Содержание

[Введение](#)
[Предварительные условия](#)
[Требования](#)
[Используемые компоненты](#)
[Условные обозначения](#)
[Обзор потока](#)
[Настройка](#)
[Шаг 1. Подготовьте ISE для использования внешнего Идентификационного Поставщика SAML](#)
[Шаг 2. Настройте Портал Спонсора для использования Внешнего Идентификационного Поставщика](#)
[Шаг 3. Настройте PingFederate как IdP для обработки Запросов аутентификации ISE](#)
[Шаг 4. Импортируйте метаданные IdP в ISE внешний профиль поставщика SAML IdP](#)
[Проверка](#)
[Устранение неполадок](#)
[Дополнительные сведения](#)

Введение

Этот документ описывает, как настроить сервер PingFederate SAML с платформой Cisco Identity Services Engine (ISE) 2.1 для обеспечения возможностей Единой точки входа (SSO) Спонсировать пользователей.

Предварительные условия

Требования

Компания Cisco рекомендует предварительно ознакомиться со следующими предметами:

- Гостевые сервисы Платформы Cisco Identity Services Engine.
- Базовые знания о развертываниях SSO SAML.

Используемые компоненты

Сведения, содержащиеся в данном документе, касаются следующих версий программного обеспечения и оборудования:

- Версия 2.1 Платформы Cisco Identity Services Engine
- Сервер PingFederate 8.1.3.0 от Идентичности Эхо-запроса.
- Windows Server 2012 R2 с Active Directory Services.

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,

удостоверьтесь, что вы понимаете потенциальное воздействие любых команд.

Условные обозначения

Более подробную информацию о применяемых в документе обозначениях см. в описании условных обозначений, используемых в технической документации Cisco

Обзор потока

Язык разметки утверждений безопасности (SAML) на основе XML стандарт для обмена данными проверки подлинности и авторизация между доменами защиты.

Спецификация SAML определяет три роли: Принципал (Спонсируют пользователя), Идентификационный Поставщик (IdP) (Эхо-запрос Федеративный сервер), и Поставщик услуг (SP) (ISE). В типичном потоке SSO SAML SP запрашивает и получает идентификационное утверждение из IdP. На основе этого результата ISE может выполнить решения о применении политики, поскольку IdP может включать конфигурируемые атрибуты, которые ISE может использовать во время решений о применении политики. Как только начальная аутентификация происходит, пользователю нельзя предложить для учетных данных снова обратиться к сервису, пока сеанс утверждения все еще активен на IdP.

Это - ожидаемый поток для этого варианта использования:

1. Пользователь пытается Войти к Порталу Спонсора путем запуска пользовательского полного доменного имени (FQDN) Портала настроенного Спонсора.
2. ISE проверяет, привязано ли там активное утверждение к этому клиенту? s сеанс через обозреватель путем запуска быстрого перенаправления к IdP. Если не будет никаких активных сеансов, то IdP принудит регистрационную информацию пользователя для входа.
3. IdP аутентифицирует Пользователя через LDAP и передает memberOf, и электронная почта приписывает ISE (SP).
4. ISE обрабатывает ответ IdP XML и на основе атрибута memberOf, и на конфигурации групп спонсора пользователю разрешат или отклонят (Проверка условия состава группы для соответствия с настроенной Sponsor Group).
5. Время сеанса для проживания будет варьироваться на каждом решении. В этом варианте использования Федеративный Эхо-запрос будет настроен с **Превышением времени ожидания сеанса** 60 минут (если не будет никаких запросов регистрации в системе SSO от ISE в 60 минут после того, как начальная аутентификация, сеанс удален), и **Сеанс Таймаут Max** 480 минут (Даже если IdP получал постоянные запросы регистрации в системе SSO от ISE для этого пользователя, сеанс истечет через 8 часов). Однажды времена сеанса, аутентификация нового пользователя принуждена IdP.
6. В то время как сеанс все еще активен, пользователь спонсора должен быть в состоянии закрыть браузер и возвращение к порталу, не вводя учетные данные.

Настройка

Следующий раздел обсудит действия настройки для интеграции ISE с Федеративным Эхо-запросом и как включить SSO браузера для Портала Спонсора.

Примечание: Несмотря на то, что различные варианты и возможности существуют при аутентификации пользователей спонсора, не, все комбинации описаны в этом документе. Однако данный пример предоставляет вам информацию, необходимую, чтобы понять, как модифицировать пример к точной конфигурации, которой вы хотите достигнуть.

Шаг 1. Подготовьте ISE для использования внешнего Идентификационного Поставщика SAML

1. На Cisco ISE перейдите к **администрированию> Управление идентификацией> Внешние Идентификационные Источники> Поставщики Идентификатора SAML**.
2. Нажмите кнопку Add
3. Под Вкладкой Общие введите имя Поставщика Идентификатора и нажмите **Save**. Остаток конфигурации в этом разделе будет зависеть от метаданных, которые должны быть импортированы из IdP.

Шаг 2. Настройте Портал Спонсора для использования Внешнего Идентификационного Поставщика

1. Перейдите для **Работы Центров>, Гостевой доступ> Настраивает> Порталы Спонсора**
2. Щелкните **по Sponsor Portal (по умолчанию)** или создайте новый портал.
3. Под **Настройками портала** вводят пользовательское полное доменное имя (FQDN), связанное с этим Порталом Спонсора.
4. Выберите от **Идентификационной Исходной Последовательности** Внешний SAML IdP, ранее определенный.

5. Проверьте, что блок-схема представляет следующее, и нажмите **Save**:

Шаг 3. Настройте PingFederate как IdP для обработки Запросов аутентификации ISE

1. Перейдите к **администрированию** ISE**> Управление идентификацией> Внешние Идентификационные Источники> Поставщики Идентификатора SAML>** PingFederate
2. Нажмите вкладку **Service Provider Info** и нажмите **Export**

3. Сохраните и извлеките генерируемый файл архива zip. XML-файл, содержавший здесь, будет использоваться при создании профиля в PingFederate.

4. Открытый портал PingFederate admin (как правило, https://ip:9999/pingfederate/app).

5. Под **Вкладкой конфигурация IDP>** раздел **Соединений SP** выбирают Create New.

6. Под **Типом соединения** нажимают **Next**

7. Под **Параметрами подключения** нажимают **Next**

8. Под **Метаданными Импорта** выберите **File**, файл Chose и выберите XML-файл, ранее экспортируемый от ISE.

9. В соответствии со **Сводкой Метаданных**, щелкните **по Next**.

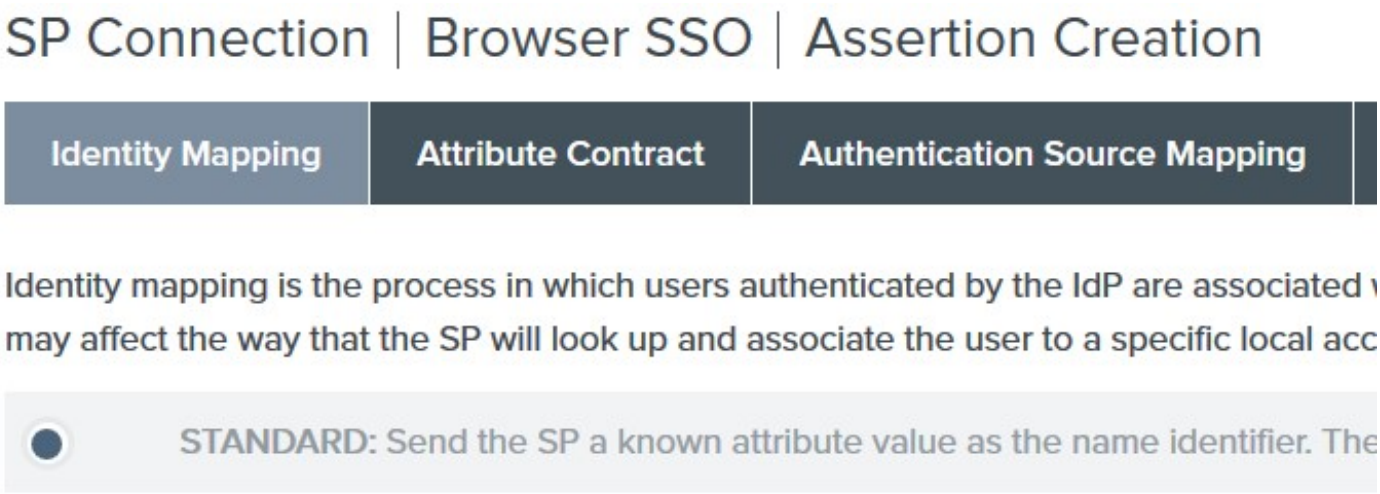
10. На Странице Общей информации, под **Именем соединения** вводят имя (ie. ISEsponsorPortal), и нажимают **Next**.

11. Под **Браузером SSO** нажимает **Configure Browser SSO**, и под **SAML Профили** проверяют эти опции и нажимают Next:

12. На **Утверждении Срок действия** нажимают **Next**

13. На **Утверждении Создание** нажимают **Configure Assertion Creation**

14. Под **Идентичностью Сопоставление** выбирает **Standard** и нажимает **Next**



15. По **Договору Атрибута> Продлевают Контракт**, вводят **почту** атрибутов, и **memberOf** и щелчок **добавляют. Нажмите кнопку Next.**

> **Примечание:** Это - критическое действие, поскольку ISE полагается на эти атрибуты для корректного сопоставления группы спонсора, и также пошлите по электронной почте, необходимо для корректных функций уведомления.

16. Под **Источником аутентификационной информации Сопоставление** нажимают **Map New Adapter Instance**.

17. На **Адаптере Экземпляр** выбирают **HTML Form Adapter**. **Нажмите кнопку Next.**

18. При **Сопоставлении Метода** выбирают вторую опцию и нажимают **Next**

19. На **Источниках Атрибута и Пользователе Поиск нажмите Add Исходную** коробку **Атрибута**.

20. Под **Хранилищем данных** вводят описание, затем выбирают от **Активного Хранилища данных** ваш экземпляр Соединения LDAP и определяют, какой Сервис каталогов это. Если нет никаких Хранилищ данных, настроенных, все же щелкают **по Manage Data Stores** для добавления нового экземпляра.

21. В соответствии с **Каталогом LDAP Поиск** определяет **Основной DN** для Поиска пользователя LDAP в домене и нажимает Next.

> **Примечание:** Это важно, поскольку это определит основной DN во время поиска

пользователя LDAP. Неправильно определенный Основной DN приведет к ошибке "Объект, Не найденный в схеме LDAP".

22. Под **LDAP Фильтр** добавляет строку **sAMAccountName= $ {имя пользователя}** и нажимает **Next**.

23. Под **Атрибутом Выполнение Договора** выбирает эти опции и нажимает **Next**

24. Проверьте конфигурацию в **Разделе Краткие выводы** и нажмите **Done**.

25. Назад в **Источниках Атрибута и Пользователе поиск** нажимают **Next**.

26. Под **Отказоустойчивым Атрибутом Источник** нажимают **Next**.

27. Под **Атрибутом Выполнение Договора** выбирает эти опции и нажимает **Next**:

27. Проверьте конфигурацию в **Разделе Краткие выводы** и нажмите **Done**.

28. Назад на **Источнике аутентификационной информации Сопоставление** нажимают **Next**.

29. Как только конфигурация была проверена под **Разделом Краткие выводы** , нажимают **Done**.

30. Назад на **Утверждении Создание** нажимают **Next**.

31. При **Параметрах протокола** нажимают **Configure Protocol Settings**.

На этом этапе должно быть 3 записи, уже заполненные. **Нажмите кнопку Next**

32. Под **Сервисными URL SLO** нажимают **Next**

33. На **Допустимом SAML Связывания** сняли флажок **с опциями ARTIFACT и SOAP** и нажимают **Next**.

34. Под **Подписью Политика** нажимают **Next**.

35. Под **Политикой шифрования** нажимают Next.

36. Рассмотрите конфигурацию в **Сводной странице** и нажмите **Done**.

37. Назад на **SSO Браузера> Параметры протокола нажимают Next**, проверяют конфигурацию и нажимают **Done**. Это возвратит вкладку **Browser SSO**. **Нажмите кнопку Next.**

38. Под **Учетными данными** нажимают **Configure Credentials** и выбирают сертификат подписания, который будет использоваться во время IdP к связи ISE и проверит **опцию Include сертификат в подписи**. **Нажмите кнопку Next.**

Примечание: Если нет никаких настроенных сертификатов, нажмите **Manage Certificates** и придерживайтесь приглашений для генерации Подписанного

сертификата, который будет использоваться для подписания IdP к связи ISE.

39. Проверьте конфигурацию под **Сводной страницей** и нажмите **Done**.

40. Назад на **Credentials** вкладка нажимают **Next**.

41. При **Активации и Сводке** выбирают на **Connection Status ACTIVE**, проверяют остаток конфигурации и нажимают **Save**.

Шаг 4. Импортируйте метаданные IdP в ISE внешний профиль поставщика SAML IdP

1. Под консолью управления PingFederate перейдите к **Конфигурации сервера> Административные функции> Экспорт Метаданных**, Если сервер был настроен для множественных ролей (IdP, и SP) выбирают опцию**, я - Идентификационный Поставщик (IdP). Нажмите кнопку Next**

2. Под **Метаданными** режим выбирают**? Выбрать Information to Include In Metadata Manually?. Нажмите кнопку Next.**

3. В соответствии с **Протоколом** нажимают **Next**.

4. На **Атрибуте Договор** нажимают **Next**.

5. Под **Ключом подписи** выбирают сертификат, ранее настроенный на профиле подключения . **Нажмите кнопку Next.**

6. Под **Метаданными Подписание** выбирает сертификат подписания, и проверка **Включают открытый ключ этого сертификата в ключевой информационный элемент. Нажмите кнопку Next.**

7. Под **XML сертификат шифрования** нажимают **Next**. Опция для осуществления шифрования вот до Сети Admin.

8. Под **Разделом Краткие выводы** нажимают генерируемый файл **Export Save the Metadata** и затем нажимают **Done**.

9. Под ISE Перейдите к **администрированию> Управление идентификацией> Внешние Идентификационные Источники> Поставщики Идентификатора SAML> PingFederate**.

10. Щелкните **по Identity Provider Config> Click Browse** и продолжите импортировать метаданные, сохраненные из операции Экспорта Метаданных Pingfederate.

11. Выберите **Groups Tab**, и под **Атрибутом Состава группы** добавляют **memberOf** и затем нажимают**, добавляют**

12. **Под именем в Утверждении** добавляют **Составное имя**, которое IdP должен возвращать назад, когда атрибут **memberOf** получен проверка подлинности LDAP формы. Эта группа будет связана с группой спонсора.

Как только вы добавляете DN и? Название в ISE? описание нажимает **OK**.

13. Выберите вкладку **Attributes** и **нажмите Add**. При этом шаге мы добавим атрибут**?**

почта?. Это содержится в аутентификации SAML; результат прошел от IdP (На основе почтового атрибута для того объекта пользователя в Active Directory).

> **Примечание:** Этот шаг важен, поскольку ISE должен быть в состоянии обработать электронную почту, связанную с сеансом Спонсора, чтобы быть в состоянии сопоставить любые учетные записи в состоянии ожидания от самозарегистрированных потоков. В противном случае учетные записи останутся в состоянии неопределенности, поскольку "человек, которого посещают" электронная почта, не будет сопоставлен с допустимым сеансом Спонсора. Это также важно для почтового уведомления, делает предложение.

14. Под **Вкладкой Дополнительно** выбирают следующие параметры настройки:

> **Примечание:** Этот раздел сообщит, что ISE для включения почтового атрибута в выход из системы запрашивает к IdP серверу. Когда Пользователь Спонсора вручную выходит из системы портала, это важно.

15. **Нажмите Save.**

16. В этом шаге администратор сопоставит Группу Active Directory, полученную IdP группе Спонсора. Перейдите для **Работы Центров>, Гостевой доступ> Настраивает> Sponsor Groups> ALL_ACCOUNTS** (Или выберите соответствующую группу). Нажмите **Members** и выберите **PingFederate:Group**, который мы сопоставили в предыдущих шагах, и добавьте его к столбцу Selected User Groups. **Затем нажмите кнопку ОК.**

17. Когда Сам Зарегистрированный поток будет настроен, учетные записи будут ожидать утверждение. В этом случае выберите**, "Утверждают и просматривают запросы от самозарегистрированных гостей?** и выберите**? Только учетные записи в состоянии ожидания, назначенные на этого спонсора?** поскольку простой способ для проверки Объектного Адреса электронной почты является AD и переданный Идентичности Спонсора в ISE через сервер IdP с помощью **Почтового** атрибута.

18. **Нажмите Save**. Это заканчивает конфигурацию в ISE.

Проверка

1. Запустите портал спонсора использование настроенного пользовательского FQDN. ISE должен перенаправить пользователя к порталу проверки подлинности пользователя PingFederate.

2. Введите учетные данные Active Directory и совершите нападки, Входят в систему. Экран входа в систему IdP перенаправит пользователя к начальному AUP на ISE? s Портал Спонсора.

На этом этапе у Пользователя Спонсора должен быть полный доступ к порталу.

3. Проверьте Единую точку входа. Когда? **Портала тестовый URL**? функцией является используемый ISE, должен попросить учетные данные Спонсора каждый раз, если SSO не настроен.

Запустите Портал Спонсора с Портала тестовой ссылкой URL. URL Спонсора ISE быстро

переключится к IdP URL для проверки статуса сеанса и как только маркер сеанса подтвержден, клиент перенаправлен назад к Порталу Спонсора без потребности ввода учетных данных.

4. Проверьте, что почтовый атрибут передают правильно от Объекта Active Directory до IdP к ISE. Самый легкий способ протестировать путем создания новой учетной записи в Портале Спонсора и выбора **Опции Notify**. Если электронная почта будет получена правильно, то это появится под полем **адреса электронной почты** Спонсора.

5. Функция **Verify Logout**. Это крайне важно для интеграции, чтобы проверить, что выход из системы спонсора инициирует Маркерный Сеанс, который будет завершен на Идентификационной Стороне сервера. Знак из Портала Спонсора и удостоверяется, что в следующий раз пользователь пытается обратиться к порталу спонсора, это будет перенаправлено назад к экрану аутентификации IdP.

Устранение неполадок

Любая транзакция аутентификации SAML будет зарегистрирована в стороне ISE под **ise-psc.log**. Существует специализированный компонент **(SAML)** при **администрировании> Регистрация>, Конфигурация Журнала Отладки>** Выбирает рассматриваемый узел> Набор компонент **SAML** к **уровню отладки**.

Мы можем обратиться к ISE через CLI и выполнить a? хвост ise-psc.log приложения show logging? и следите за развитием оперативных событий SAML, или мы можем загрузить **ise-psc.log** для дальнейшего анализа при **Операциях> Устранение неполадок>, Журналы Загрузки>** Выбирают узел ISE> вкладка **Debug Logs> ise-psc.log** щелчка для загрузки журналов.

Как правило, журнал Начальной аутентификации будет похож на это:

```
2016-06-13 10:18:58,560 DEBUG  [http-bio-14.36.157.210-8443-exec-7][]
cpm.saml.framework.impl.SAMLFacadeImpl -::::- SAML request -
spUrlToReturnTo:https://torsponsor21.rtpaaa.net:8443/sponsorportal/SSOLoginResponse.action2016-
06-13 08:39:36,925 DEBUG  [http-bio-14.36.157.210-8443-exec-7][]
cpm.saml.framework.impl.SAMLFacadeImpl -::::- SAML Response:
statusCode:urn:oasis:names:tc:SAML:2.0:status:Success2016-06-13 08:39:36,925 DEBUG  [http-bio-
14.36.157.210-8443-exec-7][] cpm.saml.framework.impl.SAMLAttributesParser -::::-
[parseAttributes] Found attribute name : mail2016-06-13 08:39:36,925 DEBUG  [http-bio-
14.36.157.210-8443-exec-7][] cpm.saml.framework.impl.SAMLAttributesParser -::::-
[parseAttributes] Delimeter not configured, Attribute=<mail> add
value=<antontor@rtpaaa.net>2016-06-13 08:39:36,925 DEBUG  [http-bio-14.36.157.210-8443-exec-7][]
cpm.saml.framework.impl.SAMLAttributesParser -::::- [parseAttributes] Found attribute name :
memberOf2016-06-13 08:39:36,925 DEBUG  [http-bio-14.36.157.210-8443-exec-7][]
cpm.saml.framework.impl.SAMLAttributesParser -::::- [parseAttributes] Delimeter not configured,
Attribute=<memberOf> add value=<CN=TOR,DC=rtpaaa,DC=net>
```

После события первоначального входа в систему каждый раз пользователь обращается к порталу спонсора мы? ll видит, что ISE получает информацию об утверждении, чтобы проверить, что маркер все еще активен. Результат должен быть похожим на это:

```
2016-06-13 10:18:58,560 DEBUG  [http-bio-14.36.157.210-8443-exec-7][]
cpm.saml.framework.impl.SAMLFacadeImpl -::::- SAML request -
spUrlToReturnTo:https://torsponsor21.rtpaaa.net:8443/sponsorportal/SSOLoginResponse.action2016-
06-13 08:39:36,925 DEBUG  [http-bio-14.36.157.210-8443-exec-7][]
cpm.saml.framework.impl.SAMLFacadeImpl -::::- SAML Response:
```

statusCode:urn:oasis:names:tc:SAML:2.0:status:**Success**2016-06-13 08:39:36,925 DEBUG [http-bio-14.36.157.210-8443-exec-7][] cpm.saml.framework.impl.SAMLAttributesParser -:::::- [parseAttributes] Found attribute name : **mail**2016-06-13 08:39:36,925 DEBUG [http-bio-14.36.157.210-8443-exec-7][] cpm.saml.framework.impl.SAMLAttributesParser -:::::- [parseAttributes] Delimeter not configured, Attribute=<mail> add value=<antontor@rtpaaa.net>2016-06-13 08:39:36,925 DEBUG [http-bio-14.36.157.210-8443-exec-7][] cpm.saml.framework.impl.SAMLAttributesParser -:::::- [parseAttributes] Found attribute name : **memberOf**2016-06-13 08:39:36,925 DEBUG [http-bio-14.36.157.210-8443-exec-7][] cpm.saml.framework.impl.SAMLAttributesParser -:::::- [parseAttributes] Delimeter not configured, Attribute=<memberOf> add value=<CN=TOR,DC=rtpaaa,DC=net>

Дополнительные сведения

Комментарии к выпуску для платформы Cisco Identity Services Engine, выпуска 2.1

Руководство администратора платформы Cisco Identity Services Engine, выпуск 2.1