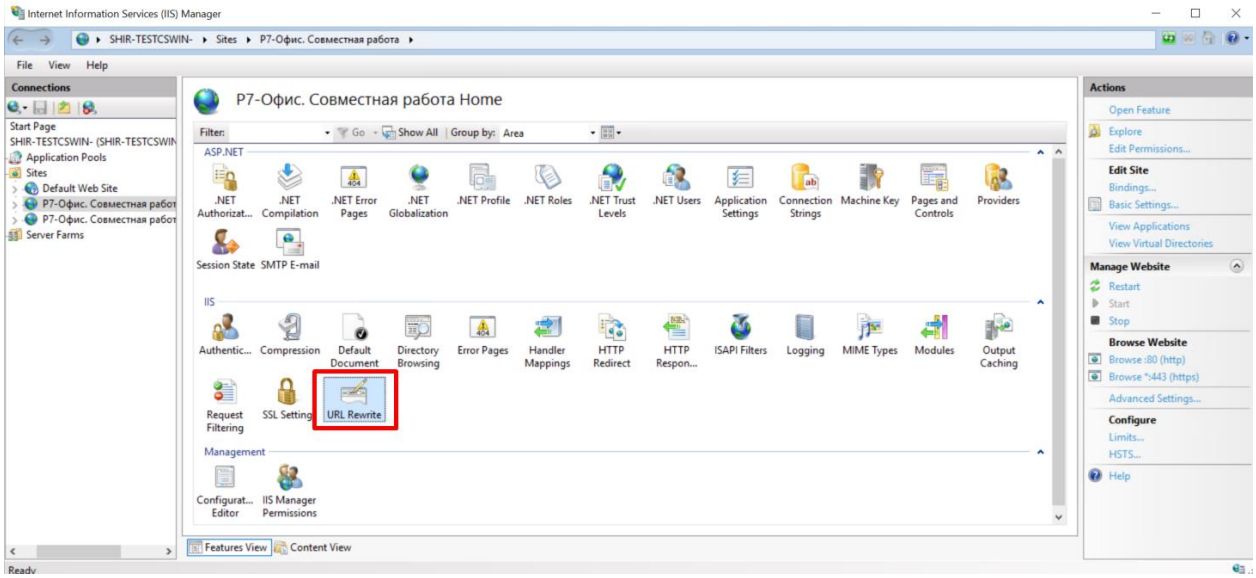
3. В открывшемся окне нажмите кнопку Добавить:



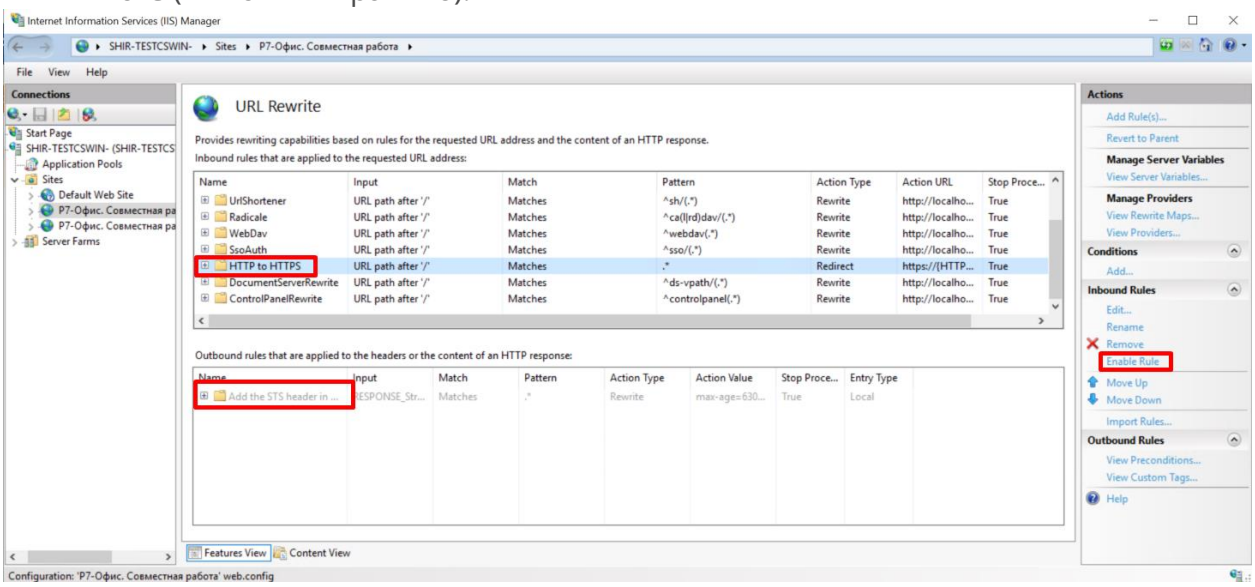
4. Измените тип на https и выберите из выпадающего меню SSL-сертификат предварительно созданный сертификат:



5. Используйте опцию **URL Rewrite** (Переопределение URL-адресов) в меню справа, чтобы открыть окно **URL Rewrite**.



6. Найдите следующие правила: HTTP to HTTPS и Add Strict-Transport-Security when HTTPS и для каждого из них выберите на правой панели опцию **Enable Rule** (Включить правило).



Следующие действия не являются обязательными, но если вы хотите обеспечить безопасность инсталляции **Р7-Офис. Сервер. Профессиональный**, настоятельно рекомендуется их выполнить. Перейдите на страницу IIS Crypto. Это бесплатный инструмент, который дает администраторам возможность включать или отключать протоколы, шифры, хэш-функции и алгоритмы смены ключей в Windows Server 2008, 2012 и 2016. Программа также позволяет переупорядочивать наборы шифров SSL/TLS, предлагаемых IIS, применять наилучшие методы в один клик, создавать пользовательские шаблоны и тестировать сайт. Скачайте и запустите эту программу, выберите опцию **Best Practices**, а затем **Apply**. После этого перезапустите сервер.

Проверить, все ли правильно получилось, можно следующим образом:

- Откройте портал, используя префикс https://. Если портал открывается и работает, значит, вы все сделали правильно.
- Если **Р7-Офис. Сервер. Профессиональный** доступен в интернете, вы можете проверить его безопасность с помощью сайта SSL Server Test. Введите доменное имя в поле **Hostname** и нажмите кнопку **Submit**. Дождитесь результатов. Класс защищенности должен быть не ниже, чем **A**.

Как переключить Р7-Офис. Сервер. Профессиональный на протокол HTTPS с помощью собственного сертификата на Linux версии?

Введение

В большинстве случаев доступ к порталу по протоколу HTTPS намного безопаснее, чем по протоколу HTTP, который используется по умолчанию. Но для изменения способа доступа к порталу необходимо выполнить определенные действия. Прочитайте следующие инструкции, чтобы узнать, как переключить **Р7-Офис. Сервер. Профессиональный** на протокол HTTPS.

Создание сертификата безопасности и закрытого ключа

Прежде чем начинать переключение **Сервера совместной работы** на протокол HTTPS, необходимо создать сертификат безопасности и закрытый ключ сертификата.

Для автоматической генерации SSL-сертификата с помощью сервиса letsencrypt вы можете обратиться к этой статье.

Когда у вас будет сертификат, переходите к последующим действиям.

Переключение Сервера совместной работы на HTTPS с помощью скрипта

Быстрее всего можно переключить **Сервер совместной работы** на протокол HTTPS с помощью готового скрипта. Он находится здесь:

```
/var/www/r7-office/Tools/default-r7-office-ssl.sh
```

Поместите созданные сертификаты в папку /var/www/r7-office/Data/certs/. Там должно быть два файла:

- /var/www/r7-office/Data/certs/r7-office.crt
- /var/www/r7-office/Data/certs/r7-office.key

Примечание: имена сертификатов обязательно должны быть r7-office.crt и r7-office.key

И запустите скрипт:

```
sudo bash /var/www/r7-office/Tools/default-r7-office-ssl.sh
```

Он выполнит все необходимые действия для переключения инсталляции **Р7-Офис. Сервер. Профессиональный** на HTTPS.

Переключение Р7-Офис. Сервер. Профессиональный на HTTPS вручную

Все действия, которые выполняет скрипт, вы можете выполнить вручную. Для этого сделайте следующее:

1. Остановите сервис NGINX:

```
sudo service nginx stop
```

2. Скопируйте файл **r7-office-communityserver-common-ssl.conf.template** (находится по пути /etc/nginx/includes/r7-office-communityserver-common-ssl.conf.template) в файл **r7-office** (находится по пути /etc/nginx/sites-available/r7-office) с помощью следующей команды:

```
sudo cp -f /etc/nginx/includes/r7-office-communityserver-common-ssl.conf.template /etc/nginx/sites-available/r7-office
```

Для CentOS файл **r7-office-communityserver-common-ssl.conf.template** /etc/nginx/includes/r7-office-communityserver-common-ssl.conf.template необходимо скопировать в файл **r7-office.conf** (находится по пути /etc/nginx/conf.d/r7-office.conf). Для этого выполните следующую команду:

```
sudo cp -f /etc/nginx/includes/r7-office-communityserver-common-ssl.conf.template /etc/nginx/conf.d/r7-office.conf
```

3. Отредактируйте файл **r7-office** (находится по пути /etc/nginx/sites-available/r7-office), заменив все параметры в двойных фигурных скобках **{{...}}** на фактически используемые:
   - **{{SSL_CERTIFICATE_PATH}}** — путь к вашему сертификату SSL;
   - **{{SSL_KEY_PATH}}** — путь к закрытому ключу сертификата SSL;
   - **{{SSL_VERIFY_CLIENT}}** — параметр, определяющий, включена ли проверка клиентских сертификатов (допустимые значения: on, off, optional и optional_no_ca);

- **{{CA_CERTIFICATES_PATH}}** — путь к клиентскому сертификату, который будет проверяться, если проверка включена в предыдущем параметре;
- **{{R7-OFFICE_HTTPS_HSTS_MAXAGE}}** — дополнительный параметр настройки для задания параметра max-age HSTS в конфигурации виртуального хоста NGINX для **Сервера совместной работы**, применяется только в тех случаях, когда используется SSL (как правило, по умолчанию задается значение 31536000, что считается достаточно безопасным);
- **{{SSL_DHPARAM_PATH}}** — путь к параметру Диффи-Хеллмана;
- **{{R7-OFFICE_NGINX_KEEPLIVE}}** — максимальное число неактивных постоянных соединений с серверами группы, которые будут сохраняться в кэше каждого рабочего процесса (для получения дополнительной информации об этом параметре обратитесь к документации NGINX);
- **{{SSL_OCSP_CERTIFICATE_PATH}}** — путь к файлу с доверенными сертификатами CA в формате PEM, которые используются для проверки клиентских сертификатов и ответов OCSP (Online Certificate Status Protocol), если включён ssl_stapling.

Обратитесь к документации NGINX для получения дополнительной информации о параметрах SSL, которые используются в файле конфигурации.

4. Откройте файл конфигурации /var/www/r7-office/Services/MailAggregator/ASC.Mail.Aggregator.CollectionService.exe.config и задайте для параметра mail.default-api-scheme значение https. После этого перезапустите сервис почтового агрегатора:

```
sudo service restart r7-officeMailAggregator
```

5. Переключите **Чат** на протокол TLS. Обратитесь к этой статье, чтобы узнать, как это сделать.
6. Когда все изменения будут внесены, можно снова запустить сервис NGINX:

```
sudo service nginx start
```

Примечание: Для правильной работы портала должен быть открыт порт 443.

Примечание: При работе с самоподписанными сертификатами или сертификатами у которых невозможно проверить подлинность, необходимо отключить проверку.
Для этого необходимо скорректировать файл /etc/r7-office/documentserver/**default.json**
В строке **«rejectUnauthorized»:** поменять значение на **false** .
Для применения изменений, необходимо перезапустить сервисы Сервера Документов:
supervisorctl restart all

Мы рекомендуем, перед перезапуском сервисов, выполнить запуск скрипта bash /usr/bin/documentserver-prepare4shutdown.sh , который завершит все сессии редактирования документов, соберет их версии и поместит документы в хранилище, что позволит избежать потери информации.

Настройка Shibboleth v2.x — 3.x IdP и Р7-Офис SP

Введение

Вы можете настроить Shibboleth 2.x — 3.x в качестве поставщика учетных записей (IDP) для корпоративных учетных записей в Р7-Офис. Процесс настройки состоит из двух основных шагов: регистрации вашего поставщика учетных записей в разделе **SSO Панели управления** Р7-Офис и регистрации Р7-Офис SP в поставщике учетных записей **Shibboleth**.

Р7-Офис SP поддерживает поток атрибутов givenName, sn, title, locality, mobile и mail корпоративной учетной записи от корпоративного поставщика учетных записей. Когда пользователь осуществляет вход с использованием корпоративной учетной записи, и Р7-Офис SP получает атрибуты с именами givenName, sn и mail (обязательные атрибуты), Р7-Офис SP заполняет полное имя и адрес электронной почты для учетной записи пользователя значениями, полученными от поставщика учетных записей.

Регистрация Shibboleth в качестве корпоративного поставщика учетных записей в Р7-Офис SP

1. Убедитесь, что вы зашли в качестве администратора вашей организации в **Панель управления** Р7-Офис, и щелкните вкладку **SSO**.

Примечание: Вы можете зарегистрировать только одного корпоративного поставщика учетных записей для вашей организации на портале Р7-Офис.

2. Включите SSO, используя переключатель **Включить аутентификацию с помощью технологии единого входа**.
3. Введите метаданные для поставщика учетных записей, используя один из трех приведенных ниже вариантов:
   - **По ссылке (Загрузить данные)** – если метаданные Shibboleth IdP доступны извне по ссылке (например, https://{shibboleth-idp-domain}/idp/shibboleth), вставьте ссылку в поле **URL-адрес XML-файла метаданных IdP** и нажмите

кнопку со стрелкой вверх. После этого все настройки отобразятся в расширенной форме.

- **Файл (ВЫБРАТЬ ФАЙЛ)** – по умолчанию Shibboleth предоставляет файл метаданных IdP в SHIBBOLETH_HOME/metadata. Если файл метаданных доступен, загрузите его, используя кнопку **ВЫБРАТЬ ФАЙЛ** и указав файл SHIBBOLETH_HOME/metadata/idp-metadata.xml с локальной машины. После этого все настройки отобразятся в расширенной форме.
- **Параметры** – если файл с метаданными недоступен, вручную введите значения и укажите запрашиваемые параметры: **Идентификатор сущности поставщика учетных записей**, **URL-адрес конечной точки единого входа IdP**, **URL-адрес конечной точки единого выхода IdP**, сертификаты для подписи и прочее. Для получения этих значений обратитесь к администратору Shibboleth.

5. В поле **Пользовательская надпись для кнопки входа** вы можете ввести любой текст вместо стандартного «*Single Sign-on*«. Этот текст будет отображаться на кнопке для входа с помощью сервиса Single Sign-on на странице аутентификации портала Р7-Офис.
6. Если ваш Shibboleth IdP требует, чтобы входящие данные были подписаны и/или зашифрованы, то необходимо создать/добавить сертификаты для этого в разделе **Сертификаты поставщика сервиса**. В расширенных настройках также можно указать, какие запросы стоит подписывать, нужно ли расшифровывать данные, выбрать соответствующие алгоритмы подписи и расшифровки.
7. В разделе **Сопоставление атрибутов** укажите соответствие полей модуля «Люди» Р7-Офис атрибутам пользователя, которые будут возвращаться из Shibboleth IdP.
8. Нажмите кнопку **СОХРАНИТЬ**.
9. Должен открыться раздел **Метаданные поставщика сервиса Р7-Офис**.

10. Проверьте, что настройки доступны публично, кликнув по кнопке **СКАЧАТЬ XML-ФАЙЛ МЕТАДАННЫХ ПОСТАВЩИКА СЕРВИСА**. Должно отобразиться содержимое XML-файла.

Регистрация Р7-Офис в качестве проверенного поставщика сервиса в Shibboleth IdP

1. Настройте Р7-Офис SP в качестве проверяющей стороны в Shibboleth.
   A. Получите файл метаданных вашего портала Р7-Офис и сохраните его как XML-файл. Для получения файла метаданных войдите в **Панель управления** Р7-Офис в качестве администратора и щелкните вкладку **SSO**. Нажмите на кнопку **СКАЧАТЬ XML-ФАЙЛ МЕТАДАННЫХ ПОСТАВЩИКА СЕРВИСА** и сохраните данные как файл **sp-R7-OFFICE.xml**.

B. Добавьте Р7-Офис в качестве проверенного поставщика сервисов в Shibboleth посредством задания нового элемента MetadataProvider в файле SHIBBOLETH_HOME/conf/metadata-providers.xml. Для этого добавьте приведенный ниже фрагмент кода в корневой элемент MetadataProvider. Предоставьте путь к XML-файлу метаданных вашей организации (сохраненному на предыдущем шаге **a**):

C. <MetadataProvider id="R7-OFFICESP" xsi:type="FilesystemMetadataProvider" metadataFile="<PATH_TO_THE_SAVED_METADATA>/metadata/sp-R7-OFFICE.xml"/>

2. Настройте атрибуты пользователя, которые будут возвращаться из Shibboleth IdP.
   A. Отредактируйте файл SHIBBOLETH_HOME/conf/attribute-resolver.xml. Закомментируйте или удалите все существующие определения атрибутов и коннекторов данных.
   B. Добавьте следующую запись атрибутов в раздел resolver:AttributeResolver.

```
<resolver:AttributeResolver
xmlns:resolver="urn:mace:shibboleth:2.0:resolver"
xmlns:pc="urn:mace:shibboleth:2.0:resolver:pc"
xmlns:ad="urn:mace:shibboleth:2.0:resolver:ad"
xmlns:dc="urn:mace:shibboleth:2.0:resolver:dc"
xmlns:enc="urn:mace:shibboleth:2.0:attribute:encoder"
xmlns:sec="urn:mace:shibboleth:2.0:security"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="urn:mace:shibboleth:2.0:resolver
http://shibboleth.net/schema/idp/shibboleth-attribute-resolver.xsd
urn:mace:shibboleth:2.0:resolver:pc http://shibboleth.net/schema/idp/shibboleth-attribute-resolver-pc.xsd
urn:mace:shibboleth:2.0:resolver:ad http://shibboleth.net/schema/idp/shibboleth-attribute-resolver-ad.xsd
urn:mace:shibboleth:2.0:resolver:dc http://shibboleth.net/schema/idp/shibboleth-attribute-resolver-dc.xsd
urn:mace:shibboleth:2.0:attribute:encoder
http://shibboleth.net/schema/idp/shibboleth-attribute-encoder.xsd
urn:mace:shibboleth:2.0:security http://shibboleth.net/schema/idp/shibboleth-security.xsd">
<!-- ========================================== -->
<!--   Attribute Definitions -->
<!-- ========================================== -->
<!-- Schema: Core schema attributes-->
<resolver:Dependency ref="myLDAP" />
<resolver:AttributeEncoder xsi:type="enc:SAML1String"
name="urn:mace:dir:attribute-def:mail" encodeType="false" />
```

```
<resolver:AttributeEncoder xsi:type="enc:SAML2String"
name="urn:oid:0.9.2342.19200300.100.1.3" friendlyName="mail"
encodeType="false" />
</resolver:AttributeDefinition>
<resolver:AttributeDefinition xsi:type="ad:Simple" id="mobileNumber"
sourceAttributeID="mobile">
<resolver:Dependency ref="myLDAP" />
<resolver:AttributeEncoder xsi:type="enc:SAML1String"
name="urn:mace:dir:attribute-def:mobile" encodeType="false" />
<resolver:AttributeEncoder xsi:type="enc:SAML2String"
name="urn:oid:0.9.2342.19200300.100.1.41" friendlyName="mobile"
encodeType="false" />
</resolver:AttributeDefinition>
<resolver:AttributeDefinition xsi:type="ad:Simple" id="surname"
sourceAttributeID="sn">
<resolver:Dependency ref="myLDAP" />
<resolver:AttributeEncoder xsi:type="enc:SAML1String"
name="urn:mace:dir:attribute-def:sn" encodeType="false" />
<resolver:AttributeEncoder xsi:type="enc:SAML2String" name="urn:oid:2.5.4.4"
friendlyName="sn" encodeType="false" />
</resolver:AttributeDefinition>
<resolver:AttributeDefinition xsi:type="ad:Simple" id="locality"
sourceAttributeID="l">
<resolver:Dependency ref="myLDAP" />
<resolver:AttributeEncoder xsi:type="enc:SAML1String"
name="urn:mace:dir:attribute-def:l" encodeType="false" />
<resolver:AttributeEncoder xsi:type="enc:SAML2String" name="urn:oid:2.5.4.7"
friendlyName="l" encodeType="false" />
</resolver:AttributeDefinition>
<resolver:AttributeDefinition xsi:type="ad:Simple" id="title"
sourceAttributeID="title">
<resolver:Dependency ref="myLDAP" />
<resolver:AttributeEncoder xsi:type="enc:SAML1String"
name="urn:mace:dir:attribute-def:title" encodeType="false" />
<resolver:AttributeEncoder xsi:type="enc:SAML2String" name="urn:oid:2.5.4.12"
friendlyName="title" encodeType="false" />
</resolver:AttributeDefinition>
<resolver:AttributeDefinition xsi:type="ad:Simple" id="givenName"
sourceAttributeID="givenName">
<resolver:Dependency ref="myLDAP" />
<resolver:AttributeEncoder xsi:type="enc:SAML1String"
name="urn:mace:dir:attribute-def:givenName" encodeType="false" />
```

```
<resolver:AttributeEncoder xsi:type="enc:SAML2String" name="urn:oid:2.5.4.42"
friendlyName="givenName" encodeType="false" />
</resolver:AttributeDefinition>
</resolver:AttributeResolver>
```

C. Настройте атрибуты для включения в поставщик сервиса. Отредактируйте файл SHIBBOLETH_HOME/conf/attribute-filter.xml и добавьте следующее:

```
<AttributeFilterPolicyGroup id="ShibbolethFilterPolicy"
xmlns="urn:mace:shibboleth:2.0:afp"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="urn:mace:shibboleth:2.0:afp
http://shibboleth.net/schema/idp/shibboleth-afp.xsd">
<!-- Release some attributes to an SP. -->
<AttributeFilterPolicy id="R7-OFFICESP">
<PolicyRequirementRule xsi:type="OR">
<Rule xsi:type="Requester" value="https://{portal-domain}/sso/metadata" />
</PolicyRequirementRule>
<AttributeRule attributeID="mail">
<PermitValueRule xsi:type="ANY" />
</AttributeRule>
<AttributeRule attributeID="surname">
<PermitValueRule xsi:type="ANY" />
</AttributeRule>
<AttributeRule attributeID="givenName">
<PermitValueRule xsi:type="ANY" />
</AttributeRule>
<AttributeRule attributeID="mobileNumber">
<PermitValueRule xsi:type="ANY" />
</AttributeRule>
<AttributeRule attributeID="title">
<PermitValueRule xsi:type="ANY" />
</AttributeRule>
<AttributeRule attributeID="locality">
<PermitValueRule xsi:type="ANY" />
</AttributeRule>
</AttributeFilterPolicy>
</AttributeFilterPolicyGroup>
```

Замените {portal-domain} на доменное имя вашего портала.

3. Отредактируйте файл SHIBBOLETH_HOME/conf/relying-party.xml.

A. Скопируйте приведенный ниже XML-код и вставьте его в элементы shibboleth.RelyingPartyOverrides, чтобы перезаписать настройки по умолчанию для Shibboleth IdP:

```
<util:list id="shibboleth.RelyingPartyOverrides">
<bean parent="RelyingPartyByName" c:relyingPartyIds="https://{portal-domain}/sso/metadata">
<property name="profileConfigurations">
<list>
  <bean parent="Shibboleth.SSO" p:postAuthenticationFlows="attribute-release" />
   <bean parent="SAML2.SSO" p:encryptAssertions="true" p:postAuthenticationFlows="attribute-release" />
   <bean parent="SAML2.Logout" />
</list>
 </property>
</bean>
```

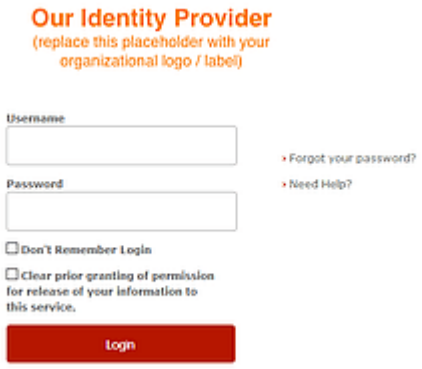
Примечание: Замените {portal-domain} на доменное имя вашего портала.

4. Перезапустите программный агент (Linux) или службу (Windows) Shibboleth.

Проверка работы Р7-Офис SP и Shibboleth IdP

Вход в Р7-Офис на стороне SP

1. Перейдите на страницу аутентификации Р7-Офис (например, https://myportal-address.com/auth.aspx).
2. Нажмите на кнопку **Single sign-on** (название кнопки может отличаться, если вы указали свой вариант при настройке Р7-Офис SP). Если этой кнопки нет, то SSO не включен.
3. Если всё настроено верно в SP и IdP, мы будем перенаправлены на форму логина в Shibboleth IdP:



4. Введите логин и пароль учетной записи в Shibboleth IdP и поставьте галочку Don't Remember Login.
5. Если учетные данные указаны правильно, откроется новое окно. Разрешите передачу данных, нажав на кнопку Accept.
6. Если всё пройдёт хорошо, мы будем перенаправлены на главную страницу портала (если такого пользователя нет на портале, он будет создан автоматически, а если данные были изменены в IdP, они будут обновлены).

Профили пользователей, добавленных с помощью SSO-аутентификации

Возможность редактирования профилей пользователей, созданных с помощью SSO-аутентификации, ограничена. Поля профиля пользователя, полученные из IdP, заблокированы для редактирования (а именно: Имя, Фамилия, Email, Позиция и Местоположение). Эти поля можно отредактировать только из вашей учетной записи в IdP.

Пользователи, созданные с помощью SSO-аутентификации, отмечены в списке пользователей значком SSO для администраторов портала.

Чтобы выйти из Shibboleth IdP (если не была поставлена галочка **Don't Remember Login** при логине), нужно перейти по ссылке следующего вида: https://{shibboleth-idp-domain}/idp/profile/Logout

Как развернуть несколько порталов с помощью функции мультитенантности?

Если у вас много пользователей, вам может потребоваться решение, позволяющее снизить затраты на приобретение лицензий и на инфраструктуру, а также упростить развертывание и эксплуатацию программного обеспечения. Серверная версия **Р7-Офис. Сервер. Профессиональный** предоставляет такую возможность. Вы можете запустить несколько отдельных порталов из одной инсталляции **Р7-Офис. Сервер. Профессиональный** вместо того, чтобы устанавливать несколько экземпляров приложения на отдельных серверах.

Например, вы можете создать отдельные порталы для некоторых отделов вашей организации, чтобы каждый портал содержал собственные данные и у него были индивидуальные настройки, но при этом можно было централизованно обновлять все порталы и управлять ими через **Панель управления**.

Шаг 1. Настройка домена

Чтобы использовать функцию мультитенантности, у вас должно быть зарегистрированное доменное имя. Создайте следующие записи в настройках DNS вашего домена:

1. Создайте **запись A**, связывающую доменное имя с IP-адресом сервера, на котором установлена серверная версия **Р7-Офис**.
2. Создайте **запись A** с подстановочным знаком, указав в качестве имени звездочку «*», чтобы обеспечить возможность использования поддоменов.

Шаг 2. Настройка текущего портала

Чтобы открыть **Панель управления**, войдите на портал и нажмите на ссылку 'Панель управления' на **Стартовой странице**. Можно также перейти в 'Настройки' портала и нажать на ссылку 'Панель управления' на левой боковой панели.

В **Панели управления** перейдите на вкладку **Мультитенантность**. Укажите доменное имя в первом поле ввода. Затем введите во втором поле любое имя портала, которое вам нужно (оно должно содержать не менее 6 символов), и нажмите кнопку **ПОДКЛЮЧИТЬ**.

Стартовая страница портала откроется в новой вкладке браузера по адресу portalname.domainname.com

Примечание: Если в дальнейшем вы захотите переименовать портал, это можно будет сделать в настройках портала: **Настройки**->**Общие**->**Кастомизация**. Перейдите в раздел **Изменение имени портала** , укажите новое имя портала в соответствующем поле и нажмите кнопку **Сохранить**.

Шаг 3. Создание нового портала

На вкладке **Мультитенантность** в **Панели управления** нажмите кнопку **НОВЫЙ ПОРТАЛ** и укажите имя для второго портала, затем нажмите кнопку **ОК**, чтобы сохранить его. Если вы не сняли галочку с опции **Зайти на этот портал после создания**, включенной по умолчанию, вы будете перенаправлены на новый портал, доступный по адресу newportalname.domainname.com.

В новой вкладке браузера откроется страница первоначальной настройки портала. Задайте и подтвердите пароль и в случае необходимости измените адрес электронной почты для создания учетной записи **Администратора**. Вам не потребуется загружать файл лицензии, так как она применяется ко всем порталам сразу.

Чтобы задать для нового портала некоторые индивидуальные настройки, перейдите в **Настройки портала**. Вы можете изменить настройки из раздела **Персонализация** (язык и часовой пояс портала, настройки страницы приветствия, шаблон команды, цветовую схему), выбрать нужные **Модули и инструменты** для использования, задать настройки **Безопасности** и параметры **SMTP**.

Шаг 4. Управление порталами

Вы можете переходить в **Панель управления** с любого из созданных порталов. На вкладке **Мультитенантность** можно посмотреть общее количество созданных порталов и сведения о лицензии. Если вы захотите перейти на тарифный план с более широкими возможностями, нажмите на ссылку **Параметры тарифного плана**, чтобы перейти на страницу **Платежи**.

На вкладке **Мультитенантность** также отображены адреса всех созданных порталов. Вы можете переходить на них, нажав на адрес нужного портала.

Внимание: Настоятельно не рекомендуется изменять доменное имя при наличии данных на портале, поскольку это может привести к непредсказуемым последствиям.

Если по каким-то причинам вы все же решите изменить доменное имя, нажмите кнопку **ИЗМЕНИТЬ** в разделе **Параметры домена**. В открывшемся окне задайте новое доменное имя и нажмите кнопку **ОК**.

Удаление портала

Для удаления необходимо перейти в нужный портал, далее выбрать **Настройки портала** => **Безопасность** => **Удаление портала.**

После изменения доменного имени вам может также потребоваться повторно настроить некоторые параметры. Например, если вы подключали Jabber-клиенты, в настройках клиента понадобится указать новое доменное имя.

Модуль люди

Добавление новых участников портала

Как владелец портала или администратор с полным доступом, вы можете добавлять на портал новых участников.

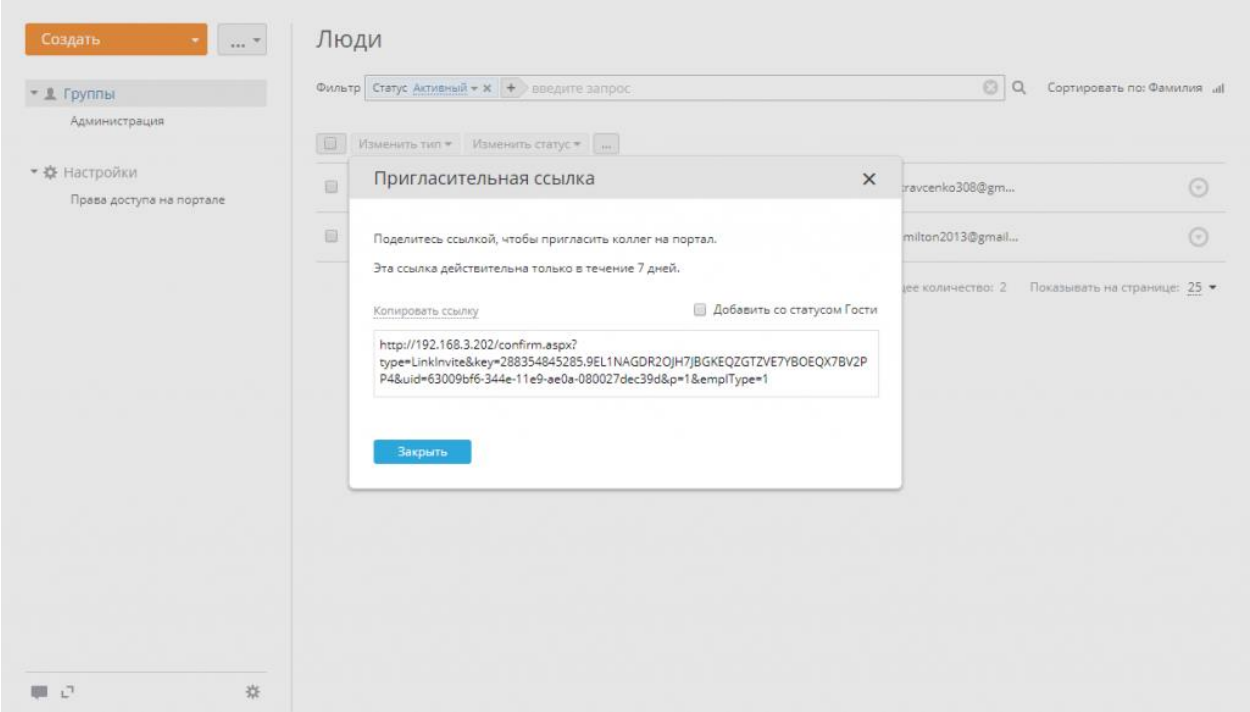
Использование пригласительной ссылки

Если вы только что создали портал и еще не добавили пользователей, в каждом из модулей портала на левой боковой панели будет доступна кнопка **Пригласить пользователей**. С ее помощью можно быстро и просто пригласить на портал новых участников, чтобы они могли присоединиться к нему:

1. нажмите кнопку **Пригласить пользователей** Пригласительная ссылка будет сразу скопирована в буфер обмена, и откроется окно **Пригласительная ссылка**, в котором можно изменить дополнительные параметры ссылки:
   - установите флажок **Добавить со статусом Гости**, чтобы пригласить на портал людей с правами только на просмотр (если надо, чтобы эти люди могли создавать контент на портале, оставьте этот флажок снятым). После изменения этого параметра не забудьте скопировать обновленную ссылку с помощью опции **Копировать ссылку**.
   - можно также **Получить сокращенную ссылку**, более удобную для вставки в сообщение
2. вставьте скопированную ссылку в пригласительное сообщение и отправьте его или поделитесь ссылкой через социальные сети, используя соответствующие значки в окне **Пригласительная ссылка**

Ссылка действительна только 7 дней.

Примечание: В дальнейшем вы можете нажать кнопку в левом верхнем углу модуля **Люди** и выбрать опцию **Пригласительная ссылка**, чтобы скопировать ссылку и вызвать соответствующее окно.



Управление правами доступа

В онлайн-офисе существует три основных уровня доступа: **гость** с правами только на просмотр, **пользователь** с базовыми привилегиями и **администратор** с дополнительными привилегиями.
Среди администраторов есть:

- **администраторы модуля**, которые управляют отдельным модулем или несколькими из них
- **администраторы с полным доступом**, которые управляют всеми модулями портала
- **владелец портала**, который осуществляет контроль над всем порталом

Обычно владелец портала — это тот, кто создал портал. Если он хочет назначить другого участника портала на эту позицию, ему необходимо:

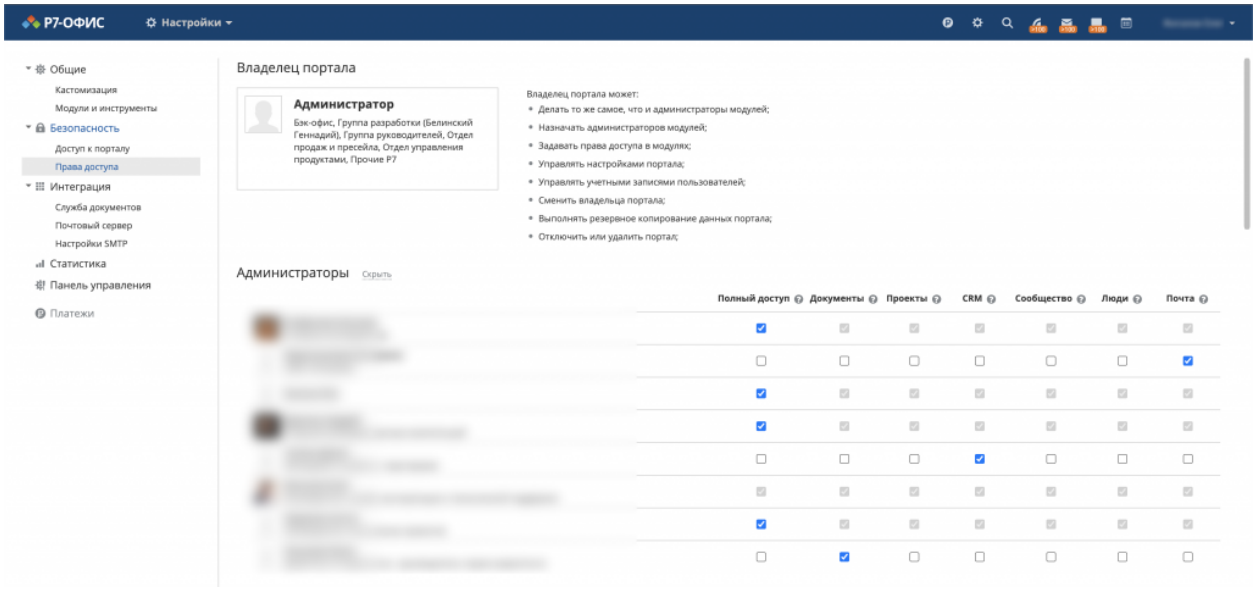
1. переключиться на настройки портала, выбрав в верхнем меню опцию **Настройки**
2. развернуть раздел **Безопасность** на левой боковой панели и выбрать подраздел **Права доступа**
3. из выпадающего списка под своей фотографией выбрать другого человека
4. нажать на кнопку **Сменить владельца портала**
5. проверить почтовый ящик и перейти по ссылке для подтверждения, отправленной в сообщении по электронной почте

Владелец портала обладает такими же правами, как и администратор с полным доступом, и может выполнять следующие операции:

АДМИНИСТРАТОР С ПОЛНЫМ ДОСТУПОМ	ВЛАДЕЛЕЦ ПОРТАЛА
добавление участников портала редактирование профилей участников назначение администраторов модулей изменение настроек портала (см. раздел https://support.r7-office.ru/category/community_server/settings_cs/) резервное копирование данных портала (см. https://support.r7-office.ru/community_server/control_panel/backup/)	+ смена владельца портала

После того как участник портала добавлен на портал, он получает права пользователя или гостя. Администраторы с полным доступом могут предоставить привилегии администратора только пользователям. Для этого надо выполнить следующие шаги:

1. переключиться на настройки портала, выбрав в верхнем меню опцию **Настройки**
2. выбрать опцию **Права доступа** на левой боковой панели
3. нажать на ссылку **Показать** рядом с заголовком **Администраторы**
4. нажать на ссылку **Выбрать пользователя** под списком администраторов
5. выбрать человека или нескольких человек сразу из существующих пользователей/гостей или создать нового администратора прямо здесь, нажав на ссылку **Создать новый профиль**
6. нажмите кнопку **Сохранить**
7. выбранный человек по умолчанию получит максимальный доступ ко всем модулям портала; для ограничения этого доступа снимите флажки, соответствующие тем модулям, к которым вы не хотите предоставлять доступ администратору



Такая структура прав доступа — гость/пользователь/администратор — действительна для следующих модулей портала:

- Документы
- CRM
- Сообщество
- Люди
- Почта

Примечание: У гостей вообще нет доступа к модулю **Почта** и **CRM** и **Люди**. Они могут только просмотреть и отредактировать свой собственный профиль.

Основные права доступа перечислены в таблице ниже.

	ДОКУМЕНТЫ	**CRM**	**СООБЩЕСТВО**	**ЛЮДИ**	**ПОЧТА**
ГОСТЬ	просмотр файлов, доступных всем участникам; скачивание файлов из папки **Общие документы**, а также документов, к которым гостю предоставили доступ; загрузка файлов в папки, к которым гостю предоставили доступ	добавление комментариев к существующим записям, прикрепление файлов к комментариям	редактирование собственного профиля		

ПОЛЬЗОВАТЕЛЬ	создание/редактирование/управление/обмен файлами и папками в разделе **Мои документы**, просмотр файлов в разделе **Общие документы**	создание нового контента и редактирование собственных материалов	редактирование собственного профиля, просмотр профилей других участников	управление своими учетными записями почты, получение и отправка писем	
АДМИНИСТРАТОР МОДУЛЯ	+ создание/редактирование/управление/обмен файлами и папками в разделе **Общие документы**	+ модерация всего контента в модуле	+ добавление/приглашение участников, создание групп и редактирование профилей других участников	+ управление Почтовым сервером (добавление своего домена, создание почтовых ящиков, почтовых групп) и общими настройками почты	

Инструменты онлайн-офиса — Почта, Чат, Календарь, Лента — доступны всем пользователям портала.

Гости могут пользоваться всеми инструментами, кроме Почты.

Переназначение данных и удаление профилей пользователей

Переназначение данных при удалении профилей

Что происходит с данными без переназначения

Если не переназначать данные при удалении заблокированных пользователей, также будут **удалены** принадлежащие пользователю материалы, созданные им на портале, а именно:

- В модуле **Документы** личные документы и папки удаляются, а общие документы, созданные пользователем, переназначаются:

    - Личные документы и папки, недоступные для других пользователей (в том числе и для администраторов), удаляются.
    - Личные документы и папки, к которым был предоставлен доступ для других пользователей, удаляются.
    - Документы и папки, созданные пользователем в разделе **Общие**, не удаляются, но владение ими передается администратору, инициировавшему удаление пользователя.
- В модуле **Почта** удаляются письма и почтовые ящики.
- В **Чате** удаляются сообщения и файлы, отправленные пользователем.
- В модуле **CRM** удаленный пользователь также удаляется из списка менеджеров, ответственных за контакт. Отчеты, созданные пользователем, удаляются (по аналогии с личными документами). Другие сущности CRM, связанные с удаленным пользователем, не затрагиваются.
- В модуле **Проекты** все сущности, связанные с удаленным пользователем, не затрагиваются (например, имя удаленного пользователя остается в числе пользователей, ответственных за открытую задачу).

Чтобы избежать удаления данных, можно переназначить сущности модулей **Документы**, **Проекты** и **CRM** активному пользователю.

В настоящее время, возможность переназначения данных доступна только для пользователей со статусом **Заблокирован**, нельзя переназначить данные, принадлежащие активному пользователю.

Что происходит с данными при переназначении

После переназначения данных и удаления пользователя будут **переданы / сохранены** следующие материалы:

- Модуль **Документы**
    - Личные документы, доступные для других пользователей портала, будут перенесены в раздел **Мои документы** выбранного активного пользователя, где будет создана новая папка с названием типа ‘Документы пользователя Иван Иванов’. Все права доступа, предоставленные другим пользователям портала, будут сохранены;
    - Владение документами, созданными заблокированным пользователем в разделе **Общие**, будет передано выбранному пользователю;
    - Документы из раздела **В проектах**, созданные заблокированным пользователем, остаются, владелец не меняется.
- Модуль **Проекты**
    - Активные и приостановленные проекты, открытые вехи и задачи переназначаются выбранному активному пользователю.
- Модуль **CRM**
    - Контакты, открытые задачи и незакрытые сделки переназначаются выбранному активному пользователю. Указанный пользователь также

добавляется в качестве участника в открытые мероприятия заблокированного пользователя.

После переназначения данных и удаления пользователя будут **удалены** следующие материалы:

- Личные документы, к которым не был предоставлен доступ для других пользователей в модуле **Документы**;
- Письма и почтовые ящики в модуле **Почта**;
- История сообщений и отправленные файлы в **Чате**;
- Закрытые проекты, вехи, задачи в модуле **Проекты**;
- Закрытые задачи и возможные сделки в модуле **CRM**.

Удаление отдельного пользователя

Чтобы удалить отдельного пользователя,

1. Откройте список заблокированных пользователей, выбрав соответствующий статус в фильтре наверху,
2. Нажмите на кнопку **Действия** рядом с заблокированным пользователем,
3. Выберите в меню опцию **Удалить профиль**,
4. Откроется окно подтверждения, где будет предложено переназначить данные пользователя.
5. Нажмите на кнопку **Передать данные** в окне подтверждения.
6. Откроется новая страница, где можно выбрать пользователя портала, которому вы хотите передать данные. Выберите из списка нужного активного пользователя.
7. Опция **Удалить профиль после завершения передачи данных** отмечена по умолчанию, что позволяет автоматически удалить профиль после переназначения данных.
8. Нажмите кнопку **Передать**.
   Теперь можно закрыть эту страницу. После того, как передача данных завершится, вы получите оповещение по электронной почте. Если вы сняли пометку с опции **Удалить профиль после завершения передачи данных**, можно вернуться к списку заблокированных пользователей и вручную удалить пользователя без потери его данных.

Удаление нескольких пользователей

Переназначение данных — это индивидуальное действие, то есть, если вы хотите удалить несколько пользователей одновременно, предварительно потребуется переназначить данные для каждого из них в отдельности.

Чтобы переназначить данные любого заблокированного пользователя,

1. Нажмите на кнопку **Действия** рядом с заблокированным пользователем.
2. Выберите в меню опцию **Передать данные**.
3. Откроется новая страница, где можно выбрать пользователя портала, которому вы хотите передать данные. Выберите из списка нужного активного пользователя.
4. Отметьте опцию **Удалить профиль после завершения передачи данных**, чтобы автоматически удалить профиль после переназначения данных.
5. Нажмите кнопку **Передать**.

После переназначения всех нужных данных (если вы не отметили опцию **Удалить профиль после завершения передачи данных**) можно вернуться к списку заблокированных пользователей, отметить галочками пользователей, которых требуется удалить, и нажать кнопку **Удалить** над списком пользователей, чтобы удалить нескольких пользователей одновременно без потери их данных.

Иерархия разрешений на доступ к папкам в модуле «Документы»

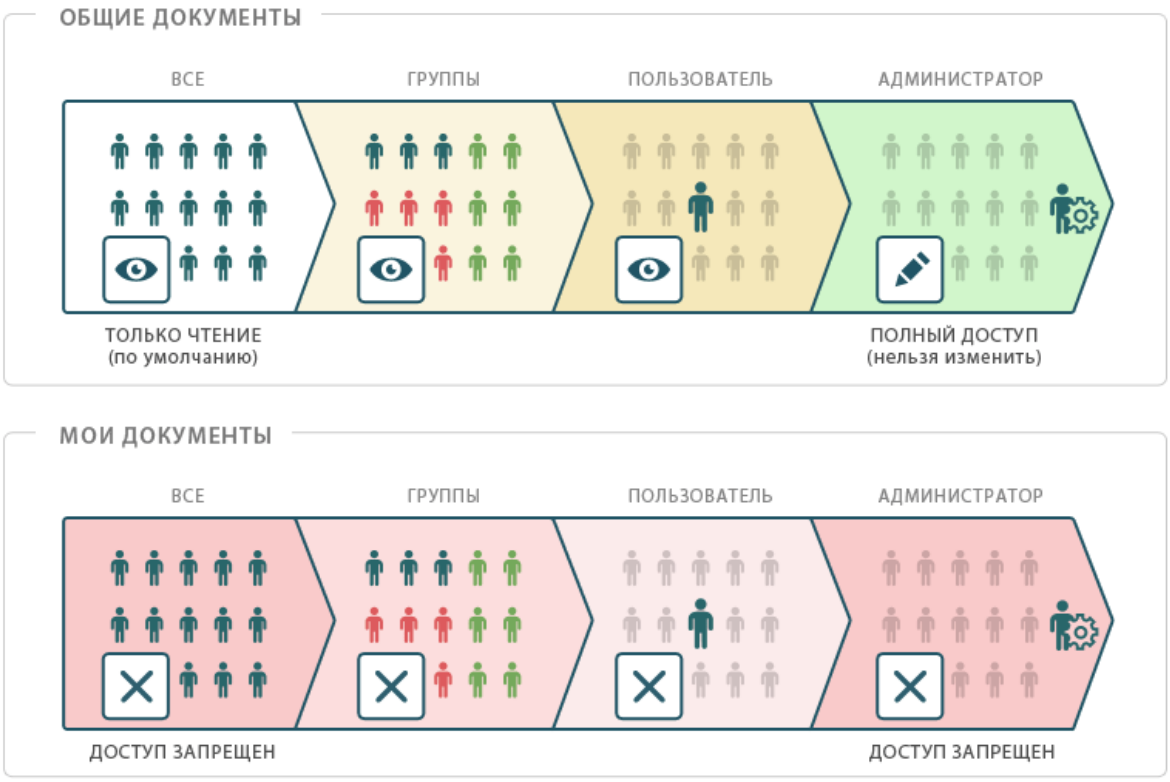
Если вы хотите создать сложную структуру папок с несколькими уровнями вложенности и задать различные разрешения для групп, вам могут пригодиться сведения о том, как реализован порядок приоритетов разрешений в модуле **Документы**.

Основные принципы

В модуле **Документы** существует три уровня приоритетности (перечислены в порядке возрастания значимости):

1. **Иерархия папок**: *родительские папки* и *вложенные папки*
   - Если для вложенной папки не заданы определенные разрешения, вложенная папка наследует разрешения родительской папки.
   - Если для вложенной папки заданы особые разрешения, то разрешения для вложенной папки имеют более высокий приоритет, чем разрешения для родительской папки.
2. **Профиль**: *Все*, *Группы*, *Пользователь*, *Администратор*
   - Разрешения пользователя имеют более высокий приоритет, чем разрешения группы (то есть можно назначить разрешения для конкретного пользователя независимо от того, какие разрешения имеет группа, в которую он входит).
   - Иерархии групп нет, все группы равны (одна группа не может быть приоритетнее другой).

Четыре уровня приоритетности (перечислены в порядке возрастания значимости):



3. **Права доступа**: *Полный доступ*, *Только чтение*, *Доступ запрещен*
    - Права доступа **«Доступ запрещен»** имеют более высокий приоритет, чем права **«Только чтение»**.
    - Права доступа **«Только чтение»** имеют более высокий приоритет, чем права **«Полный доступ»**.
    - Если пользователь состоит в нескольких группах с разными разрешениями на доступ к папке, пользователь получает права с более высоким приоритетом.

Когда пользователь пытается получить доступ к общей папке, проверка разрешений осуществляется в соответствии с порядком приоритетов, приведенным выше:

1. имеет ли текущая папка разрешения, отличные от разрешений родительской папки,
2. какие разрешения на базе профиля заданы для текущей папки,
3. какие права доступа имеет пользователь.

Примеры

ПРИМЕР 1

Следующий пример иллюстрирует сценарий, при котором пользователь состоит в группе, имеющей **Полный доступ** к родительской папке и доступ **«Только чтение»** к вложенной папке, при этом пользователю индивидуально предоставлен **Полный доступ** к вложенной папке.

Следующие примеры иллюстрируют сценарии, при которых пользователь входит в несколько групп с разными разрешениями на доступ к папке.

ПРИМЕР 2

Если первой группе предоставлен **Полный доступ** к папке, а у второй группы доступ к этой же папке **«Только чтение»**, пользователь, который входит в обе эти группы одновременно, получает права доступа с более высоким приоритетом (в данном случае **«Только чтение»**).

Если пользователь входит в группу, у которой нет доступа к папке, и в группу с доступом **«Только чтение»**, права **«Доступ запрещен»** имеют более высокий приоритет, следовательно, у пользователя нет доступа к папке.

Если вы хотите, чтобы у этого пользователя были другие права доступа, надо предоставить ему индивидуальные права доступа.

ПРИМЕР 3

Если папка содержит несколько вложенных папок, разрешениями для вложенных папок можно управлять независимо от разрешений родительской папки.

Если один и тот же пользователь входит в несколько групп с разными правами доступа, его права доступа к каждой из вложенных папок могут различаться в зависимости от заданных разрешений для каждой группы.

Обновление

Обновление сервера Р7-Офис. Профессиональный, для Windows до последней версии

Введение

Программу установки последней версии **Р7-Офис. Сервер. Профессиональный** можно найти на странице загрузок

Для обновления старой версии **Р7-Офис. Сервер. Профессиональный** до последней версии надо скачать и запустить программу установки последней версии для Windows.

Шаг 1. Создайте резервную копию базы данных

Чтобы предотвратить потерю данных, выполните резервное копирование следующих папок:

- C:\Program Files (x86)\R7-OFFICE\CommunityServer\Data\ (или используйте тот путь, по которому установлена предыдущая версия)
- C:\Program Files (x86)\R7-OFFICE\CommunityServer\WebStudio\ (или используйте тот путь, по которому установлена предыдущая версия)

Создайте резервную копию базы данных MySQL с помощью любой программы, которую вы используете для этой цели.

После выполнения резервного копирования всех данных убедитесь, что портал запускается корректно, и запомните какие-нибудь пользовательские данные, чтобы можно было проверить их после обновления.

Шаг 2. Скачайте установочный файл Р7-Офис. Сервер. Профессиональный

Чтобы скачать установочный файл **Р7-Офис. Сервер. Профессиональный**, перейдите на страницу загрузки Р7-Офис. Сервер. Профессиональный, нажмите кнопку **Скачать** в разделе «Windows» и дождитесь окончания загрузки.

Шаг 3. Обновите версию программы

Когда загрузка завершится, можно переходить к установке.

Перед тем, как начать обновление, пожалуйста, закройте все окна браузера на компьютере, используемом для установки серверной версии **Р7-Офис. Сервер. Профессиональный**, чтобы избежать дополнительных ошибок.

Запустите установочный файл последней версии, который вы скачали. Следуйте инструкциям мастера установки.

Когда установка завершится, запустите портал и убедитесь в его корректной работе и наличии данных.

Обновление только Р7-Офис. Профессиональный. Сервер документов.

Шаг 1. Остановка Р7-Офис. Сервер документов

Из-за особенностей работы, Р7-Офис. Сервер документов сохраняет документ только после того, как документ был закрыт всеми пользователями, которые его редактировали. Чтобы избежать потери данных, вы должны принудительно отключить пользователей Р7-Офис. Сервер редактирования, когда вам нужно остановить Р7-Офис. Сервер документов в случае обновления приложения. Для этого запустите следующий .bat-файл:

«C:\Program Files\R7-Office\DocumentServer\bin\documentserver-prepare4shutdown.bat»

Выполнение скрипта может занять много времени (до 5 минут).

Отключение пользователей может занять много времени (до 5 минут).

Шаг 2. Удаление Р7-Офис. Сервер документов

Щелкните правой кнопкой мыши кнопку **«Пуск»** в **Windows**, откройте панель управления и перейдите в раздел **«Программы»** -> **«Программы и компоненты»**.

Найдите в списке Р7-Офис. Сервер документов и удалите его.

Шаг 3. Установка новой версии Р7-Офис. Сервер документов

Загрузите последнюю версию установочного файла Р7-Офис. Сервер документов.

Дважды щелкните на скаченный ранее файл (например r7-office-documentserver-ie-6.0.1.exe), который вы только что скачали, чтобы запустить мастер установки и выполните действия предусмотренные мастером установки.

По завершении процесса установки запустите Р7-Офис. Сервер документов и проверьте его правильность работы.

Обновление серверной версии Р7-Офис. Сервер. Профессиональный с помощью скрипта для ОС Linux

Введение

Скрипт автоматической установки для операционных систем Linux удобно использовать для обновления серверной версии **Р7-Офис. Корпоративный Сервер. Профессиональный**.

Подготовка

Рекомендуем предварительно создать резервную копию сервера, для восстановления работоспособности в случае появления ошибок в ходе обновления средствами используемыми в эксплуатации и иметь актуальную версию резервной копии из Панели управления.

Так же выполните завершение всех сессий редактирования файлов на сервере, используя следующий скрипт:

```
bash /usr/bin/documentserver-prepare4shutdown.sh
```

Данный скрипт принудительно помещает в хранилище все открытые на редактирования файлы и выключит работу сервиса Сервер Документов. Редактирование будет не доступно.

Для включения сервера документов потребуется перезапуск сервера или выполнение команды:

```
supervisorctl start all
```

Обновление компонентов

Чтобы обновить серверную версию, запустите скрипт, указав параметр `-u true`.

ПАРАМЕТР	ОПИСАНИЕ	ЗНАЧЕНИЯ	ПО УМОЛЧАНИЮ
-u, --update	обновить существующие компоненты	true|false	false

Этот параметр позволяет установить последние версии нужных компонентов, если соответствующие компоненты, установленные на вашем сервере, устарели. Вы можете скачать нужный вам скрипт Примеры Для ОС Linux CentOS/RedHat

```
bash install-RedHat.sh -u true
```

Для ОС Astra Linux

```
bash install-AstraLinux.sh -u true
```

Для ОС ALT Linux

```
bash install-ALTLinux.sh -u true
```

В результате будут установлены последние версии соответствующих компонентов **Р7-Офис. Корпоративный сервер. Профессиональный**, которые требуется обновить. Если текущая версия компонента совпадает с последней доступной версией, такой компонент не будет затронут. Данные, сохраненные на портале, должны подхватиться автоматически.

После обновления сервера выполните следующие команды:

Измените значения files.docservice.secret и files.docservice.secret.header в файле web.appsettings.config.
nano /var/www/r7-office/WebStudio/web.appsettings.config
Значения которые необходимо указать в файле web.appsettings.config находятся в файле /etc/r7-office/documentserver/local.json и равны значению параметров «token» — «inbox» — «header» и «secret» — «inbox» — «string»
nano /etc/r7-office/documentserver/local.json
Измените значения в файле web.appsettings.config:
files.docservice.secret на значение из «secret» — «inbox» — «string»
files.docservice.secret.header на значение из «token» — «inbox» — «header»
После изменения файла необходимо перезапустить службу MONO:
systemctl restart monoserve

Если при попытке активации лицензии возникает ошибка «Некорректная лицензия» необходимо изменить владельца папки **Data**:
chown r7-office:r7-office /var/www/r7-office/**Data**

После этого необходимо заменить лицензию через панель «Платежи». В таком случае новая лицензия применится на портале.

Обновление Корпоративного Сервера Docker версии

Пожалуйста, убедитесь, что на сервере, где установлен Корпоративный сервер Р7 Docker, Имеется достаточное для обновления дисковое пространство.

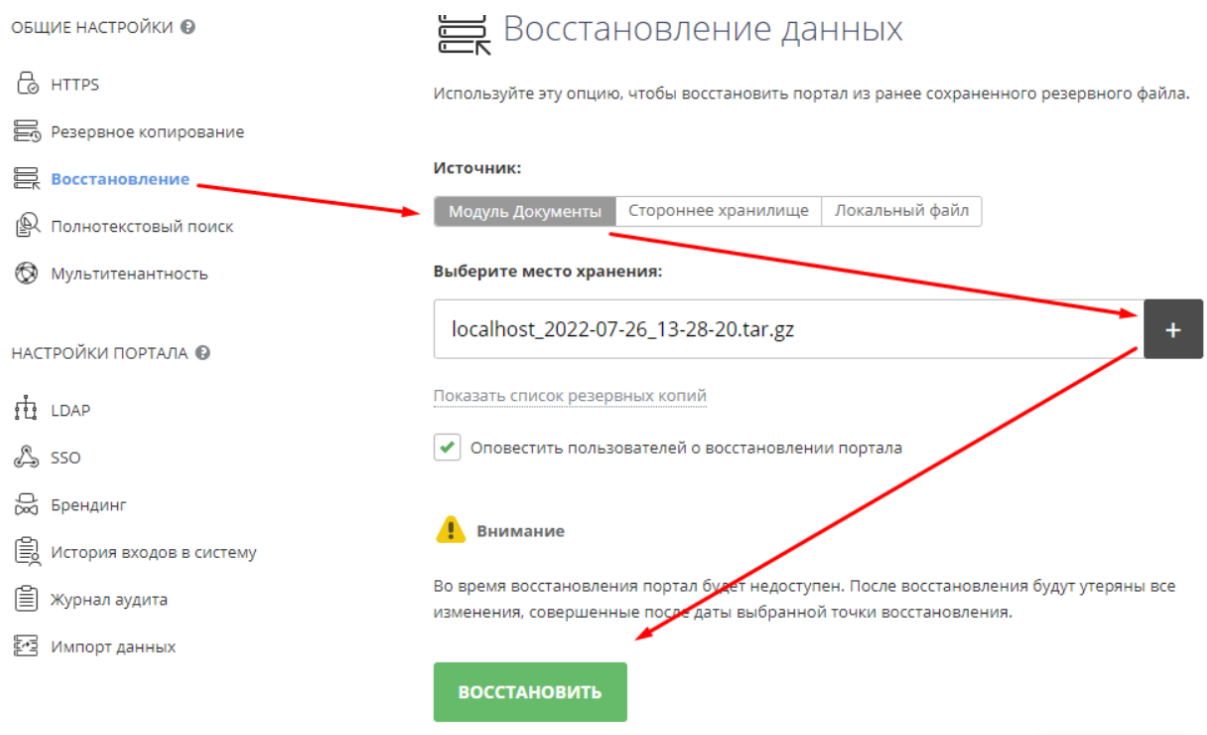
Выполнить сохранение всех не сохраненных документов на сервере

```
docker exec -it $(docker ps -a -q) /usr/bin/documentserver-prepare4shutdown.sh
```

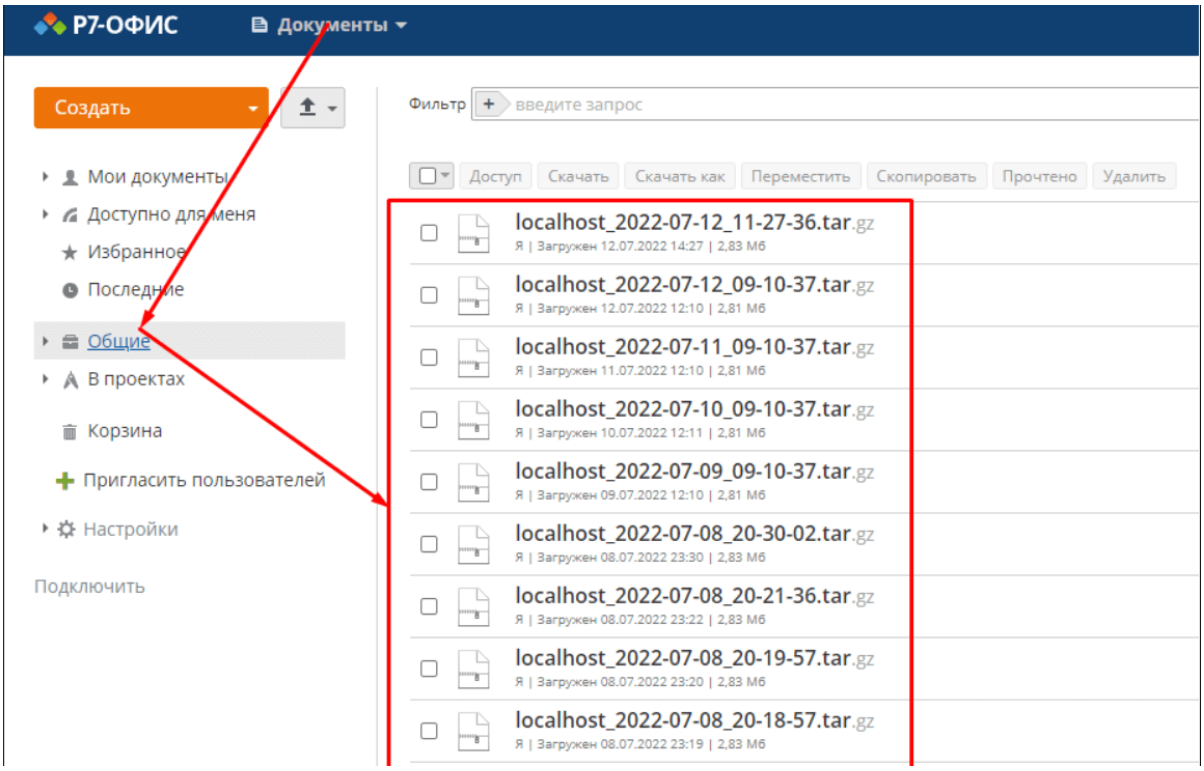
Остановить документ сервер

```
docker exec -it $(docker ps -a -q) supervisorctl stop ds:docservice
```

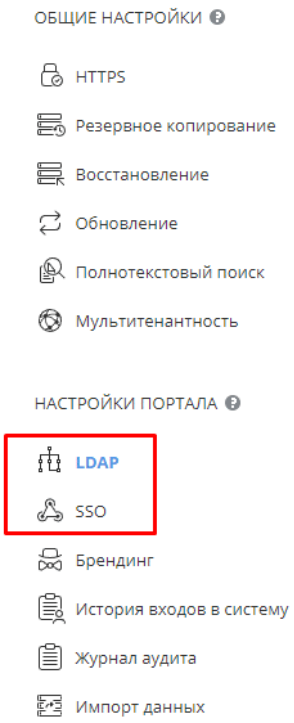
Сделать резервную копию через веб интерфейс:



И сохранить только что сделанную копию на локальном компьютере.



Если вы используете интеграцию с LDAP и (или) SSO, перейдите в соответствующие разделы контрольной панели и запишите текущие настройки, так как настройки не сохранятся в резервной копии.



В консоли, где установлен Р7-офис в докере требуется сделать резервные копии файла лицензии — license.lic, каталога с сертификатом ssl и ключом — certs.

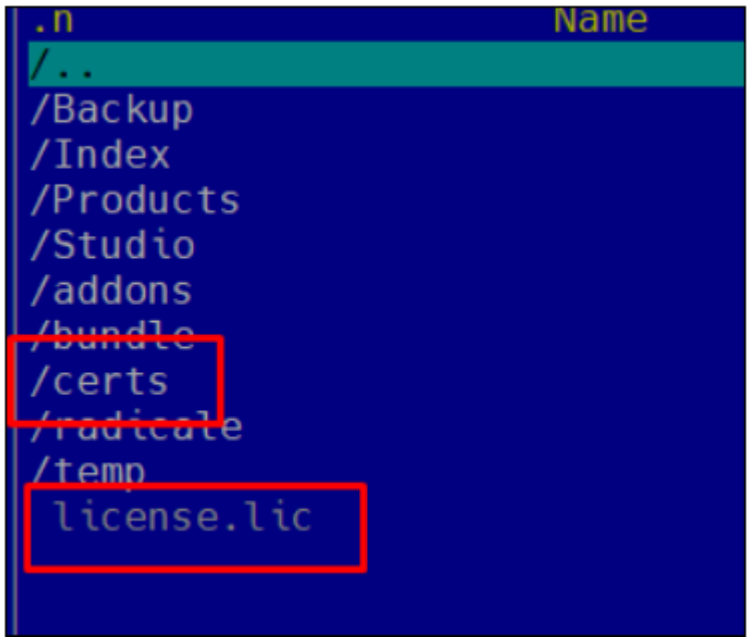
Если позволяет дисковое пространство, рекомендуется сохранить весь каталог с установленным контейнером, для этого требуется:

Остановить контейнер

```
docker stop $(docker ps -a -q)
```

И переименовать каталог, куда установлен корпоративный сервер.

```
/{Каталог_установки}/app/r7-office/www/r7-office/Data
```



Скачать и распаковать архив с новой версией Корпоративного сервера для Docker. Запустить установку:

```
cd /root
wget https://download.r7-office.ru/docker/communityserver/docker_r7-office_cs_v12.0.1158.zip
mkdir /root/newdocker
unzip /root/docker_r7-office_cs_v12.0.1158.zip -d /root/newdocker
cd /root/newdocker
bash install.sh
```

Переместить (скопировать) каталог certs и файл лицензии в каталог Data:

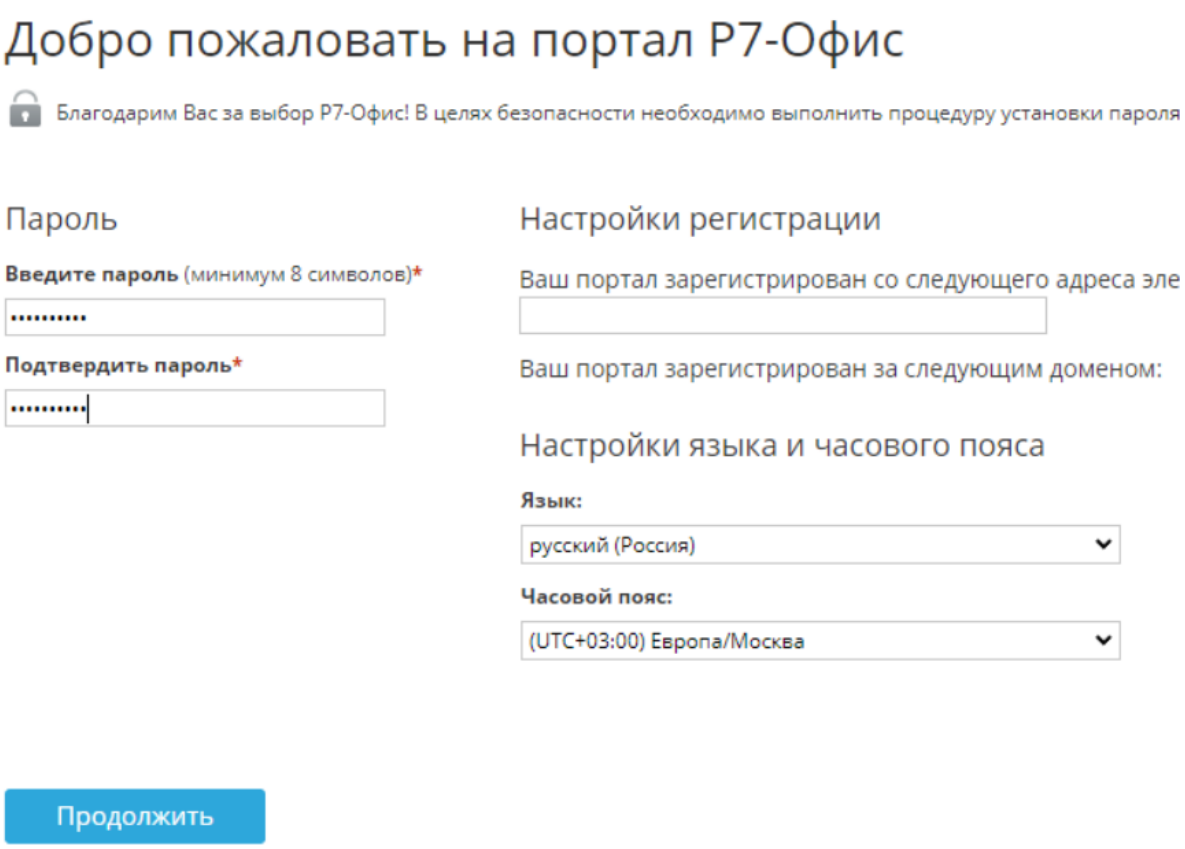
```
/{Каталог_установки}/app/r7-office/www/r7-office/Data
```

Выполнить команду, для перехода на https:

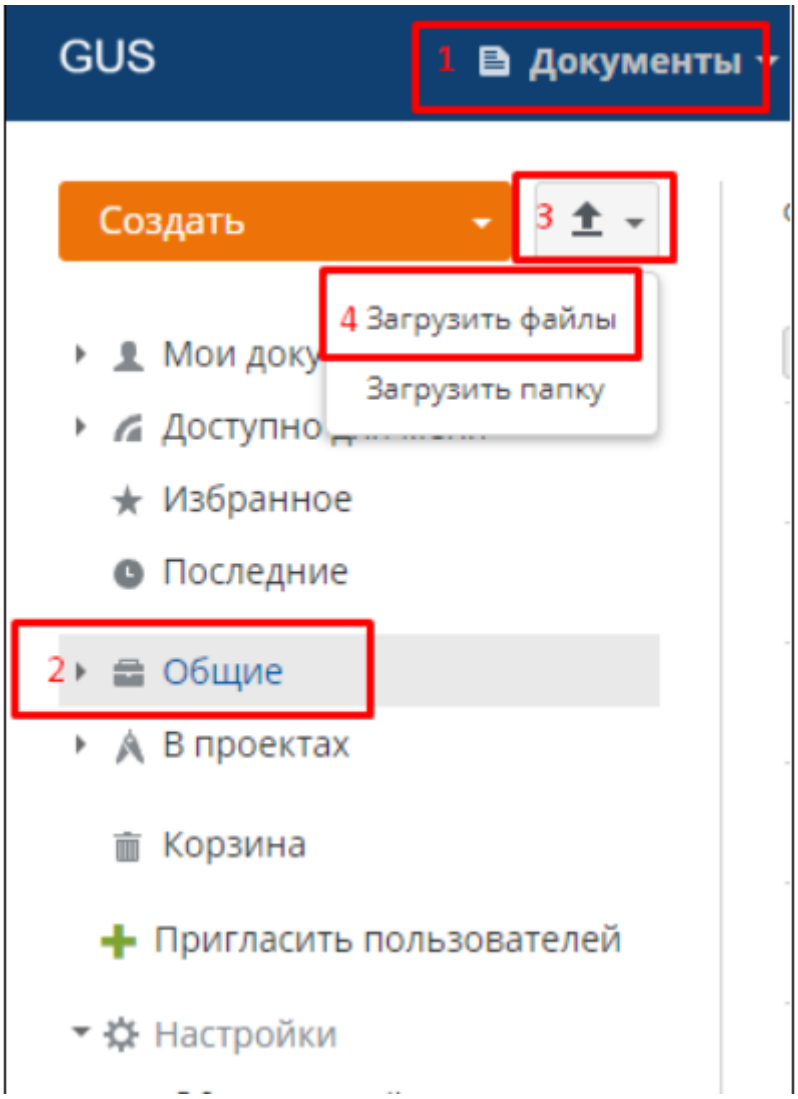
```
docker exec -it $(docker ps -a -q) sudo bash /var/www/r7-office/Tools/default-r7-office-ssl.sh
```

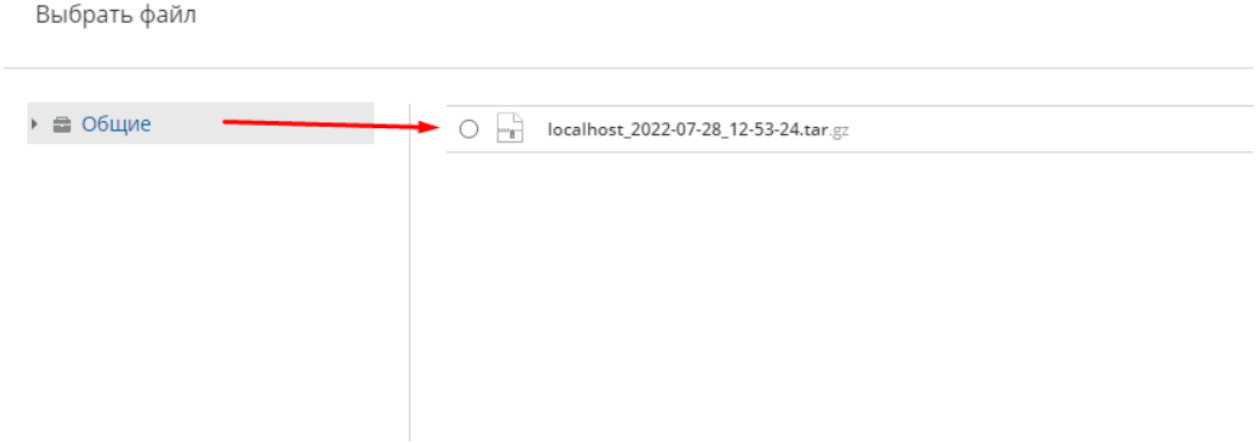
Открываем в браузере портал.

Вводим регистрационный почтовый адрес и дважды пароль.



Загрузить, ранее сохраненный, файл резервной копии в документы (каталог «Общие»)





Если файл резервной копии размером более 100ГБ и его загрузка на сервер завершается с ошибкой, требуется выполнить увеличение квоты на загружаемые файлы:

Подключиться к контейнеру

```
docker exec -it $(docker ps -a -q) bash
```

Подключиться к СУБД

```
mysql -p
```

Введите пароль.

Пароль к базе данных можно найти в файле web.connections.config, который расположен в директории:

```
/{Каталог_установки}/app/r7-office/www/r7-office/WebStudio/
```

Выберите базу данных **r7-office**:

```
use r7-office;
```

Выполните команду, где max_file_size задает максимальный размер файла в мегабайтах:

```
UPDATE tenants_quota SET `max_file_size`=512000 WHERE `tenant`=-1000;
UPDATE tenants_quota SET max_file_size='512000' WHERE tenant='-1';
```

Выполните выход из MySQL

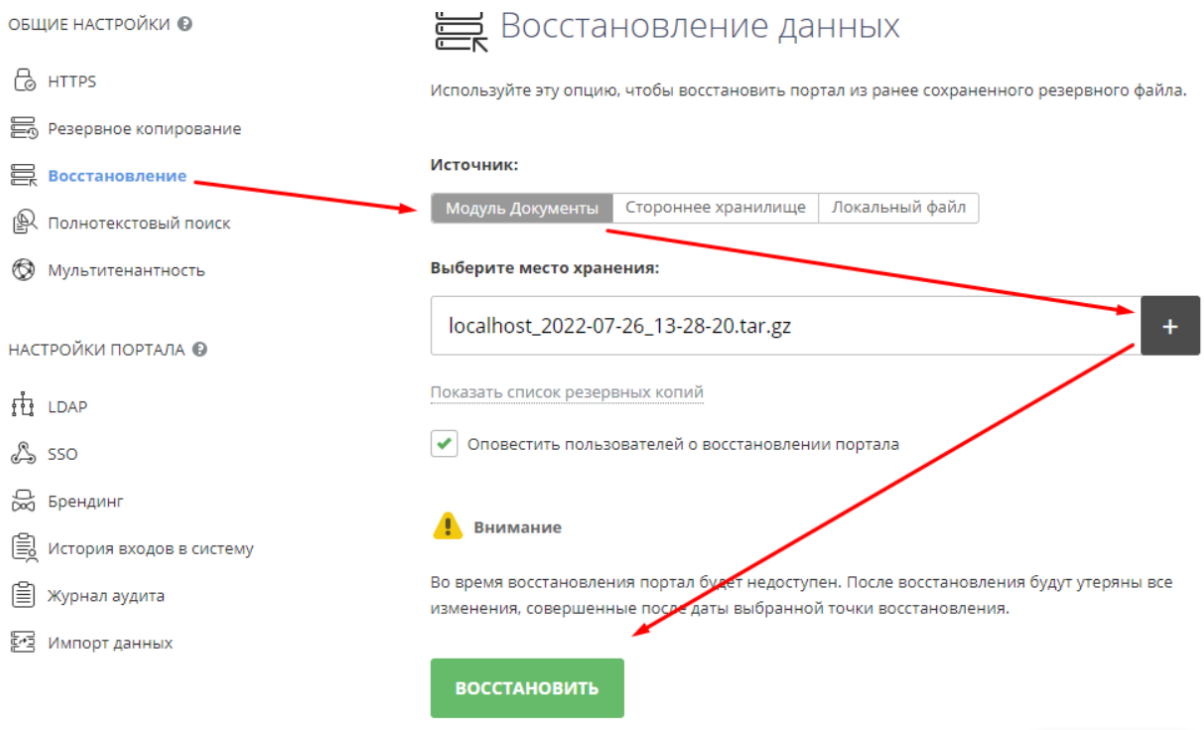
```
exit
```

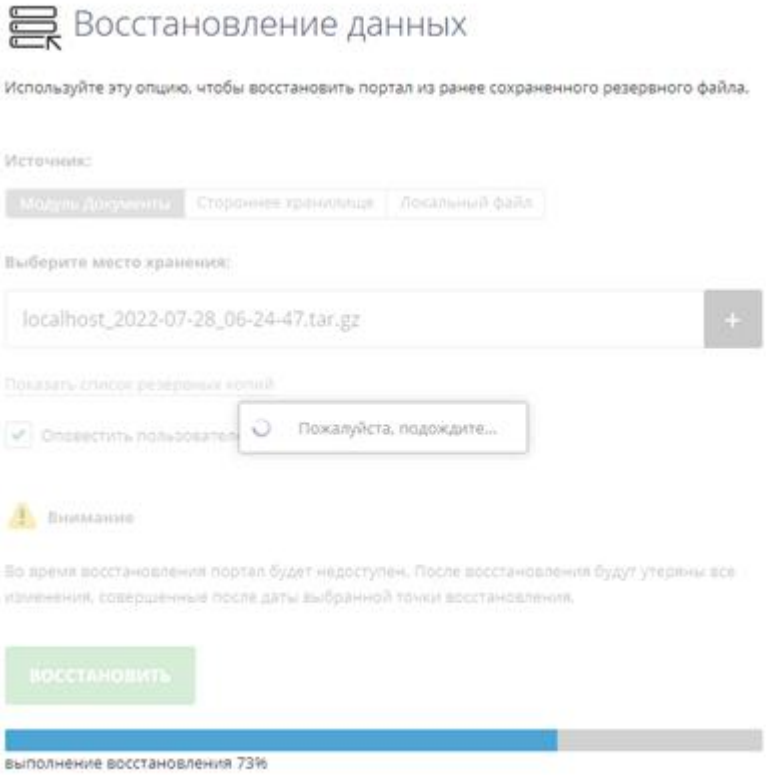
В панели управления, перейти в раздел «Восстановление»

Выбрать источник «Модуль Документы»

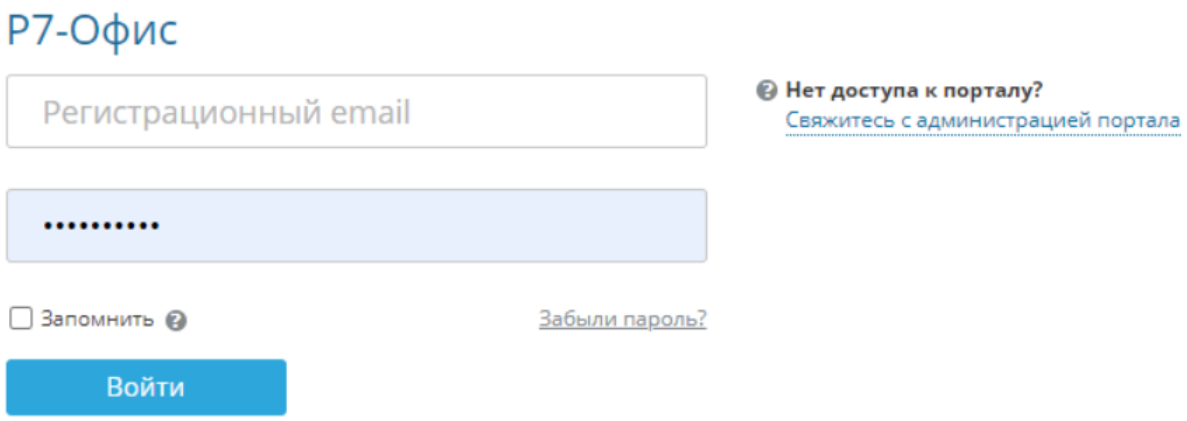
Выбрать, загруженный, файл резервной копии

Нажать кнопку «Восстановить»





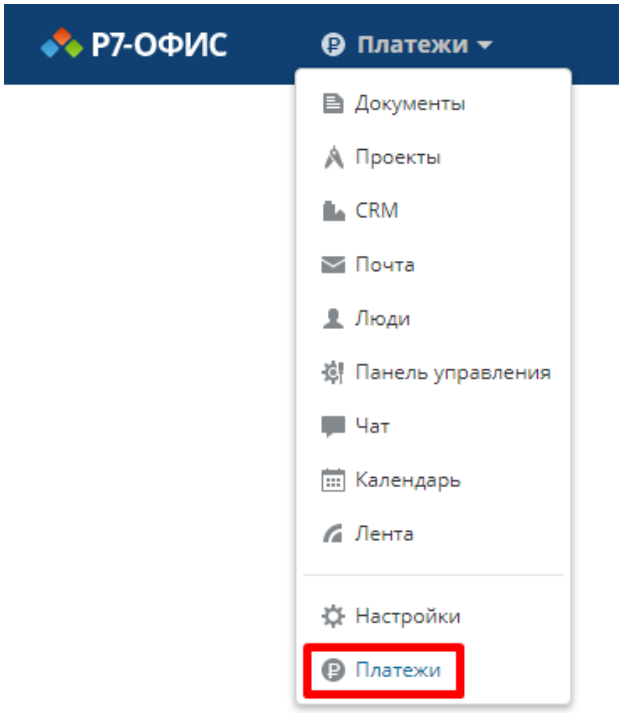
После восстановления, логин и пароль требуется ввести те, которые использовались при регистрации старого портала.



Часто задаваемые вопросы

Проблемы с обновлением или установкой новой лицензии для Корпоративного сервера

В Корпоративном сервер используется лицензия формата .lic, в которой указываются параметры лицензирования. Установить лицензию возможно через страницу **Платежи:**

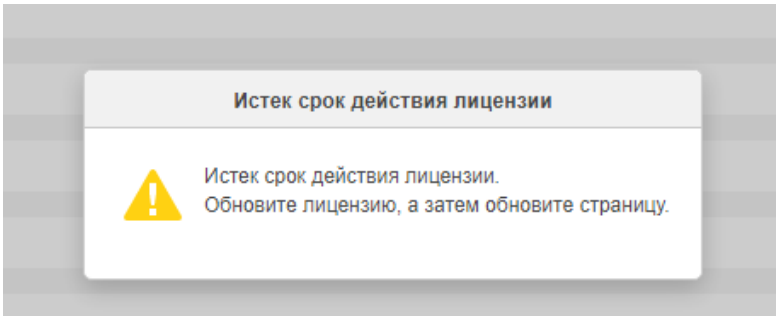


Для загрузки новой лицензии перейдите в Платежи и загрузите файл лицензии в формате .lic, после нажмите Активировать.

В случае если информация не обновилась и указывается некорректная дата в первой строке:

Вы используете "Р7-Офис. Сервер. Профессиональный." Ваша подписка на техподдержку и обновления истекает 18 ноября 2120 г..

Или при открытии файла на редактирование появляется сообщение об истечении срока лицензии:



Возможно подложить файл лицензии в ручном режиме в каталог:
Для Linux: */var/www/r7-office/Data/*

Для Windows: *C:\Program Files (x86)\R7-OFFICE\CommunityServer\Data*

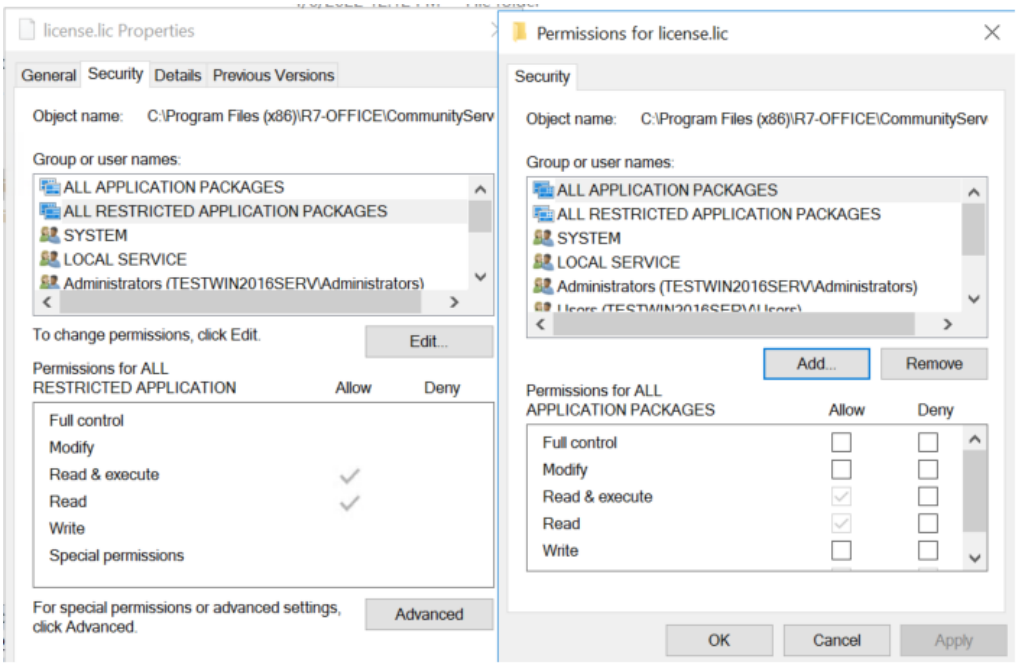
Удалите файл лицензии с именем license, имеющийся в каталоге. Переименуйте новый файл в license.lic и подложите файл лицензии в каталог.

Так же может потребоваться предоставить файлу права:

Для Linux:

chmod -R 777 /var/www/r7-office/Data/license.lic
chown r7-officce:r7-office license.lic

Для Windows: Свойства файла – Security:



Снятия ограничения на копирование с WebDav более 100мб

- Для снятия ограничений со стороны Сервера Совместной работы, на ограничение открытия файлов более 100 МБ.
  (Если сам файл весит более 100 МБ)
  - Добавьте в конфиг web.appsettings.config находящийся по пути C:\Program Files (x86)\R7-OFFICE\CommunityServer\WebStudio\web.appsettings.config ключ:
    <add key="web.available-file-size" value="524288000" />
    В value указывается значение в байтах 524288000 — (500 МБ)
- Для снятия ограничений со стороны Сервера документов, на ограничение открытия файлов более 100 МБ.
  (Если содержимое файла весит более 100 МБ)
- Измените конфигурации local-production-linux.json, находящийся по пути C:\Program Files (x86)\R7-OFFICE\DocumentServer\config\production-linux.json.

Предварительно, перед внесением изменений в файлы конфигурации, рекомендуем сделать бекап имеющегося файла production-linux.json

Добавив следующие строки:

```
.....
  "FileConverter": {
    "converter": {
      "fontDir": "/usr/share/fonts",
      "maxDownloadBytes": 524288000,
      "inputLimits": [ {
        "type": "docx;dotx;docm;dotm",
              "zip": {
                    "uncompressed": "500MB",
                    "template": "*.xml"
                   }
      }, {
        "type": "xlsx;xltx;xlsm;xltm",
             "zip": {
                    "uncompressed": "500MB",
                    "template": "*.xml"
                  }
      }, {
        "type": "pptx;ppsx;potx;pptm;ppsm;potm",
```

```
            "zip": {
                "uncompressed": "500MB",
                "template": "*.xml"
                }
     }
   ],
    "presentationThemesDir": "/var/www//sdkjs/slide/themes",
    "x2tPath": "/var/www//server/FileConverter/bin/x2t",
    "docbuilderPath": "/var/www//server/FileConverter/bin/docbuilder",
    "docbuilderAllFontsPath": "/var/lib//App_Data/docbuilder/AllFonts.js",
    "docbuilderCoreFontsPath": "/var/www//core-fonts"
  }
 },
.....
```

- Или замените на файл, прикреплённый (production-linux.txt), если до этого момента изменений в файлах конфигурации не производилось (production-linux.json).
  Значение параметров:
  - maxDownloadBytes — это максимальный размер файла, который может быть скачан в кеш (в байтах) Сервером Документов для просмотра или редактирования. Размер по умолчанию 100Мб.
  - inputLimits uncompressed — это общий размер всех .xml файлов внутри документа (Для каждого вида Документ/таблица/Презентация отдельное ограничение)
- Чтобы проверить размер файла Openxml*, файлы можно переименовать в zip и открыть архиватором. Внутри будет папка с файлами, будет возможно оценить общий размер содержащихся в ней .xml файлов.
  *docx/xlsx/pptx...
- Завершить все сессии редактирования документов:
  - **linux**: bash /usr/bin/documentserver-prepare4shutdown.sh
  - **Windows**: «C:\Program Files (x86)\R7-OFFICE\DocumentServer\bin\documentserver-prepare4shutdown.bat«
- Перезагрузить Сервер.
- Загрузите новый файл, чтобы проверить возможность его открытия.

Документы, которые были открыты с ошибкой, продолжат открываться с ошибкой, т.к документ уже находится в кеше БД и хранилища.

Перенос хранилища документов с одного логического диска на другой на Windows Server

Перед переносом данных, рекомендуем Вам, выполнить бекап сервера или создать снимок состояния, во избежание потери информации.

Для переноса пользовательских данных на отдельный диск, необходимо переместить всю папку C:\Program Files (x86)\R7-OFFICE\CommunityServer**Data**

Измените файл конфигурации: C:\Program Files (x86)\R7-OFFICE\CommunityServer\WebStudio**web.storage.config**
Отредактируйте в файле строку <property name=»$STORAGE_ROOT» value=»**..\Data**» />
к виду <property name=»$STORAGE_ROOT» value=»**C:\Test\Data**» />
где **C:\Test\Data** путь к новому расположению каталога **Data**.

Для применения изменений, необходимо перезапустить сайты (Р7-Офис. Совместная работа и Р7-Офис. Совместная работа. Системное API) в IIS.

Вы можете оставить файл лицензии по старому адресу: C:\Program Files (x86)\R7-OFFICE\CommunityServer**Data\license.lic**, тогда при замене лицензии, через страницу «Платежи», файл будет автоматически обновлен.
В случае перемещения файла лицензии, необходимо отредактировать файл настройки сервера Документов.
Отредактируйте файл C:\Program Files (x86)\R7-OFFICE\DocumentServer\config\local.json
Где необходимо изменить строку:
«license»: {
«license_file»: «C:/Test/Data/license.lic»
где **C:/Test/Data/** путь к новому расположению каталога **Data**.

После изменения настроек конфигурации необходимо перезапустить сервисы редактора документов.

Перенос хранилища документов с одного логического диска на другой на Linux

Для переноса пользовательских данных, мы рекомендуем скопировать всю папку **/var/www/r7-office/Data/**

Перед переносом данных, рекомендуем Вам, выполнить бекап Портала.

cp -r /var/www/r7-office/Data /var/Data/ где /var/Data/ путь к новому расположению каталога Data.

1. Измените файл конфигурации: **nano /var/www/r7-office/WebStudio/web.storage.config**
   Отредактируйте в файле строку **<property name=»$STORAGE_ROOT» value=»../Data/» />**
   к виду **<property name=»$STORAGE_ROOT» value=»/var/Data/» />** где **/var/Data/** путь к новому расположению каталога **Data.**

Измените владельца папки **Data** на **r7-office**:
chown -R r7-office:r7-office /var/Data/ где /var/Data/ путь к новому расположению каталога **Data**.

Потребуется изменить следующие конфигурации:

2. /var/www/r7-office/Services/TeamLabSvc/radicale.config

```
filesystem_folder = /var/Data/radicale/collections/
```

3. /var/www/r7-office/Services/Jabber/web.storage.config

```
property name="$STORAGE_ROOT" value="/var/Data/"
```

4. /etc/r7-office/communityserver/storage.production.json

```
value": "/var/Data"
```

5. /etc/r7-office/communityserver/storage.json

```
"value": "\\var\\Data\\"
```

6. /var/www/r7-office/Services/TeamLabSvc/TeamLabSvc.exe.config

```
<add key="temp" value="/var/Data/temp" />
...
<add key="license.file.path" value="/var/Data/license.lic" />
```

7. /var/www/r7-office/WebStudio/web.appsettings.config

```
<add key="temp" value="/var/Data/temp" />
...
<add key="license.file.path" value="/var/Data/license.lic" />
```

8. Перенести файлы из каталога /var/www/r7-office/Data

```
cd /var/www/r7-office/Data
cp -rp ./* /var/Data/
```

Так как путь к файлу лицензии изменился, необходимо отредактировать файл настройки сервера Документов.
Отредактируйте файл nano **/etc/r7-office/documentserver/production-linux.json**
Где необходимо изменить строку:
«license»: {
«license_file»: «/var/www/r7-office/documentserver/../Data/license.lic»,
к виду **«license_file»: «/var/Data/license.lic», где /var/Data/** путь к новому расположению каталога Data.

После изменения настроек конфигурации необходимо перезагрузить сервер или перезапустите сервисы:

```
systemctl restart r7-office* monoserve
```

Неверный формат токена безопасности при открытии документа

Если при обновлении или изменении конфигурации Р7-Офис Сервера у вас возникла ошибка при открытии документа «Неверный формат токена безопасности» вам необходимо следовать нижеприведенной инструкции.

Необходимо изменить значения files.docservice.secret и files.docservice.secret.header в файле web.appsettings.config.

Для Windows Server
C:\Program Files (x86)\R7-OFFICE\CommunityServer\WebStudio\web.appsettings.config
Значения которые необходимо указать в файле **web.appsettings.config** находятся в файле

C:\Program Files (x86)\R7-OFFICE\DocumentServer\config**local.json** и равны значению у параметров «token» — «inbox» — «header» и «secret» — «inbox» — «string»

Измените значения в файле web.appsettings.config:
files.docservice.secret на значение из «secret» — «inbox» — «string»
files.docservice.secret.header на значение из «token» — «inbox» — «header»
После изменения файла необходимо перезапустить Windows Server.

Для Linux
nano /var/www/r7-office/WebStudio/web.appsettings.config
Значения которые необходимо указать в файле web.appsettings.config находятся в файле /etc/r7-office/documentserver/local.json и равны значению у параметров «token» — «inbox» — «header» и «secret» — «inbox» — «string»

nano /etc/r7-office/documentserver/local.json

Измените значения в файле web.appsettings.config:
files.docservice.secret на значение из «secret» — «inbox» — «string»
files.docservice.secret.header на значение из «token» — «inbox» — «header»

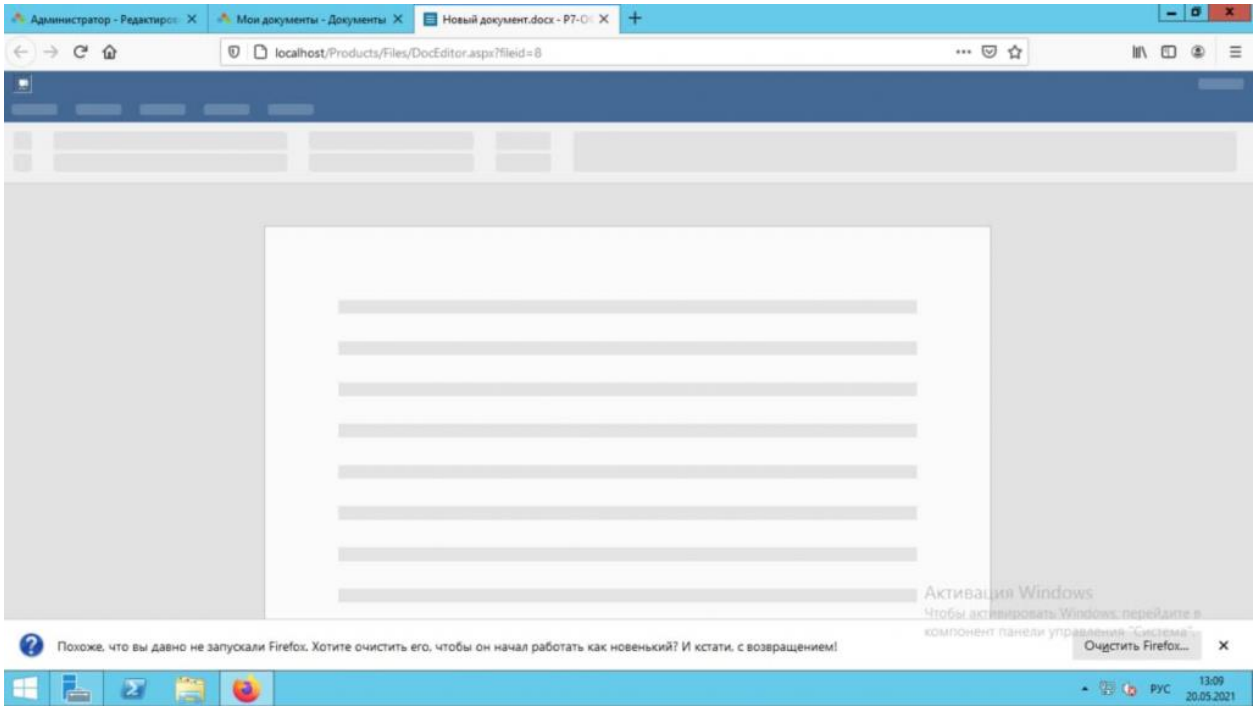
После изменения файла необходимо перезапустить службу MONO:
systemctl restart monoserve

Не открываются онлайн редакторы при создании/открытии файла

Примечание: данная проблема наблюдается только на Windows Server.

В случае, если онлайн редакторы не открываются при открытии файла или создании нового

Пример на скриншотах



Для решения проблемы необходимо выполнить следующие действия:

1. Откройте пункт меню Пуск — «RabbitMQ Server»
2. Остановите RabbitMQ — RabbitMQ Service — stop
3. Удалите службу — RabbitMQ Service — remove
4. Переустановите службу — RabbitMQ Service — (re)install
5. Запустите службу — RabbitMQ Service — start

Проверьте, что служба RabbitMQ запущена и откройте документ на редактирование.