Outlook on the web (OWA)

Outlook on the web (https://microsoft.com/microsoft-365/outlook) — это веб-почта для доступа к серверу совместной работы.

Подключение Outlook к Blitz Identity Provider выполняется по протоколу WS-Federation (частный случай протокола SAML от Microsoft). На стороне Exchange и OWA настройки будут выполняться для метода аутентификации ADFS, т.к. в данном случае Blitz Identity Provider выступает заменой ADFS. Состоит из трех этапов:

- Этап 1. Настройки Exchange organization для использования аутентификации ADFS
- Этап 2. Настройки аутентификации ADFS в Outlook on the web и в виртуальных каталогах EAC
- Этап 3. Настройки на стороне Blitz Identity Provider

Важно:

В инструкции для примера указано, что Outlook расположен на домене `https://mail.company.com/owa`, а Blitz IDP установлен на домене `https://login.company.com`. Уточните ваши адреса перед применением инструкции.

Этап 1. Настройки Exchange organization для использования аутентификации ADFS

Важно:

Нельзя использовать wildcard-сертификаты в SAML, сертификат должен быть на домене Blitz Identity Provider.

1. Необходимо получить отпечаток сертификата Blitz IDP. Для этого нужно взять его из метаданных Blitz - пройдите по ссылке `https://login.company.com/blitz/saml/profile/Metadata/SAML`, откройте XML документ с метаданными и найдите раздел `<ds:X509Certificate>`. Например:



Добавьте строки:

```
-----BEGIN CERTIFICATE-----
  <значение сертификата>
-----END CERTIFICATE-----
```

Сохраните сертификат в файл с расширением .crt. **Найдите** в данных сертификата отпечаток SHA-1.

2. Далее **введите** команду:

```
Set-OrganizationConfig -AdfsIssuer <BlitzURL> -AdfsAudienceUris "<OotwURL>","<EACURL>" -AdfsSignCertificateThumbprint "<Thumbprint>"
```

Где указать следующие значения:

- **BlitzURL**: `https://login.company.com/blitz/saml/profile/WSF-PRP/WSIGNIN/GET`
- **OotwURL** (Outlook on the web URL): `https://mail.company.com/owa/`
- **EACURL**: `https://mail.company.com/ecp/`
- **Thumbprint** (отпечаток сертификата): укажите значение, полученное в п.1

Важно:

При использовании самоподписного SAML-сертификата необходимо добавить его в доверенные корневые на серверах Exchange.

Этап 2. Настройки аутентификации AD FS в Outlook on the web и в виртуальных каталогах EAC

Для Outlook on the web и виртуальных каталогов EAC необходимо настроить аутентификацию AD FS как единственный доступный метод, отключив все остальные методы.

1. Чтобы использовать командную консоль Exchange для настройки EAC или Outlook on the web в виртуальном каталоге так, чтобы они принимали только аутентификацию ADFS, **введите** следующую команду (для примера указан сервер с именем Mailbox01):

```
Set-EcpVirtualDirectory -Identity <VirtualDirectoryIdentity> -AdfsAuthentication $true -BasicAuthentication $false -DigestAuthentication $false -FormsAuthentication $false -OAuthAuthentication $false -WindowsAuthentication $false
```

Где используются следующие значения параметра `VirtualDirectoryIdentity`:

- `"Mailbox01\ecp https://mail.company.com/ecp/"` - настройка виртуальный каталог EAC на веб-сайте по умолчанию на сервере с именем Mailbox01;

- `"Mailbox01\owa https://mail.company.com/owa/"` - настройка Outlook в виртуальном каталоге Web на веб-сайте по умолчанию на сервере с именем Mailbox01.

2. Чтобы настроить все виртуальные каталоги EAC и Outlook on the web на каждом сервере Exchange в вашей организации, выполните следующие команды:

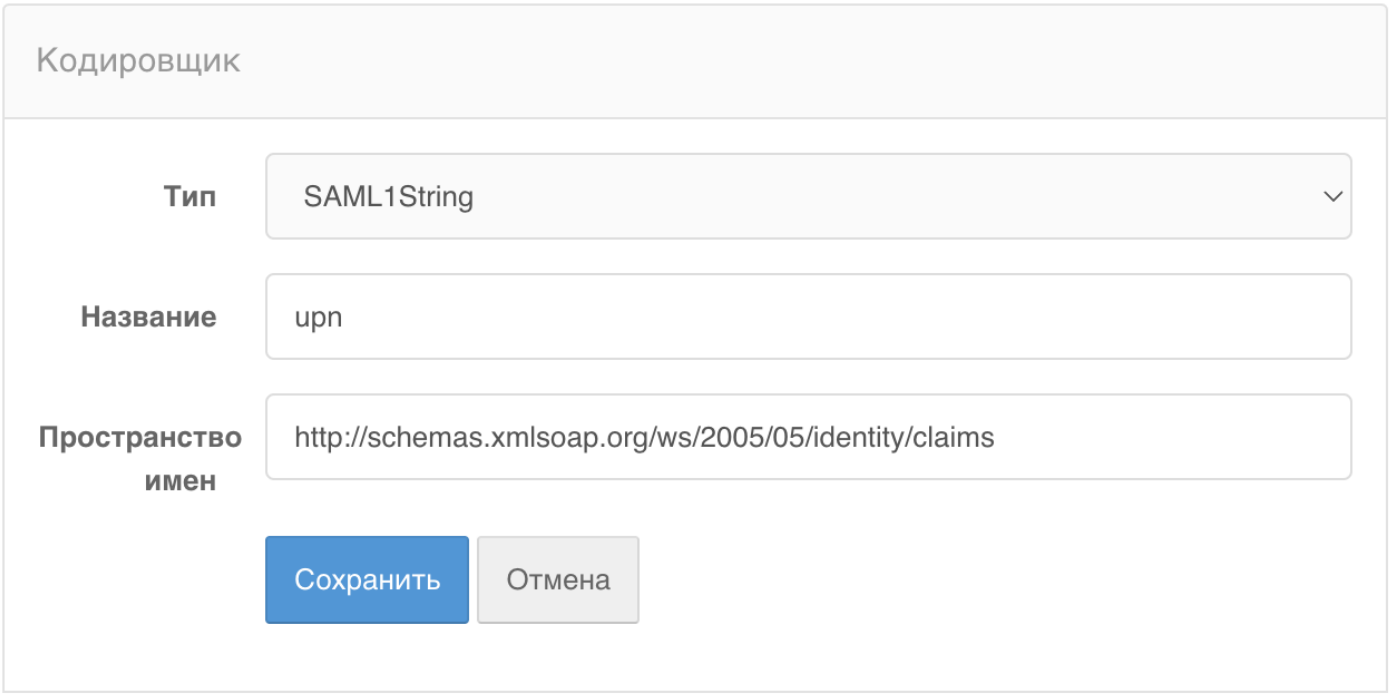
```
Get-EcpVirtualDirectory | Set-EcpVirtualDirectory -AdfsAuthentication $true -BasicAuthentication $false -DigestAuthentication $false -FormsAuthentication $false -OAuthAuthentication $false -WindowsAuthentication $false
```

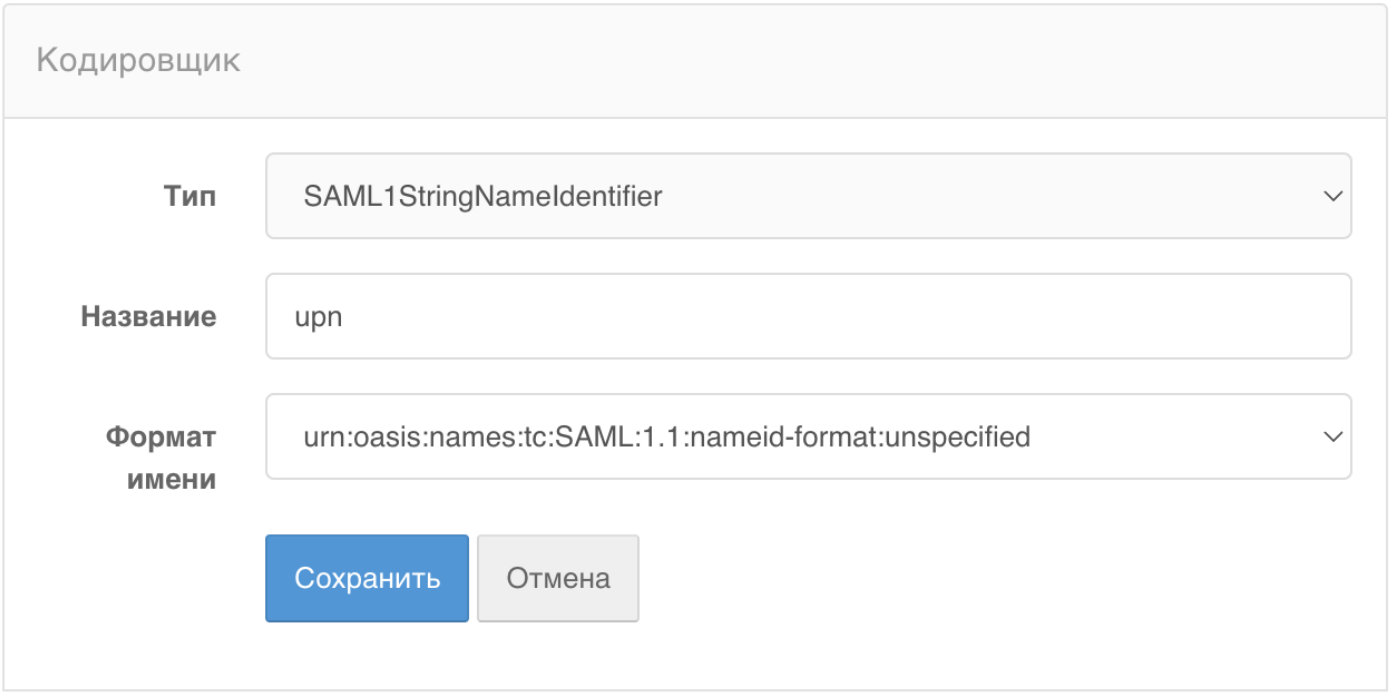
`Get-OwaVirtualDirectory | Set-OwaVirtualDirectory -AdfsAuthentication $true -BasicAuthentication $false -DigestAuthentication $false -FormsAuthentication $false -OAuthAuthentication $false -WindowsAuthentication $false`

Этап 3. Настройки на стороне Blitz Identity Provider

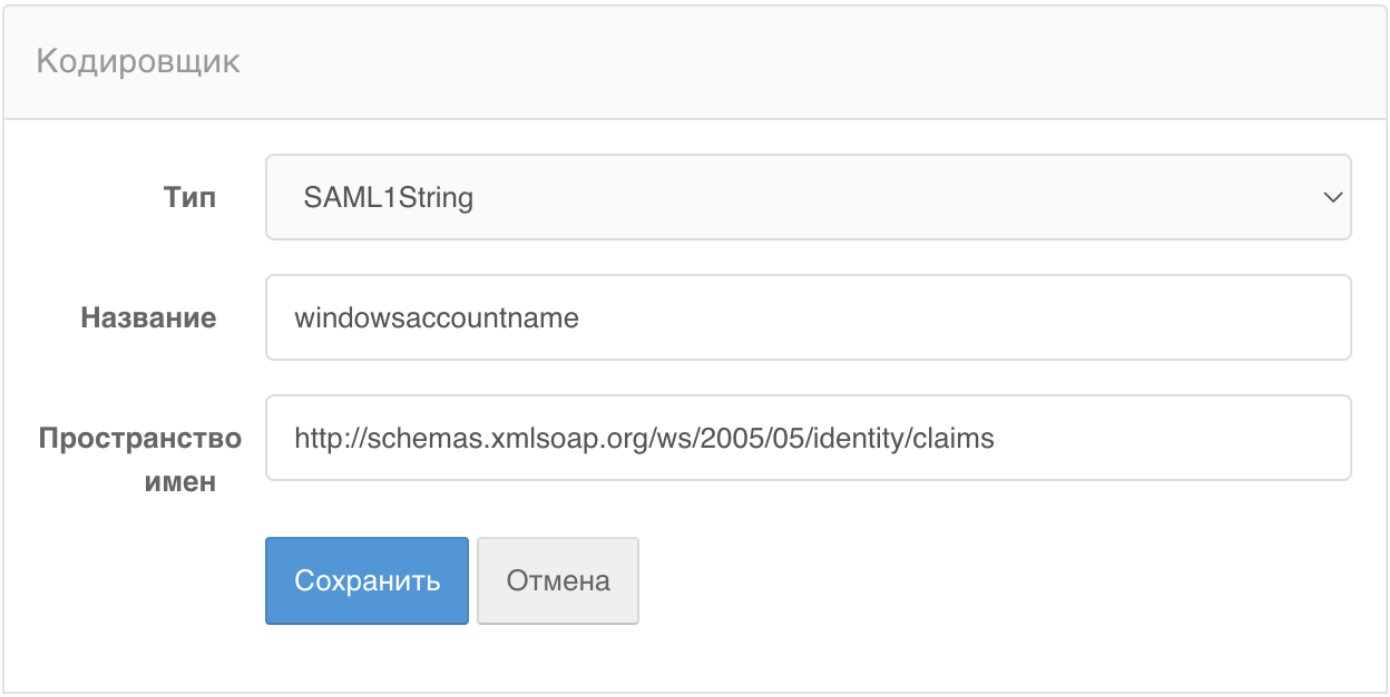
В консоли управления Blitz Identity Provider перейдите в раздел **SAML** и выполните следующие действия:

1. Нажмите **Добавить новый SAML-атрибут**.
2. Укажите название первого атрибута - `upn` и выберите из выпадающего списка его источник - атрибут, который соответствует атрибуту `userPrincipalName` в хранилище. После нажмите **Добавить**.
3. Укажите название второго атрибута - `windowsaccountname` и выберите из выпадающего списка его источник - атрибут, который соответствует атрибуту `sAMAccountName` в хранилище. После нажмите **Добавить**.
4. Далее добавьте кодировщик для каждого атрибута. Для этого выберите атрибут и нажмите **Добавить кодировщик**.
5. Для атрибута `upn` добавьте первый кодировщик `SAML1String` и укажите **Пространство имен** `http://schemas.xmlsoap.org/ws/2005/05/identity/claims`. Далее добавьте второй кодировщик - `SAML1StringNameIdentifier` и укажите **Пространство имен** `urn:oasis:name:tc:SAML:1.1:nameid-formar:unspecified`. Нажмите **Сохранить** после каждого создания кодировщика.





6. Для атрибута `windowsaccountname` добавьте кодировщик `SAML1String` и укажите **Пространство имен** `http://schemas.xmlsoap.org/ws/2005/05/identity/claims`. Нажмите **Сохранить**.



7. Далее в консоли управления *Blitz Identity Provider* перейдите в раздел **Приложения**.
8. Создайте новое приложение, задав его базовые настройки:

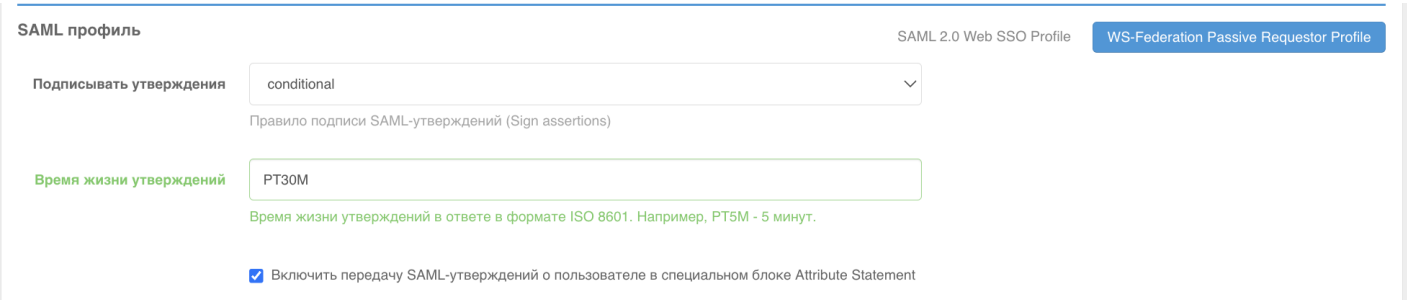
- **Идентификатор (entityID или client_id)**: `https://mail.company.com/owa/`
- **Название**: укажите название приложения, которое видно только внутри Blitz. Например, `OWA`.
- **Домен**: `https://mail.company.com/owa/`



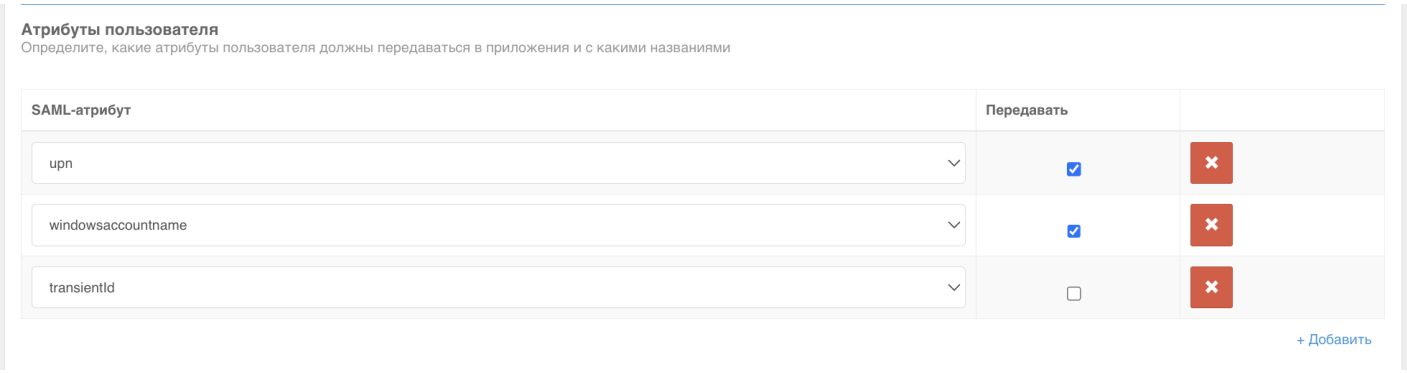
9. Нажмите **Сохранить**.
10. Далее нажмите кнопку **Параметры**  у предложения OWA и отредактируйте параметры приложения:

- **Стартовая страница приложения**: `https://mail.company.com/owa`
- **Протоколы**: выберите `SAML` и нажмите **Сконфигурировать**

- Выберите **WS-Federation Passive Requestor Profile** и нажмите **Сконфигурировать**. Установите следующие настройки:
  - **Подписывать утверждения**: `conditional`
  - **Время жизни утверждений**: `PT30M`
  - **Включить передачу SAML-утверждений о пользователе в специальном блоке AttributeStatement**: установить флажок.



11. В разделе **Атрибуты пользователя** настройте передачу в Outlook атрибутов, созданных на первом этапе SAML-атрибутов и атрибута `transientId`. Пометьте передачу атрибутов `upn` и `windowsaccountname` галочкой.



12. Нажмите **Сохранить**.
13. Далее в разделе **Метаданные** нажмите **Изменить**. Скопируйте и вставьте следующий код:

```
<?xml version="1.0" encoding="UTF-8"?>
<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
 xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
 entityID="https://mail.company.com/owa/">
 <md:SPSSODescriptor protocolSupportEnumeration="urn:mace:shibboleth:wsf-prp:1.0:protocol">
  <md:AssertionConsumerService Binding="urn:mace:shibboleth:1.0:bindings:HTTP-POST-wsignin"
  Location="https://mail.company.com/owa/"
  index="1"/>
  <md:AssertionConsumerService Binding="urn:mace:shibboleth:1.0:bindings:HTTP-POST-wsignin"
  Location="https://mail.company.com/ecp/"
  index="2"/>
```

</md:SPSSODescriptor>

</md:EntityDescriptor>

14. Нажмите **Сохранить**.

Совет:

После прохождения всех шагов рекомендуем проверить корректность входа в Outlook on the web: `https://mail.company.com/owa`

Версия #19
Admin создал 2024-09-20 11:30:20 UTC
Обновлено 2025-08-29 12:51:00 UTC