Версия 10.5 Unity Connection пример конфигурации SSO SAML

ID документа: 118772

Обновлено : 21 января 2015

Внесенный А.М.Мэхешем Бэбу, специалистом службы технической поддержки Cisco.

Родственные продукты

- Cisco Unity Connection
- CISCO UNIFIED COMMUNICATIONS MANAGER (CALLMANAGER)

Содержание

Введение

Этот документ описывает, как настроить и проверить Единую точку входа (SSO) Языка разметки утверждений безопасности (SAML) для Cisco Unity Connection (UCXN).

Предварительные условия

Требования

Настройка протокола NTP

Для SSO SAML для работы необходимо установить корректную настройку NTP и удостовериться, что разница во времени между Идентификационным Поставщиком (IdP) и Унифицированными коммуникационными приложениями не превышает три секунды. Для получения информации о синхронизирующихся часах посмотрите раздел Параметров настройки NTP в Руководстве по администрированию Операционной системы Унифицированной связи Cisco.

Настройка сервера доменных имен (DNS)

Унифицированные коммуникационные приложения могут использовать DNS для решения Полных доменных имен (FQDNs) к IP-адресам. Поставщики услуг и IdP должны быть разрешимыми браузером.

Сервис Федерации Active Directory (AD FS) Версия 2.0 должна быть установлена и настроена для обрабатывания запросов SAML.

Используемые компоненты

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

- AD версия 2.0 FS как IdP
- UCXN как поставщик услуг
- Версия Microsoft Internet Explorer 10

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.

Общие сведения

SAML на основе XML, формат данных открытого стандарта для обмена данными. Это - протокол аутентификации, используемый Поставщиками услуг для аутентификации пользователя. Информацию об аутентификации безопасности передают между IdP и Поставщиком услуг.

SAML является открытым стандартом, который позволяет клиентам аутентифицировать против любой поддерживающей SAML совместной работы (или Объединенные

коммуникации) сервис независимо от платформы клиента.

Все веб-интерфейсы Объединенных коммуникаций Cisco, такие как Cisco Unified Communications Manager (CUCM) или UCXN, используют протокол Версии 2.0 SAML в функции SSO SAML. Для аутентификации пользователя Протокола LDAP UCXN делегирует запрос аутентификации к IdP. Этим запросом аутентификации, генерируемым UCXN, является Запрос SAML. IdP аутентифицирует и возвращает Утверждение SAML. Утверждение SAML показывает или Да (аутентифицируемый) или No (подведенная аутентификация).

SSO SAML позволяет пользователю LDAP входить в клиентские приложения с именем пользователя и паролем, которое аутентифицируется на IdP. Пользовательский вход в систему к любому из поддерживаемых web - приложений на продуктах Объединенных коммуникаций после активации опции SSO SAML также получает доступ к этим web - приложениям на UCXN (кроме CUCM и IM CUCM и Присутствия):

Пользователи Unity Connection	Web - приложения
Пользователи LDAP с правами администратора	• Администрирование UCXN • Cisco удобство обслуживания UCXN • Cisco унифицированное удобство обслуживания • Личный помощник по связи Cisco • Веб-папка "Входящие" • Мини-веб-Папка "Входящие" (версия для настольно компьютера)
Пользователи LDAP без прав администратора	• Личный помощник по связи Cisco • Веб-папка "Входящие" • Мини-веб-Папка "Входящие" (версия для настольно компьютера) • Клиенты Cisco Jabber

Настройка

Схема сети

Установка каталога

1. Знак в Страницу администратора UCXN и выбирает **LDAP** и нажимает **LDAP Setup**.

2. Проверка **Позволяет Синхронизироваться от Сервера LDAP** и нажимает **Save**.

3. Нажмите **LDAP**.

4. Нажмите **LDAP Directory Configuration**.

5. **Нажмите Добавить нов.**

6. Настройте эти элементы:

   Настройки учетной записи каталога LDAPАтрибуты пользователя, которые будут синхронизироватьсяСписок синхронизацииИмя хоста сервера LDAP или IP-адрес и номер порта

7. Проверьте **SSL Использования**, если вы хотите использовать Протокол SSL для передачи с каталогом LDAP.

   Совет: Если вы настраиваете LDAP через SSL, загружаете сертификат каталога LDAP на CUCM. См. содержание каталога LDAP в Cisco Unified Communications Manager SRND для получения информации о механизме синхронизации учетной записи для определенных продуктов LDAP и общих оптимальных методах для синхронизации LDAP.

8. Нажмите **Perform Full Sync Now**.

   Примечание: Удостоверьтесь, что сервис **Cisco DirSync** включен в веб-странице Удобства обслуживания перед нажатием Save.

9. Разверните **Пользователей** и выберите **Import Users**.

10. В **Менеджере Унифицированной связи Находки** список **Конечных пользователей** выберите **LDAP Directory**.

11. Если вы хотите импортировать только подмножество пользователей в каталоге LDAP, с которым вы интегрировали UCXN, введите применимые спецификации в поля поиска.

12. Выберите **Find**.

13. В На основе списка Шаблона, выберите **шаблон Администратора**, который вы хотите, чтобы UCXN использовал, когда это создает выбранных пользователей.

    Внимание. : Если вы зададите шаблон администратора, то у пользователей не будет почтовых ящиков.

14. Проверьте флажки для пользователей LDAP, для которых вы хотите создать пользователей UCXN и нажать **Import Selected**.

Включите SSO SAML

1. Войдите в интерфейс пользователя администрирования UCXN.

2. Выберите **System>, SAML Single Sign-on** и SAML SSO Configuration window открываются.

3. Для включения SSO SAML на кластере нажмите **Enable SAML SSO**.

4. В Окне предупреждения Reset нажмите **Continue.**

5. На экране SSO нажмите **Browse** для импорта XML-файла метаданных **FederationMetadata.xml** с **Загрузкой** шаг **Метаданных Idp**.

6. Как только файл метаданных загружен, нажмите **Import IdP Metadata** для импорта информации о IdP к UCXN. Подтвердите, что импорт был успешен, и нажмите **Next** для продолжения.

7. Нажмите **Download Trust Metadata Fileset** (сделайте это, только если вы уже не настроили ADFS с Метаданными UCXN), чтобы сохранить метаданные UCXN к локальному каталогу и перейти , Добавляют UCXN как Передающий Партийное Доверие. Как только AD конфигурация FS завершена, продолжитесь к Шагу 8.

8. Выберите **SSO** как административного пользователя и нажмите **Run SSO Test**.

9. Проигнорируйте Предупреждения Сертификата и продолжитесь далее. Когда вам предложат для учетных данных, введите пользовательское имя пользователя и пароль SSO и нажмите **OK**.

   Примечание: Этот пример конфигурации основывается на UCXN и AD подписанных сертификатах FS. В случае, если вы используете сертификаты Центра сертификации (CA), соответствующие сертификаты должны быть установлены и на AD FS и на UCXN. См. Управление сертификатами и Проверку для получения дополнительной информации.

10. После того, как все шаги завершены, вы получаете "Следовавший Тест SSO!"

сообщение. Нажмите **Close** и **Finish** для продолжения.

Вы теперь успешно завершили задачи конфигурации для включения SSO на UCXN с AD FS.

Обязательный Примечание: Запущенный Тест SSO для Абонента UCXN, если это - кластер для включения SSO SAML. AD FS должен быть настроен для всех узлов UCXN в кластере.

Совет: Если вы настроите XML-файлы метаданных всех узлов на IdP, и вы начинаете включать операцию SSO на одном узле, то SSO SAML будет включен на всех узлах в кластере автоматически.

Если вы хотите использовать SSO SAML для Клиентов Cisco Jabber и дать истинный опыт SSO конечным пользователям, можно также настроить CUCM и IM CUCM и Присутствие для SSO SAML.

Проверка

Откройте web-браузер и введите FQDN UCXN, и вы видите новую опцию в соответствии с Установленными Приложениями под названием **URL Восстановления для обхода Единой точки входа (SSO)**. Как только вы щелкаете по ссылке **Cisco Unity Connection**, вам предлагает для учетных данных AD FS. После ввода пользовательских учетных данных SSO вы будете успешно зарегистрированы в страницу Unity Administration, Унифицированную страницу Serviceability.

Примечание: SSO SAML не включает доступ к этим страницам:
- Главное лицензирование менеджера
- Администрирование ОС
- Система Восстановления после отказа

Устранение неполадок

Для этой конфигурации в настоящее время нет сведений об устранении проблем.

См. Устранение проблем SSO SAML для продуктов Совместной работы 10.x для получения дополнительной информации.

Соответствующие дискуссии сообщества технической поддержки Cisco

Сообщество технической поддержки Cisco является форумом, в котором можно задавать вопросы и получать ответы, обмениваться предложениями и сотрудничать со своими равноправными коллегами.

См. Условные обозначения технических советов Cisco для получения информации по условным обозначениям, которые используются в данном документе.

Обновлено : 21 января 2015
ID документа: 118772