SSO Contact Center с идентификационным поставщиком Okta

Содержание

Введение

Этот документ описывает конфигурацию Идентификационного Сервиса (ИДЕНТИФИКАТОРЫ) и Идентификационный Поставщик (IdP) для Okta основанная на облачных вычислениях Единая точка входа (SSO).

Продукт	Развертывания
UCCX	Совместно расположенный
PCCE	Совместно расположенный с CUIC (Cisco унифицированный интеллектуальный центр) и L (оперативные данные)
UCCE	Совместно расположенный с CUIC и LD для 2k развертываний. Автономный для 4k и 12k развертываний.

Предварительные условия

Требования

Корпорация Cisco рекомендует ознакомиться со следующими темами:

- Cisco Unified Contact Center Express, Cisco Unified Contact Center Enterprise (UCCE) или Упакованное предприятие Contact Center (PCCE)
- Язык разметки утверждений безопасности (SAML) 2.0
- Okta

Используемые компоненты

- UCCE 11.6
- Okta **Примечание:** Ссылки этого документа UCCE в снимках экрана и примерах, однако конфигурация подобна относительно Идентификационного Сервиса Cisco (UCCX/UCCE/PCCE) и IdP.

Сведения, представленные в этом документе, были получены от устройств, работающих в

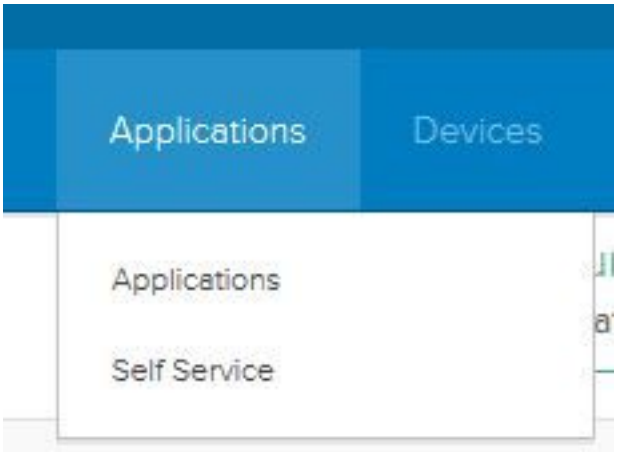
специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Настройте Okta как идентификационного поставщика услуг

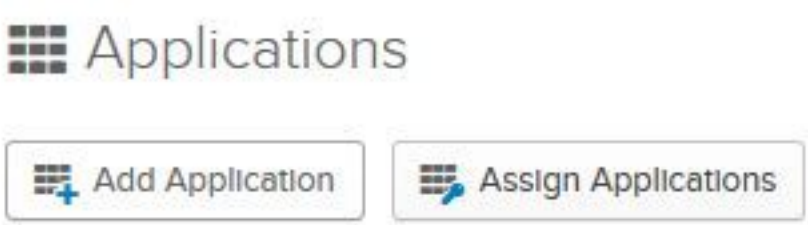
Шаг 1. Войдите к Идентификационному Сервису (ИДЕНТИФИКАТОРЫ) в веб-страницу и перейдите к **Параметрам настройки** и загрузите файл метаданных путем нажатия **Download Metadata File.**

Шаг 2. Войдите к серверу Okta и выберите **вкладку Admin**.

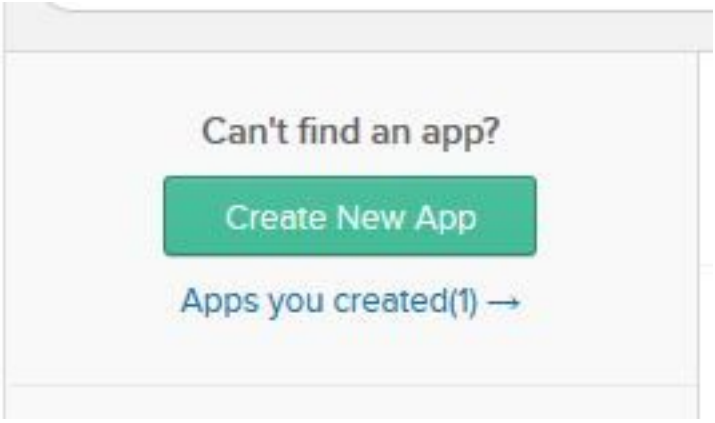
Шаг 3. От информационной панели Okta выберите **Applications> Applications.**



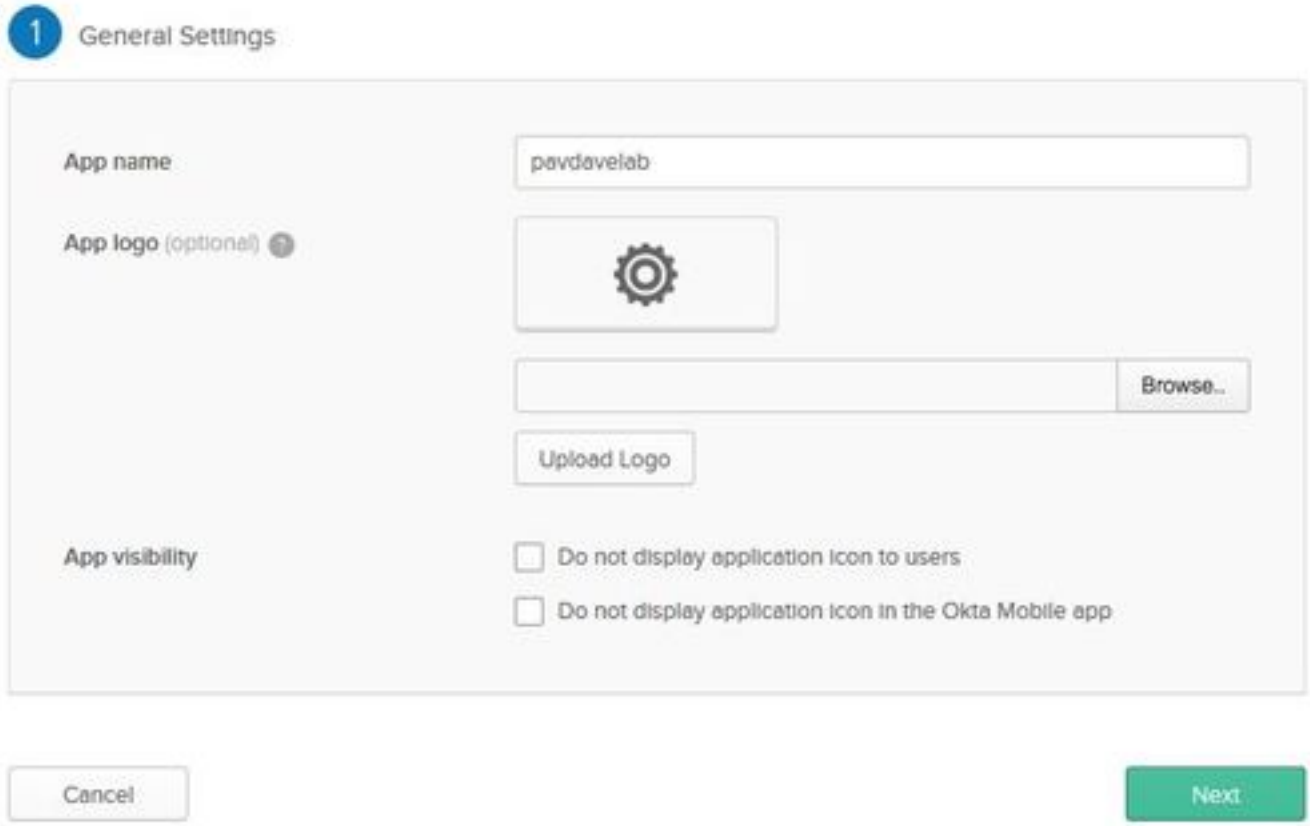
Шаг 4. . Нажмите **Create a New App** для создания нового пользовательского приложения с помощью мастера.



Шаг 5. . На Создавании Окна интеграции Нового приложения, для Платформы выбирают **Web** на выпадающем списке и выбирают **SAML 2.0** как Знак на методе и выбирают, создают.



Шаг 6. Введите имя Приложения и нажмите **Next**.



Шаг 7. На Интеграции SAML страница Create SAML вводит подробные данные.

- **URL единой точки входа** - От файла метаданных, введите URL, заданный в как индекс 0 AssertionConsumerService.

```
<AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
Location="https://cuicpub-ids.pavdave.xyz:8553/ids/saml/response" index="0" isDefault="true"/>
```

- **Используйте это для URL Получателя и Целевого URL** - Проверка эта опция, чтобы позволить совпасть получателя и целевых URL
- **Позвольте этому приложению запрашивать другие URL SSO** - Проверка эта опция, если вы имеете множественные узлы IdS в своих развертываниях и хотите позволить запросы от других URL SSO помимо Издателя IdS.
  - **URL SSO Requestable** — Это поле появляется, только если вы проверяете вышеупомянутый флажок. Можно ввести URL SSO для других узлов. Можно найти

URL ACS в файле метаданных путем поиска всего AssertionConsumerService (ACS) адреса, которые используют Привязку HTTP-POST. Добавьте те подробные данные для этого поля. Нажмите кнопку Add Another для добавления mulitple URL.

- **URI аудитории (ID Объекта SP)** - От файла метаданных, введите адрес **entityID**.

```
<?xml version="1.0" encoding="UTF-8"?><EntityDescriptor
xmlns="urn:oasis:names:tc:SAML:2.0:metadata" entityID="cuicpub-ids.pavdave.xyz">
```

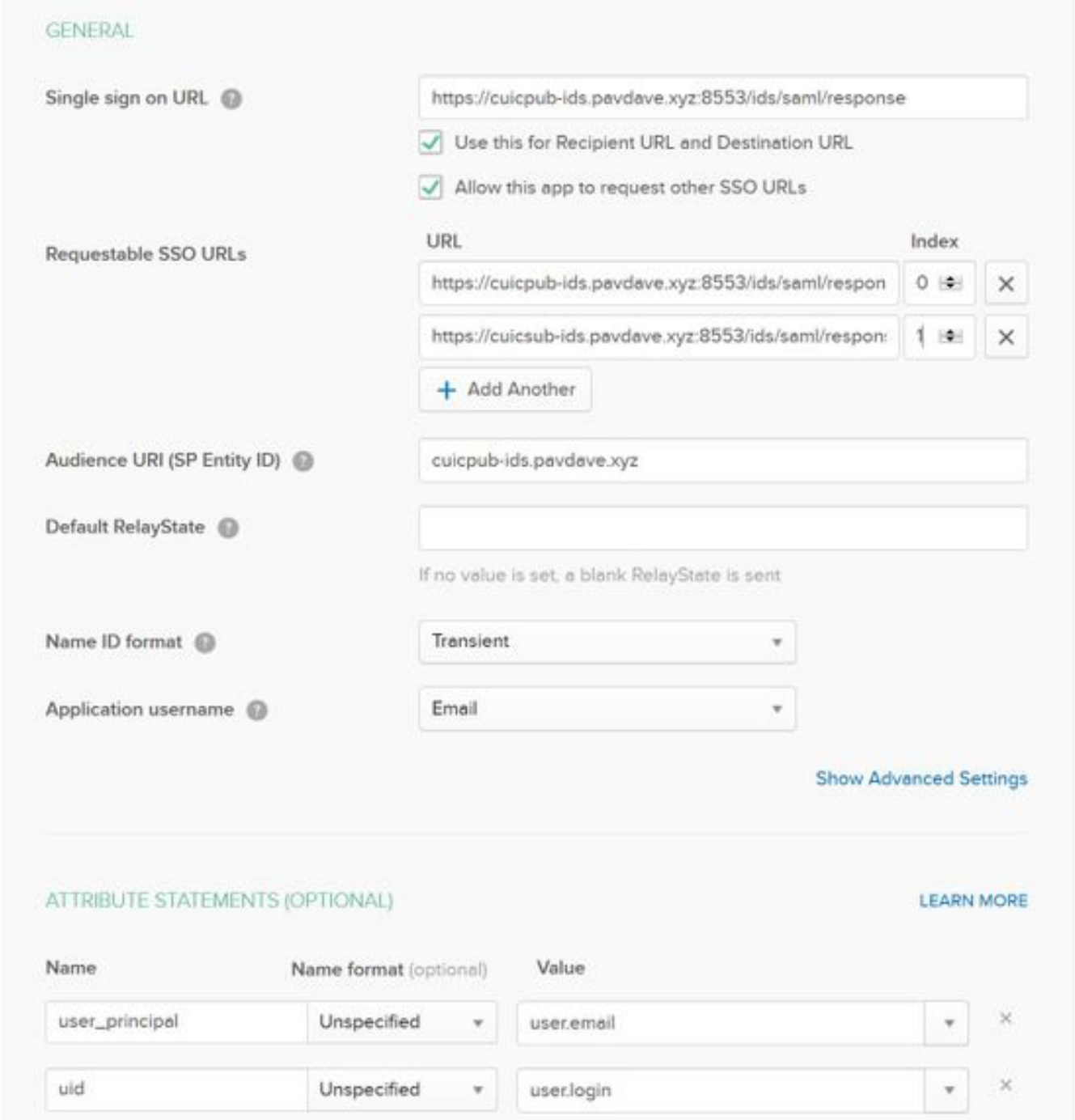
- **RelayState по умолчанию** - Оставляют это незаполненное поле.
- **ID названия Формат -** Выбирает **Transient** из выпадающего списка.
- **Имя пользователя приложения** - Выбирает формат имени пользователя, который совпадает**, Имя пользователя**, настроенное в **Унифицированном администрировании CCE>, Управляют> Агенты.**

Примечание: Этот снимок экрана является определенным для UCCE/PCCE.

Шаг 8. Добавьте операторы обязательного атрибута.

- **uid** - Определяет проверенного пользователя в требовании, передаваемом приложениям
- **user_principal** - Определяет область аутентификации пользователя в утверждении, передаваемом Идентификационному Сервису Cisco

.



Шаг 9. Выберите **Next.**

Шаг 10. Выберите **"I am a software vendor. I would like to integrate my app with Okta"** и нажмите Finish.

Шаг 11. На **Sign On** вкладка загружают **Идентификационные метаданные Поставщика.**

Шаг 12. Откройте загруженный файл метаданных и измените две линии NameIDFormat к следующему и сохраните файл.

```
<?xml version="1.0" encoding="UTF-8"?><EntityDescriptor
xmlns="urn:oasis:names:tc:SAML:2.0:metadata" entityID="cuicpub-ids.pavdave.xyz">
```

Настройте идентификационный сервис

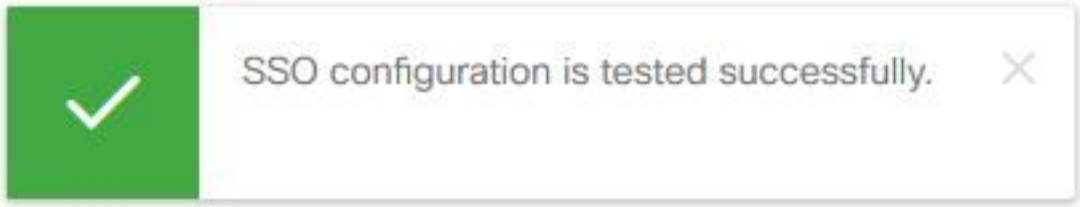
Шаг 1. Перейдите к своему Идентификационному серверу Сервиса.

Шаг 2. Нажмите **Settings.**

Шаг 3. **Нажмите кнопку Next.**

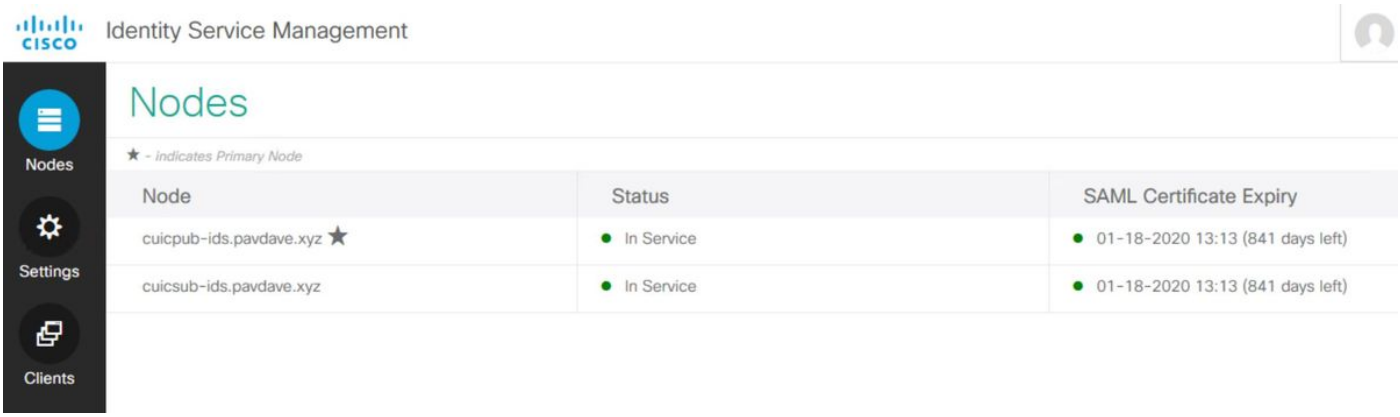
Шаг 4. . Файл метаданных загрузки, загруженный от Okta и, нажимает **Next**.

Шаг 5. . Нажмите **Test SSO Setup**. Новое окно побудит вход в систему аутентифицироваться на Okta. Успешная регистрация в системе покажет, что галочка с **Конфигурацией SSO протестирована успешно** на нижнем правом угле экрана.



> **Примечание:** Если вы будете уже аутентифицироваться на Okta, то вам не предложат войти снова, но будете видеть краткое всплывающее окно, в то время как IdS проверяет учетные данные.

На этом этапе конфигурация Идентификационных Поставщиков Сервиса и Идентичности завершена и должна видеть узлы в обслуживании.



Дальнейшая конфигурация для единой точки входа

После Идентификационного Поставщика Сервиса и Идентичности настроены, следующий шаг должен установить Единую точку входа для UCCE или UCCX.

- UCCE/PCCE
- UCCX

Дополнительное изучение

- Единая точка входа UCCE/PCCE
- Единая точка входа UCCX

- Cisco Unified Communications Manager (CUCM) - идентификационная конфигурация поставщика Okta