Настройте гостевой ISE 2.1 портал с PingFederate SAML SSO

Содержание

Введение

Этот документ описывает, как настроить платформу Cisco Identity Services Engine (ISE) версия 2.1 для обеспечения возможностей Единой точки входа (SSO) гостевых пользователей портала через Язык разметки утверждений безопасности (SAML).

Предварительные условия

Требования

Компания Cisco рекомендует предварительно ознакомиться со следующими предметами:

- Гостевые сервисы Платформы Cisco Identity Services Engine.
- Базовые знания о 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 как Идентификационный Поставщик SAML (IdP)

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 любой примененной конфигурации.

Обзор потока

SAML на основе XML стандарт для обмена данными проверки подлинности и авторизация между доменами защиты.

Спецификация SAML определяет три роли: Принципал (Гость), Идентификационный Поставщик [IdP] (IPing 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 (т.е. Группа и адрес электронной почты, привязанный к объекту AD).

Ожидаемый Поток для этого Варианта использования

1. Контроллер беспроводной локальной сети (WLC) или Коммутатор доступа настроены для типичного потока Центральной веб-аутентификации (CWA).

   Совет: Найдите примеры конфигурации для потоков CWA в Разделе связанных сведений у основания статьи.

2. Клиентские подключения и сеанс аутентифицируются против ISE. Устройство доступа к сети (NAD) применяется, атрибуты перенаправления оценивают пар (AVP), возвращенные ISE (acl перенаправления URL и перенаправление URL).

3. Клиент открывает браузер, генерирует трафик HTTP или Трафик HTTPS, и перенаправлен к Гостевому Порталу ISE.

4. Однажды в портале клиент будет в состоянии ввести ранее назначенные гостевые учетные данные (**Созданный Спонсор**) и самонастроить новую гостевую учетную запись или использовать ее AD учетные данные для регистрации (**Вход в систему Сотрудника**), который предоставит возможности Единой точки входа через SAML.

5. Как только пользователь выбирает опцию “Входа в систему Сотрудника”, ISE проверяет, существует ли активное утверждение, привязанное к сеансу через обозреватель этого клиента против IdP. Если не будет никаких активных сеансов, то IdP принудит регистрационную информацию пользователя для входа. При этом шаге пользователю предложат ввести AD учетные данные в портал IdP непосредственно.

6. IdP аутентифицирует пользователя через LDAP, и это создает новое Утверждение, которое останется в живых в течение настраиваемого времени.

Примечание: Эхо-запрос, Федеративный по умолчанию, применяет **Превышение времени ожидания сеанса** 60 минут (это означает, что, при отсутствии запросов регистрации в системе SSO от ISE через 60 минут после начальной аутентификации, сеанс удален), и **Сеанс Таймаут Max** 480 минут (даже если IdP получил постоянные запросы регистрации в системе SSO от ISE для этого пользователя, сеанс истечет через 8 часов).

Пока сеанс Утверждения все еще активен, Сотрудник испытает SSO, когда он будет использовать Гостевой Портал. Однажды времена сеанса, аутентификация нового пользователя будет принуждена IdP.

Настройка

В этом разделе рассматриваются действия настройки для интеграции ISE с Федеративным Эхо-запросом и как включить SSO Браузера для Гостевого Портала.

Примечание: Несмотря на то, что различные варианты и возможности существуют при аутентификации Гостей, 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 выберите **Administration> Identity Management> External Identity Sources> SAML Id Providers**.
2. **Нажмите Add.**
3. Под Вкладкой **Genaral** введите **Имя Поставщика Идентификатора**. **Нажмите Save** . Остаток конфигурации в этом разделе зависит от метаданных, которые должны быть импортированы из IdP в более поздних шагах.

Шаг 2. Настройте Гостевой портал для использования внешнего Идентификационного Поставщика

1. Выберите **Work Centers> Guest Access> Configure> Guest Portals.**
2. Создайте новый портал и выберите **Self-Registered Guest Portal**.

Примечание: Это не будет основным порталом, что пользовательский опыт, но подпортал, который будет взаимодействовать с IdP для проверки статуса сеанса. Этот портал называют SSOSubPortal.

3. Разверните **Настройки портала** и выберите **PingFederate for Authentication Method**.

4. От **Идентификационной Исходной Последовательности** выберите, External SAML IdP ранее определил (PingFederate).

5. Разверните **политику допустимого использования (AUP)** и разделы **Параметров настройки Страницы Постбаннера входа в систему** и отключите обоих.

Портала поток:

6. Сохраните изменения.

7. Вернитесь к Гостевым Порталам и создайте новый с помощью **Самозарегистрированного Гостевого Параметра портала.**

> **Примечание:** Это будет Основным порталом, видимым клиенту. Основной портал будет использовать SSOSubportal в качестве интерфейса между ISE и IdP. Этот портал называют PrimaryPortal.

8. Разверните **Параметры настройки Страницы входа** и выберите**, SSOSubPortal**, созданный на предыдущем этапе под "**, Позволяют следующему гостевому порталу идентификационного поставщика использоваться для входа в систему**".

9. Разверните **AUP политики допустимого использования и Параметры настройки Страницы Постбаннера входа в систему** и снимите флажок с ними.

На этом этапе портала поток должен быть похожим на это:

10. Выберите **Portal Customization> Pages> Login**. У вас должна теперь быть опция для настройки **Альтернативных Опций Входа в систему** (Значок, текст, и так далее).

> **Примечание:** Заметьте, что на правой части, под портала предварительным просмотром, дополнительная опция входа в систему видима.

11. **Нажмите Save.**

Теперь оба портала появляются под Гостевым Списком Портала.

Шаг 3. Настройте PingFederate для действия как Идентификационный Поставщик для Гостевого Портала ISE

1. В ISE выберите **Administration> Identity Management> External identity Sources> SAML Id Providers> PingFederate** и нажмите **Service Provider Info.**
2. Под **Информацией Поставщика услуг Экспорта** нажмите **Export.**

3. Сохраните и извлеките генерируемый файл архива zip. XML-файл, содержавший здесь , используется для создания профиля в PingFederate в более поздних шагах.

> **Примечание:** С этого момента этот документ покрывает конфигурацию PingFederate. Эта конфигурация - то же для множественных решений как портал Спонсора, MyDevices и порталы BYOD. (Те решения не охвачены в этой статье).

4. Откройте 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** нажмите **Next.**

7. Под **Параметрами подключения** нажмите **Next.**

8. Под **Метаданными Импорта** нажмите кнопку с зависимой фиксацией **File**, нажмите **файл Chose** и выберите XML-файл, ранее экспортируемый от ISE.

9. В соответствии со **Сводкой Метаданных**, нажмите **Next**.

10. На странице General Info, под Именем соединения, вводят имя (такое как ISEGuestWebAuth) и нажимают **Next**.

11. Под **SSO Браузера** нажмите **Configure Browser SSO**, и под **SAML Профили** проверяют 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.**

Конфигурация этой опции позволяет Идентификационному Поставщику передавать **MemberOf** и **Почтовые** атрибуты, предоставленные Active Directory ISE, который ISE может использовать позже в качестве условия во время решения о применении политики.

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 методов** выбирают вторую опцию вниз и нажимают **Next.**

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

20. Под **Хранилищем данных** вводят описание, и выбирают экземпляр соединения LDAP из **Активного Хранилища данных** и определяют, какой Сервис каталогов это. Если нет никаких **Хранилищ данных**, настроенных, все же нажимают **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 Объекту, Не найденному в схеме LDAP.

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

23. Под **Атрибутом Выполнение Договора** выбирает данные 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.**

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

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

30. Как только конфигурация была проверена под **Сводной страницей**, нажимают **Done**.

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

32. При **Параметрах протокола** нажмите **Configure Protocol Settings**. На этом этапе должно быть две записи, уже заполненные. **Нажмите кнопку Next.**

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

34. На Допустимых Связываниях SAML снимите флажок с опциями ARTIFACT и SOAP и нажмите **Next.**

35. Под Подписью Политика нажимают **Next**.

36. Под Политикой шифрования нажимают **Next**.

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

38. Назад на SSO Браузера> Параметры протокола **нажимают Next**, проверяют конфигурацию и нажимают **Done**.

39. Вкладка SSO браузера появляется. **Нажмите кнопку Next.**

40. 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, нажимают **Manage Certificates** и придерживаются приглашений для генерации **Подписанного сертификата**, который будет использоваться для подписания IdP к связи ISE.

41. Проверьте конфигурацию под сводной страницей и нажмите **Done**.

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

43. При **Активации и Сводке** выбирают **Connection Status ACTIVE**, проверяют остаток конфигурации и нажимают **Done**.

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

1. Под консолью управления PingFederate выберите **Server Configuration> Administrative Functions> Metadata Export.** Если сервер был настроен для множественных ролей (IdP и SP), выберите опцию**, я - Идентификационный Поставщик (IdP). Нажмите кнопку Next.**
2. Под **Метаданными** режим выбирают **“Select 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**.

Примечание: Опция для осуществления шифрования вот до Сети Admin.

8. Под **Разделом Краткие выводы** нажимают **Export**. Сохраните генерируемый файл Метаданных и затем нажмите **Done**.

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

10. Нажмите **Identity Provider Config> Browse** и продолжите импортировать метаданные, сохраненные из операции Экспорта Метаданных PingFederate.

11. Вкладка **Choose Groups**, под **Атрибутом Состава группы** добавляют **memberOf** и затем **нажмите Add**

Под именем в Утверждении добавляют Составное имя, которое должен возвратить **IdP** , когда атрибут **memberOf** получен форма аутентификация LADP. В этом случае группа настроила , связан с группой спонсора TOR, и DN для этой группы следующие:

Как только вы добавляете, что DN и “Название в ISE” описание нажимают **OK**.

12. Выберите вкладку **Attributes** и **нажмите Add**.

При этом шаге добавьте атрибут “почта”, которая содержится в маркере SAML, который передают от IdP, что на основе запроса Пина по LDAP, это должно содержать почтовый атрибут для того объекта.

Примечание: Шаги 11 и 12 гарантируют, что ISE получает атрибуты Электронного письма и MemberOf объекта AD посредством действия входа в систему IdP.

Проверка

1. Запустите Гостевой Портал использование Портала Тестового URL или следующим поток CWA. У пользователя будут опции, чтобы ввести гостевые учетные данные, создать их собственную учетную запись и Вход в систему Сотрудника.

2. Нажмите **Employee Login**. С тех пор нет никаких Активных сеансов, пользователь будет перенаправлен к порталу входа в систему IdP.

3. Введите AD учетные данные и нажмите **Sign On**.

4. Экран входа в систему IdP перенаправит пользователя к Гостевой Странице Успеха Портала.

5. На этом этапе каждый раз пользователь возвращается к Гостевому Порталу, и выберите **"Employee Login"**, который им разрешат в сети, пока Сеанс все еще активен в IdP.

Устранение неполадок

Любая проблема аутентификации SAML будет зарегистрирована под ise-psc.log. Существует специализированный компонент (SAML) при **администрировании> Регистрация>, Отладка регистрирует Конфигурацию>, Выбирают рассматриваемый узел>** Набор компонент SAML к **уровню отладки**.

Можно обратиться к ISE через CLI и ввести **хвост ise-psc.log приложения команды show logging** и следить за развитием событий SAML, или можно 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.

```
2016-06-27 16:15:39,366 DEBUG  [http-bio-14.36.157.210-8443-exec-3][]
cpm.saml.framework.impl.SAMLFacadeImpl -:::::- SAMLUtils::isOracle() - checking whether IDP URL
indicates that its OAM. IDP URL: https://14.36.147.1:9031/idp/sso.saml2
2016-06-27 16:15:39,366 DEBUG  [http-bio-14.36.157.210-8443-exec-3][]
cpm.saml.framework.impl.SAMLFacadeImpl -:::::- SPProviderId for PingFederate is: http://CiscoISE
/5b4c0780-2da2-11e6-a5e2-005056a15f11
2016-06-27 16:15:39,366 DEBUG  [http-bio-14.36.157.210-8443-exec-3][]
cpm.saml.framework.impl.SAMLFacadeImpl -:::::- ResponseValidationContext:
        IdP URI: PingFederate
        SP URI: http://CiscoISE/5b4c0780-2da2-11e6-a5e2-005056a15f11
        Assertion Consumer URL: https://14.36.157.210:8443/portal/SSOLoginResponse.action
        Request Id: _5b4c0780-2da2-11e6-a5e2-005056a15f11_DELIMITERportalId_EQUALS5b4c0780-2da2-
11e6-a5e2-005056a15f11_SEMIportalSessionId_EQUALS309f733a-99d0-4c83-8
b99-2ef6b76c1d4b_SEMI_DELIMITER14.36.157.210
        Client Address: 14.0.25.62
        Load Balancer: null
2016-06-27 16:15:39,366 DEBUG  [http-bio-14.36.157.210-8443-exec-3][]
cpm.saml.framework.validators.BaseSignatureValidator -:::::- Determine the signing certificate
2016-06-27 16:15:39,366 DEBUG  [http-bio-14.36.157.210-8443-exec-3][]
cpm.saml.framework.validators.BaseSignatureValidator -:::::- Validate signature to SAML standard
with cert:CN=14.36.147.1, OU=TAC, O=Cisco, L=RTP, C=US serial:1465409531352
2016-06-27 16:15:39,367 DEBUG  [http-bio-14.36.157.210-8443-exec-3][]
org.opensaml.xml.signature.SignatureValidator -:::::- Creating XMLSignature object
2016-06-27 16:15:39,367 DEBUG  [http-bio-14.36.157.210-8443-exec-3][]
org.opensaml.xml.signature.SignatureValidator -:::::- Validating signature with signature
algorithm URI: http://www.w3.org/2001/04/xmldsig-more#rsa-sha256
```

```
2016-06-27 16:15:39,368 DEBUG  [http-bio-14.36.157.210-8443-exec-3][]
cpm.saml.framework.validators.SAMLSignatureValidator -::::- Assertion signature validated
succesfully
2016-06-27 16:15:39,368 DEBUG  [http-bio-14.36.157.210-8443-exec-3][]
cpm.saml.framework.validators.WebSSOResponseValidator -::::- Validating response
2016-06-27 16:15:39,368 DEBUG  [http-bio-14.36.157.210-8443-exec-3][]
cpm.saml.framework.validators.WebSSOResponseValidator -::::- Validating assertion
2016-06-27 16:15:39,368 DEBUG  [http-bio-14.36.157.210-8443-exec-3][]
cpm.saml.framework.validators.AssertionValidator -::::- Assertion issuer succesfully validated
2016-06-27 16:15:39,368 DEBUG  [http-bio-14.36.157.210-8443-exec-3][]
cpm.saml.framework.validators.AssertionValidator -::::- Subject succesfully validated
2016-06-27 16:15:39,368 DEBUG  [http-bio-14.36.157.210-8443-exec-3][]
cpm.saml.framework.validators.AssertionValidator -::::- Conditions succesfully validated
2016-06-27 16:15:39,368 DEBUG  [http-bio-14.36.157.210-8443-exec-3][]
cpm.saml.framework.impl.SAMLFacadeImpl -::::- SAML Response: validation succeeded for guest
IDPResponse
:
        IdP ID: PingFederate
        Subject: guest
        SAML Status Code:urn:oasis:names:tc:SAML:2.0:status:Success
        SAML Success:true
        SAML Status Message:null
        SAML email:guest@rtpaaa.net
        SAML Exception:null
2016-06-27 16:15:39,368 DEBUG  [http-bio-14.36.157.210-8443-exec-3][]
cpm.saml.framework.impl.SAMLFacadeImpl -::::- AuthenticatePortalUser - about to call
authenticateSAMLUser messageCode:null subject:guest
2016-06-27 16:15:39,375 DEBUG  [http-bio-14.36.157.210-8443-exec-3][]
cpm.saml.framework.impl.SAMLFacadeImpl -::::- Authenticate SAML User - result:PASSED
```

Дополнительные сведения

- Центральная веб-аутентификация с WLC Cisco и примером конфигурации ISE.
- Центральная веб-аутентификация с коммутатором и примером конфигурации платформы Identity Services Engine.
- Комментарии к выпуску для платформы Cisco Identity Services Engine, выпуска 2.1
- Руководство администратора платформы Cisco Identity Services Engine, выпуск 2.1