# Установите и Настройте Идентификационного Поставщика Шибболета (IdP) для Идентификационного Сервиса Cisco (ИДЕНТИФИКАТОРЫ) для включения SSO

## Содержание



## Введение

Этот документ описывает конфигурацию на Идентификационном Поставщике OpenAM (IdP) для включения Единой точки входа (SSO).

### Модели развертывания Cisco IDS

| 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

Компания Cisco рекомендует предварительно ознакомиться со следующими предметами:

- Cisco Unified Contact Center Express (UCCX) Выпуск 11.6 или Выпуск 11.6 Cisco Unified Contact Center Enterprise или Упакованное предприятие Contact Center (PCCE) Выпуск 11.6 как применимый.

  **Примечание:** Этот документ ссылается на конфигурацию относительно Сервиса Cisco Identitify (ИДЕНТИФИКАТОРЫ) и Идентификационный Поставщик (IdP). Ссылки на документы UCCX в снимках экрана и примерах, однако конфигурация подобна относительно Сервиса Cisco Identitify (UCCX/UCCE/PCCE) и IdP.

### Используемые компоненты

Настоящий документ не имеет жесткой привязки к каким-либо конкретным версиям программного обеспечения и оборудования.

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в данном документе, были запущены с конфигурацией по умолчанию. Если ваша сеть является оперативной, гарантируйте понимание потенциального воздействия любой команды.

## Установить

Шибболет является проектом с открытым исходным кодом, который предоставляет возможности Единой точки входа и позволяет узлам делать информированные решения об авторизации для индивидуального адреса защищенных онлайновых ресурсов сохраняющим конфиденциальность способом. Это поддерживает Язык разметки утверждений безопасности (SAML2). IdS является клиентом SAML2 и ожидаемый поддержать Шибболет с минимальным или никакими изменениями в IdS. В 11.6, IdS квалифицирован для работы с Шибболетом IdP.

**Примечание:** Ссылочный выпуск 3.3.0 Шибболета этого документа как часть квалификации с SSO

### Требования к системе

| Компонент | Подробные данные |
|---|---|
| Версия шибболета | v3 3.0 |
| Расположение загрузки | http://shibboleth.net/downloads/identity-provider/ |
| Установите платформу | Ubuntu 14.0.4<br>версия Java "1.8.0_121" |
| Версия Протокола LDAP | Active Directory 2.0 |
| Веб-сервер шибболета | Tomcat/8.5.12 Apache |

Обратитесь Wiki для установки Шибболета

https://wiki.shibboleth.net/confluence/display/IDP30/Installation

## Настройка

## Интегрируйтесь с Сервером LDAP

Для интеграции Сервера LDAP с шибболетом поля должны быть обновлены в **where$shibboleth_home $shibboleth_home/conf/ldap.properties** (по умолчанию/opt/shibboleth-idp), ссылается на каталог установки, который используется в установке шибболета.

| Поле | Ожидаемое значение | Описание |
|---|---|---|
| idp.authn. LDAP.trustCertificates | Ресурс для загрузки трастовых привязок из, обычно локальный файл в $ {idp.home} / учетные данные где idp.home является переменной среды, экспортируемой как JAVA_OPTS в setenv.sh | % {Idp.home}/credentials/ldap-server.crt |
| idp.authn. LDAP.trustStore | Ресурс для загрузки Java keystore, который содержит трастовые привязки, обычно локальный файл в % {idp.home} / учетные данные | % {Idp.home}/credentials/ldap-server.truststore |
| idp.authn. LDAP.returnAttributes | Список разделенных запятой значений LDAPAttributes, который должен быть возвращен. Если вы хотите возвратить все атрибуты, добавьте "*". | * |
| idp.authn. LDAP.baseDN | BaseDN, в котором должен быть выполнен поиск LDAP | CN=users, DC=cisco, DC=com |
| idp.authn. LDAP.subtreeSearch | Искать ли рекурсивно | tRUE |
| idp.authn. LDAP.userFilter | Фильтр поиска LDAP | (sAMAccountName = {пользователь}) * |
| idp.authn. LDAP.bindDN | DN для привязки с тем, когда выполнен поиск | administrator@cisco.com |
| idp.authn. LDAP.bindDNCredential | Пароль для привязки с тем, когда выполнен поиск | |
| idp.authn. LDAP.dnFormat | Строка форматирования для генерации пользовательских DN для аутентификации | %s@adfsserver. cisco . com (%s@domainname) |
| idp.authn. LDAP.authenticator | Управляет потоком операций для того, как аутентификация происходит против LDAP | bindSearchAuthenticator |
| idp.authn. LDAP.ldapURL | URI соединения для каталога LDAP | |

Для получения дополнительной информации обратитесь:

https://wiki.shibboleth.net/confluence/display/IDP30/LDAPAuthnConfiguration

## Эталонный файл конфигурации

#
т

imeinmilliseconds to wait for responses
#idp.authn.LDAP.responseTime

out

=PT3S##SSLconfiguration,eitherjvmTrust,certif

icateTrust,orkeyStoreTrust#idp.authn.LDAP.sslConfig

=
c
e
r
t
i
f
i
c
a
t
e
T
r
u
s
t
#
#
I
f
u
s
i
n
g
c
e
r
t
i
f
i
c
a
t
e
T
r
u
s
t
a
b
o
v
e
,
s
e
t
t
o
t
h

etrustedcertificate's pathidp.authn.LDAP.trustCertificates

=
%
{
i
d
p
.
h
o
m
e
}
/
c
r
e
d
e
n
t
i
a
l
s
/
l
d
a
p
-
s
e
r
v
e
r
.
c
r
t
#
#
I
f
u
s
i
n
g
k
e
y
S
t
o
r

e
T
r
u
s
t
a
b
o
v
e
,
s
e
t
t
o
t
h
e
t
r
u
s
t
s
t
o
r
e
p
a
t
h
i
d
p
.
a
u
t
h
n
.
L
D
A
P
.
t
r
u
s
t
S
t
o
r
e

=%{idp.home}/credentials/ldap-server.truststore

```
#
#
R
e
t
u
r
n
a
t
t
r
i
b
u
t
e
s
d
u
r
i
n
g
a
u
t
h
e
n
t
i
c
a
t
i
o
n
#
i
d
p
.
a
u
t
h
n
.
L
D
A
P
.
r
e
t
u
r
n
A
t
t
r
```

ibutes

=userPrincipalName,sAMAccountName
idp.authn

.LDAP.returnAttributes

=*##DNresolutionproperties

s
#
#
#SearchDNresolution,usedbyanonSearchAuthenticator,bindSearchA

uthenticator#

forAD:CN=Users,DC=example,DC=orgidp.authn.LDAP.base

DN

=CN=users,DC=cisco,DC=com
idp.authn.L

DAP.subtreeSearch

=true*

idp.auththn.LDAP.userFil

t
e
r

=
(
s
A
M
A
c
c
o
u
n
t
N
a
m
e
=
{
u
s
e
r
}
)
*
#
b
i
n
d
s
e
a
r
c
h
c
o
n

```
figuration
#
forAD:idp.authn.LDAP.bindDN=adminuser@domain.com
idp.a
```

uthn.LDAP.bindDN

=administrator@ciscoc

omidp.authn.LDAP.bindDNCredential

=Cisco@123#Forma

tDNresolution,usedbydirectAuthenticator,adAuthenticator# forADus

```
eidp.authn.LDAP.dnFormat=%s@domain.com
#idp.authn.LDAP.dnFormat
```

=%s@adfsserver.cisco.com
#LDAPattributeconfi

guration,seeattribute-resolver.xml#Note,thislikelywon'tapplytot

**heuseoflegacyV2resolverconfigurationsidp.attributeresolver.LDAP**

.ldapURL

=%{idp.authn.LDAP.ldapURL}
idp.attribute.reso

lver.LDAP.connectTimeout

=%{idp.authn.LDAP.connectTimeout:PT

3
S
}
idp.attribute.resolver.LDAP.responseTimeout

=
%
{
idp.authn.L

DAP.responseTimeout:PT3S}
idp.attribute.resolver.LDAP.baseDN

```
=
%
{
i
d
p
.
a
u
t
h
n
.
L
D
A
P
.
b
a
s
e
D
N
:
u
n
d
e
f
i
n
e
d
}
{
i
d
p
.
a
t
t
r
i
b
u
t
e
.
r
e
s
o
l
v
e
```

r.LDAP.bindDN

=%{idp.authn.LDAP.bindDN:undefined}
idp

.attributeresolver.LDAP.bindDNCredential

=%{idp.authn.LDAP.bi

ndDNCredential:undefined}
idp.attribute.resolver.LDAP.useStartTLS

=%{idp.authn.LDAP.useStartTLS:true}
idp.attribute.resolve

r
.
L
D
A
P
.
t
r
u
s
t
C
e
r
t
i
f
i
c
a
t
e
s

=
%
{
i
d
p
.
a
u
t
h
n
.
L
D
A
P
.
t
r
u
s
t
C
e
r
t
i
f
i
c
a
t
e
s
:
u
n

defined}
idp.attribute.resolver.LDAP.searchFilter

=(sAMAcco

```
untName=$resolutionContext.principal)
```

## Позвольте запросы от всех клиентов

Чтобы гарантировать, что запросы от всех клиентов достигают, изменения требуются в **"$shibboleth_home/conf/access-control.xml"**

<ключ записи = "AccessByIPAddress">
<бобовый идентификатор = "AccessByIPAddress" порождают = "шибболет.
IPRangeAccessControl"
p : allowedRanges = "# {{'127.0.0.1/32', **'0.0.0.0/0'**, ':: 1/128', '10.78.93.103/32'}}"/>
</запись>

Добавьте **'0.0.0.0/0'** к позволенным диапазонам. Это позволяет запросы от любого диапазона IP.

## Настройте Шибболет для интеграции с IdS

### Защищенный алгоритм хэширования (SHA1) и настройка шифрования в IdS

Для настройки IdS для установки по умолчанию к
SHA1 откройте **"$shibboleth_home/conf/idp.properties"** и установите:

idp.signing.config = шибболет. SigningConfiguration. SHA1

Эта конфигурация может также быть изменена:

idp. шифрование. дополнительный = истинный

Если вы установите его в True, то сбой для определения местоположения ключа шифрования для использования, когда включено, не приведет к сбою запроса.
Это помогает делать шифрование "воспользовавшись ситуацией", т.е. шифровать каждый раз, когда возможный (совместимый ключ, как находят, в метаданных узла шифрует с) но пропускать шифрование иначе.

Настройте uid и user_principal к Ответу SAML

AttributeDefinition добавлен в **"$shibboleth_home/conf/attribute-resolver.xml"** для сопоставления sAMAccountName и userPrincipalName к к uid и user_principal в ответе SAML.

Кроме того, добавьте параметры настройки разъёма ldap с меткой <DataConnector>.

> **Примечание:** ReturnAttributes должен быть задан со значением **"sAMAccountName userPrincipalName"**.

> **Примечание:** Если существует интеграция с Active Directory (AD), LDAPProperty является обязательным в случае, если.

```
<AttributeDefinition xsi:type="Simple" id="ciscoUPN" sourceAttributeID="userPrincipalName">
 <Dependency ref="LDAP" />
 <AttributeEncoder xsi:type="SAML1String" name="user_principal" />
 <AttributeEncoder xsi:type="SAML2String" name="user_principal" friendlyName="user_principal" />
</AttributeDefinition>

<AttributeDefinition xsi:type="Simple" id="ciscoUID" sourceAttributeID="sAMAccountName">
 <Dependency ref="LDAP" />
 <AttributeEncoder xsi:type="SAML1String" name="uid" />
 <AttributeEncoder xsi:type="SAML2String" name="uid" friendlyName="uid" />
</AttributeDefinition>

    <DataConnector id="LDAP" xsi:type="LDAPDirectory"
     ldapURL="ldap://adfsserver.cisco.com"
     baseDN="CN=users,DC=cisco,DC=com"
     principal="administrator@cisco.com"
     principalCredential="<cred>">
        <FilterTemplate>
            <![CDATA[
                %{idp.attribute.resolver.LDAP.searchFilter}
            ]]>
        </FilterTemplate>
      <ReturnAttributes>sAMAccountName userPrincipalName</ReturnAttributes>
      <LDAPProperty name="java.naming.referral" value="follow"/>
    </DataConnector>
```

Включите изменения в **"$shibboleth_home/conf/attribute-filter.xml"**

```
<PolicyRequirementRule xsi:type="ANY" />
```

```
        <AttributeRule attributeID="ciscoUID">
            <PermitValueRule xsi:type="ANY" />
        </AttributeRule>

        <AttributeRule attributeID="ciscoUPN">
            <PermitValueRule xsi:type="ANY" />
        </AttributeRule>
```

Измените **"$shibboleth_home/conf/saml-nameid.xml"** toinclude

```
<bean parent="shibboleth.SAML2AttributeSourcedGenerator"
        p:format="urn:oasis:names:tc:SAML:2.0:nameid-format:persistent"
        p:attributeSourceIds="#{ {'ciscoUPN'} }" />
<bean parent="shibboleth.SAML2AttributeSourcedGenerator"
        p:format="urn:oasis:names:tc:SAML:2.0:nameid-format:persistent"
        p:attributeSourceIds="#{ {'ciscoUID'} }" />
```

### Метаданные IdP

Метаданные IdP доступны в папке **"$shibboleth_home/metadata"**. idp-metadata.xml файл может быть загружен к IdS через Прикладной программный интерфейс (API)

**PUT https://<idshost>: <idsport>/ids/v1/config/idpmetadata**

где **idsport** не является конфигурируемым объектом, и значение **"8553"**

> **% Warning:** Метаданные шибболета **могут** содержать 2 сертификата подписания, общий сертификат подписания и backchannel. Перейдите к файлу **idp-backchannel.crt** в **"$shibboleth_home/credentials"** для определения backchannel сертификата. Если сертификат обратного канала доступен в метаданных, необходимо удалить сертификат обратного канала из xml метаданных перед загрузкой на IdS. Это вызвано тем, что библиотека fedlet 12.0, что использование IdS поддерживает только один certifcate в метаданных. Если несколько сертификатов подписания доступны, fedlet использует первый доступный сертификат.

### Настройте поставщиков метаданных

Мы должны настроить поставщиков метаданных с записью в **$shibboleth_home/metadata-providers.xml.**

```
<bean parent="shibboleth.SAML2AttributeSourcedGenerator"
        p:format="urn:oasis:names:tc:SAML:2.0:nameid-format:persistent"
        p:attributeSourceIds="#{ {'ciscoUPN'} }" />
<bean parent="shibboleth.SAML2AttributeSourcedGenerator"
        p:format="urn:oasis:names:tc:SAML:2.0:nameid-format:persistent"
        p:attributeSourceIds="#{ {'ciscoUID'} }" />
```

где атрибут **"идентификатора"** может быть любым уникальным именем.

Эта запись указывает, что поставщик метаданных зарегистрирован в данном идентификаторе, и метаданные доступны в указанном файле /opt/shibboleth-idp/SP/sp.xml.

Метаданные Поставщика услуг (SP) IdS должны быть скопированы к метафайлу данных, заданному в записи.

> **Примечание:** Метаданные SP IdS могут быть получены через **GET https://<idshost>:**

**<idsport>/ids/v1/config/spmetadata,** где **idsport** не является конфигурируемым объектом и значением, **"8553".**

## Дальнейшая конфигурация для SSO

Этот документ описывает конфигурацию от аспекта IdP для SSO для интеграции с Идентификационным Сервисом Cisco. Для получения дальнейшей информации обратитесь к руководствам по конфигурации отдельного продукта:

- UCCX
- UCCE
- PCCE