Устранение проблем ADFS/IdS и Типичные проблемы

Содержание

Введение

Взаимодействие Языка разметки утверждений безопасности (SAML) между Идентификационным Сервисом Cisco (ИДЕНТИФИКАТОРЫ) и Active Directory Federation Services (AD FS) через браузер является ядром Единой точки входа (SSO), входят в поток. Этот документ поможет вам в отладке проблем, отнесенных к конфигурациям в Cisco

IDS и AD FS, наряду с рекомендованным действием решать их.

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 11.5 или Выпуск 11.5 Cisco Unified Contact Center Enterprise или Упакованное предприятие Contact Center (PCCE) Выпуск 11.5 как применимый.
- Microsoft Active Directory - AD установлен на Windows Server
- IdP (идентификационный поставщик) - сервис федерации Active Directory (AD FS) версия 2.0/3.0

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 этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Общие сведения

После того, как доверительные отношения установлены между Cisco IDS и AD FS (см. здесь для подробных данных, характерных для UCCX и UCCE), администратор, как ожидают, выполнит Тестовый SSO, Установленный в Странице настроек Идентификационного управления службами, чтобы гарантировать, что хорошо работает конфигурация между Cisco IDS и AD FS. Если тест отказывает, используйте подходящие приложения и предложения, данные в этом руководстве для решения вопроса.

Приложения и журналы, которые могут быть удобными в отладке

Приложение/Журнал	Подробные данные	Где найти программное средство
Журнал Cisco IDS	Регистратор Cisco IDS	Используйте RTMT для получения журнало

	регистрирует любую ошибку, которая произошла в Cisco IDS.	Cisco IDS. Для получения информации о то как использовать RTMT, посмотрите, Руководство для Использования RTMT Обратите внимание на то, что название RT является **Идентификационным Сервисом Cisco**. Для обнаружения журналов перейди **Идентификационному Сервису Cisco> журн**
Журналы Fedlet	Журналы Fedlet дадут больше подробных данных о любых ошибках SAML, который происходит в Cisco IDS	Используйте RTMT для получения журнало Fedlet. Местоположение для журнала Fedlet - то же как журналы Cisco IDS. Журналы fedlet запускаются с префикса **fed**
Метрики API Cisco IDS	Метрики API могут использоваться, чтобы изучить и проверить любые ошибки, которые API Cisco IDS, возможно, возвратили и количество запросов, которые обработаны Cisco IDS	Используйте RTMT для получения метрик A Обратите внимание на то, что название RT является **Идентификационным Сервисом C** Это появится под отдельной папкой **метрик** Обратите внимание на то, что **saml_metrics.** и **authorize_metrics.csv** являются соответствующими метриками для этого документа.
Просмотр событий в AD FS	Позволяет пользователям просматривать журналы событий в системе. Любая ошибка в AD FS при обработке SAML запрашивает/передает, чтобы ответ SAML был зарегистрирован здесь.	В AD машине FS перейдите **Просмотру событий> Приложения** и **Журналы Сервисо AdDFS 2.0> Admin** В Windows 2008, Просмотре событий запус от **Панели управления> Производительност Обслуживание> Средства администрирова** В Windows 2012, запуск это от Контроля Panel\System и Программные средства Security\Administrative. Посмотрите на свою документацию по Windows для наблюдения, где найти Просм событий.
Средство просмотра SAML	Средство просмотра SAML поможет в рассмотрении Запроса SAML и Ответа, которые передаются от/к Cisco IDS. Этот обозреватель очень полезен для анализа Запроса/Ответа SAML.	Это, некоторые предложили средства просмотра SAML, которые можно использовать для рассмотрения запроса SA и ответа 1. Скрипач Как использовать скрипача с FSСкрипач плагин Chrome 2. Трассировщик SAML - Firefox 3. SAML панель Chrome

Блок-схема с Параметрами отладки

Различные шаги для аутентификации SSO показывают в образе наряду с и артефактах отладки при каждом шаге в случае сбоя в том шаге.

Эта таблица дает подробные данные о том, как определить сбои при каждом шаге SSO в браузере. Другие программные средства и как может, они помогают в отладке, задан также.

Шаг	Как определить сбой в Браузере	Программные средства/Журнал	Конфигурации для взгляда на
Обработка запросов	В случае сбоя браузер не	Журналы Cisco IDS - Указывают на ошибки,	Клиентская регистрация

AuthCode Cisco IDS	перенаправлен к оконечной точке SAML или AD FS, ошибку JSON показывает Cisco IDS, который указывает, что URL Идентификатора клиента или Перенаправления недопустим.	которые происходят, в то время как запрос authcode проверен и обработан. Метрики API Cisco IDS - Указывают на количество запросов, обработанных и отказавших.	
Инициирование запроса SAML Cisco IDS	Во время сбоя браузер не перенаправлен к AD FS, и ошибочную страницу/сообщение покажет Cisco IDS.	Журналы Cisco IDS - Указывают, существует ли исключение или не, в то время как инициируется запрос. Метрики API Cisco IDS - Указывают на количество запросов, обработанных и отказавших.	Cisco IDS в состоянии NOT_CONFIGURED.
Обработка запросов SAML AD FS	Любой сбой для обработки этого запроса приведет к ошибочной странице, отображаемой AD сервером FS вместо страницы входа.	Просмотр событий в AD FS - Указывает на ошибки, которые происходят, в то время как обработан запрос. Плагин Браузера SAML - Помогает видеть запрос SAML, который отправлен к AD FS.	Полагающаяся партийная трастовая конфигурация в IdP
Передача ответа SAML AD FS	Любой сбой для передачи результатов ответа на ошибочной странице, отображаемой AD сервером FS после допустимых учетных данных, отправлен.	Просмотр событий в AD FS - Указывает на ошибки, которые происходят, в то время как обработан запрос.	• Полагающаяся партийная трастовая конфигурация в IdP • Сформируйте Настройку аутентификации в AD FS.
Обработка Ответа SAML Cisco IDS	Cisco IDS покажет 500 ошибок с причиной ошибки и страницей быстрой проверки.	Если AD FS передает ответ SAML без кода успешного состояния, просмотр событий в AD FS - Указывает на ошибку. Плагин Браузера SAML - Помогает видеть ответ SAML, передаваемый AD FS для определения что не так. Журнал Cisco IDS - Указывает , что ошибка/исключение произошла во время обработки. Метрики API Cisco IDS -	• Требование управляет конфигурацией • Сообщение и подписание утверждения

	Указывают на количество запросов, обработанных и отказавших.

Обработка запросов Authcode Cisco IDS

Отправная точка входа в систему SSO, до Cisco IDS затронута, запрос о коде авторизации из включенного приложения SSO. Проверка запроса API сделана, чтобы проверить, является ли это запрос от зарегистрированного клиента. Успешная проверка приводит к браузеру, перенаправляемому к оконечной точке SAML Cisco IDS. Любой сбой в проверке запроса приводит к ошибке page/JSON (Объектная нотация JavaScript) передаваемый обратно от Cisco IDS.

Распространенные ошибки, Встреченные во время этого Процесса

1. Клиентская регистрация, не сделанная

Краткое описание проблемы	Запрос регистрации в системе отказывает с 401 ошибкой на браузере.
	Браузер:
	401 ошибка с этим сообщением: Ошибка: "invalid_client", "error_description": "Недоп
	Журнал Cisco IDS:
	`2016-09-02 00:16:58.604 IST(+0530) [IdSEndPoints-51] WARN com.cisco.ccbu.ids IdSConfig`
	`fb308a80050b2021f974f48a72ef9518a5e7ca69 does not exist 2016-09-02 00:16:58.604 IST(+0`
	`ERROR com.cisco.ccbu.ids IdSOAuthEndPoint.java:45 - Exception processing auth request.`
	`org.apache.oltu.oauth2.common.exception.OAuthProblemException: invalid_client, Invalid`
	`org.apache.oltu.oauth2.common.exception.OAuthProblemException.error(OAuthProblemExcept`
	`com.cisco.ccbu.ids.auth.validator.IdSAuthorizeValidator.validateRequestParams(IdSAutho`
	`com.cisco.ccbu.ids.auth.validator.IdSAuthorizeValidator.validateRequiredParameters(IdS`
	`at org.apache.oltu.oauth2.as.request.OAuthRequest.validate(OAuthRequest.java:63)`

Возможная причина	Клиентская регистрация с Cisco IDS не завершена.
Рекомендуемое действие	Перейдите к Консоли управления Cisco IDS и подтвердите, зарегистрирован ли кл противном случае тогда зарегистрируйте клиентов перед продолжением SSO.

2. Пользовательское Приложение Доступов с помощью IP-адреса / Альтернативное Имя хоста

Краткое описание проблемы	Запрос регистрации в системе отказывает с 401 ошибкой на браузере. **Браузер:** 401 ошибка с этим сообщением: Ошибка: "invalid_redirectUri", "error_description": "Инвлэлид Редирект Ури"} Пользователь обращается к приложению с помощью IP-адреса / Альтернативное Имя хоста.
Возможная причина	В режиме SSO, если к приложению обращаются с помощью IP, оно не работает. К приложениям должно обратиться имя хоста, которым они зарегистрированы в Cisc IDS. Эта проблема может произойти, если пользователь обратился к альтернативному имени хоста, которое не зарегистрировано в Cisco IDS.
Рекомендуемое действие	Перейдите к Консоли управления Cisco IDS и подтвердите, зарегистрирован ли клиент в корректном перенаправлении URLand, то же используется для доступа к приложению.

Инициирование запроса SAML Cisco IDS

Оконечная точка SAML Cisco IDS является отправной точкой потока SAML в SSO основанный вход в систему. Инициирование взаимодействия между Cisco IDS и AD FS инициировано в этом шаге. Предпосылка здесь - то, что Cisco IDS должен знать, что AD FS соединяется с тем, поскольку соответствующие метаданные IdP должны быть загружены к Cisco IDS для этого шага для следования.

Распространенные ошибки, Встреченные во время этого Процесса

1. AD Метаданные FS, не добавленные к Cisco IDS

Краткое описание проблемы	Запрос регистрации в системе отказывает с 503 ошибками на браузере.
Возможная причина	**Браузер:** 503 ошибки с этим сообщением: Ошибка: "service_unavailable", "error_description "Метаданные SAML не инициализируются"} Метаданные Idp не доступны в Cisco IDS. Трастовое установление между Cisco и AD FS не завершено.
Рекомендуемое действие	Перейдите к Консоли управления Cisco IDS и посмотрите, находится ли IdS в **Состоянии not configured**. Подтвердите, загружены ли метаданные IdP или нет. В противном случае загрузите метаданные IdP, загруженные от AD FS. Для получения дополнительной информации посмотрите здесь.

Обработка запросов SAML AD FS

Обработка запросов SAML является первым шагом в AD FS в потоке SSO. Запрос SAML, отправленный Cisco IDS, считан, проверен и дешифрован AD FS в этом шаге. Успешная обработка этого запроса приводит к двум сценариям:

1. Если это - новый журнал в в браузере, AD FS показывает форму входа в систему.Если это уже - перевход в систему проверенный пользователь от существующего сеанса через обозреватель, AD FS пытается передать ответ SAML обратно непосредственно.

   Примечание: Основная предпосылка для этого шага для AD FS для имения настроенного доверия стороны ответа.

Распространенные ошибки, Встреченные во время этого Процесса

1. AD FS, не имеющий сертификат SAML последних Cisco IDS.

Краткое описание проблемы	AD FS, не показывая страницу входа, вместо этого показывает ошибочную страни
	Браузер AD FS показывает ошибочную страницу, подобную этому: Была проблема, обращающаяся к узлу. Попытайтесь перейти к узлу снова. Если проблема сохраняется, свяжитесь с администратором этого узла и предоста

	определения проблемы.
	Номер ссылки: 1ee602be-382c-4c49-af7a-5b70f3a7bd8e
	AD просмотр событий FS
	Сервис Федерации встретился с ошибкой при обработке запроса аутентификации
	Дополнительные данные
	`Exception details: Microsoft.IdentityModel.Protocols.XmlSignature.SignatureVerificatio`
	`MSIS0038: SAML Message has wrong signature. Issuer: 'myuccx.cisco.com'. at`
	`Microsoft.IdentityServer.Protocols.Saml.Contract.SamlContractUtility.CreateSamlMessage`
	`message) at`
	`Microsoft.IdentityServer.Service.SamlProtocol.SamlProtocolService.CreateErrorMessage(C`
	`createErrorMessageRequest) at`
	`Microsoft.IdentityServer.Service.SamlProtocol.SamlProtocolService.ProcessRequest(Messa`

Возможная причина	Полагающееся партийное доверие не установлено, или сертификат Cisco IDS изм загружено к AD FS.
Рекомендуемое действие	Установите доверие между AD FS и Cisco IDS с последним сертификатом Cisco ID Гарантируйте, что не истекается Сертификат Cisco IDS. Вы видите информационн Идентификационном управлении службами Cisco. Если так, восстановите сертифи настроек. Для получения дополнительной информации о том, как установить доверие метад Cisco IdS, посмотрите, здесь

Ответ SAML, передающий AD FS

ADFS передает ответ SAML обратно в Cisco IDS через браузер после того, как будет успешно аутентифицироваться пользователь. ADFS может передать ответ SAML обратно с кодом статуса, который указывает на Успешность или неуспешность. Если аутентификация формы не будет включена в AD FS тогда, то это укажет на ответ Сбоя.

Распространенные ошибки, Встреченные во время этого Процесса

1. Аутентификация формы не включена в AD FS

Краткое описание проблемы	Браузер показывает вход в систему NTLM, и затем отказывает, успешно не перенаправляя к Cisco IDS.
Шаг сбоя	Передача ответа SAML **Браузер:** Браузер показывает вход в систему NTLM, но после успешного журнала в, это отказывает со многими перенаправлениями.
Возможная причина	Cisco IDS поддерживает только основанную аутентификацию формы, аутентификация Формы не включена в AD FS.
Рекомендуемое действие	Для получения дополнительной информации о том, как включить аутентифика Формы, см.: Параметр аутентификации формы ADFS 2.0 Параметр аутентификации формы ADFS 3.0

Обработка ответа SAML Cisco IDS

На этом этапе Cisco IDS получает ответ SAML от AD FS. Этот ответ мог содержать код статуса, который указывает на Успешность или неуспешность. Ошибочный ответ от AD результатов FS в ошибочную страницу и то же должен быть отлажен.

Во время успешного ответа SAML обработка запроса может отказать по этим причинам:

- Неправильный IdP (AD FS) метаданные.
- Сбой для получения ожидаемых исходящих требований из AD FS.
- Cisco IDS и AD часы FS "not synchronized".

Распространенные ошибки, Встреченные во время этого Процесса

1. AD Сертификат FS в Cisco IDS не является последним.

Краткое описание проблемы	Запрос регистрации в системе отказывает с 500 ошибками на браузере с Кодом ош invalidSignature.
Шаг сбоя	Обработка Ответа SAML **Браузер:** 500 ошибок с этим сообщением в браузере: Код ошибки: invalidSignature Сообщение: сертификат подписания не совпадает с тем, что определено в метада объекта. **AD просмотр событий FS:** Никакая ошибка **Журнал Cisco IDS:** `2016-04-13 12:42:15.896 IST(+0530) default ERROR [IdSEndPoints-0] com.cisco.ccbu.ids IdSEndPoint.java:102 - Exception processing request com.sun.identity.saml2.common.SAML signing certificate does not match what's defined in the entity metadata. at com.sun.identity.saml2.xmlsig.FMSigProvider.verify(FMSigProvider.java:331) at com.sun.identity.saml2.protocol.impl.StatusResponseImpl.isSignatureValid(StatusRespons at com.sun.identity.saml2.profile.SPACSUtils.getResponseFromPost(SPACSUtils.java:985) com.sun.identity.saml2.profile.SPACSUtils.getResponse(SPACSUtils.java:196)`
Возможная причина	Обработка Ответа SAML отказала, поскольку сертификат IdP отличается от того, ч Cisco IDS.
Рекомендуемое действие	Загрузите последние AD метаданные FS от: **https://<ADFSServer>/federationmetada 06/federationmetadata.xml** И загрузите его к Cisco IDS через Идентификационный Сервис интерфейс пользов Managament. Для получения дополнительной информации посмотрите, Настраивают Cisco IDS

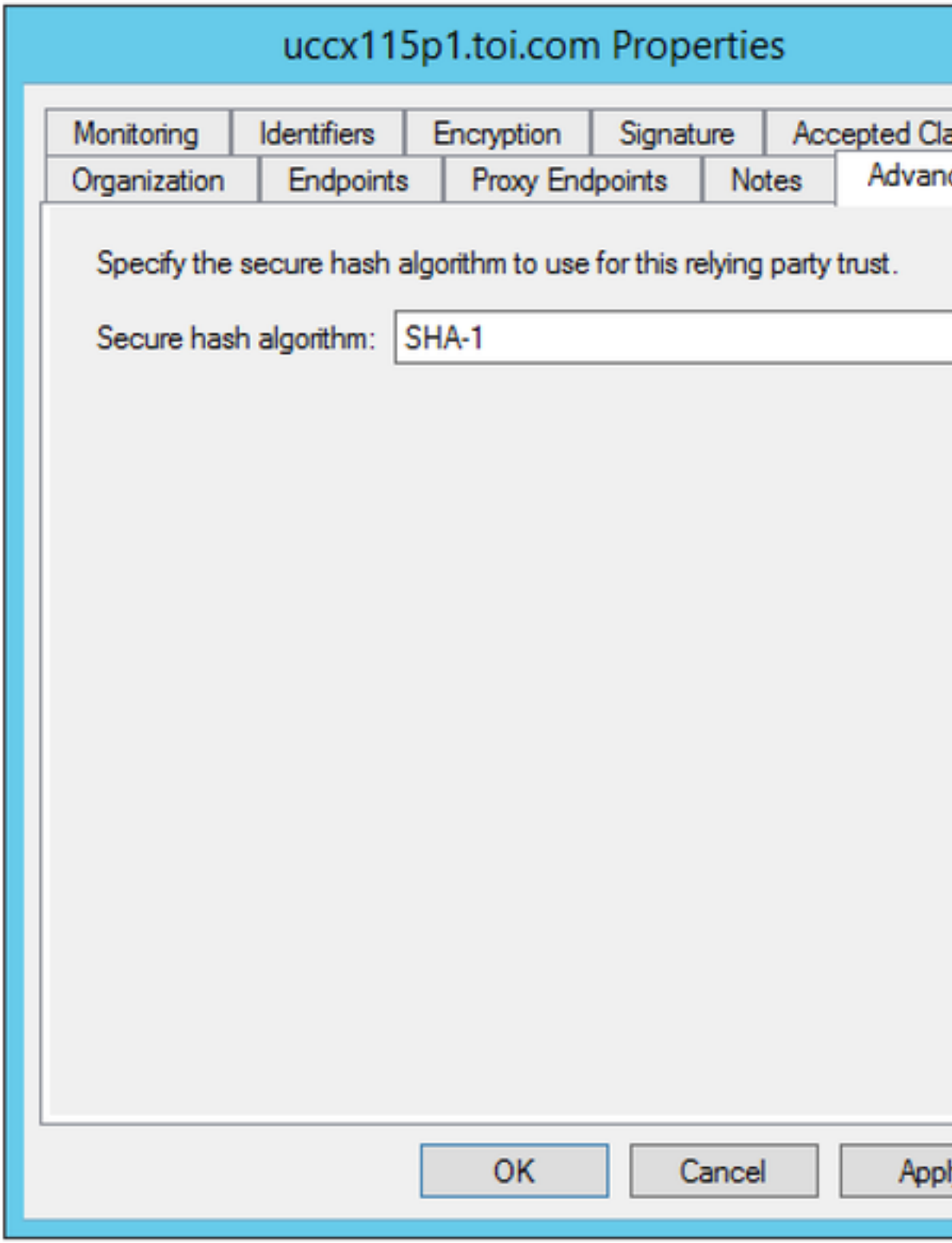
2. Cisco IDS и AD часы FS "not synchronized".

Краткое описание проблемы	Запрос регистрации в системе отказывает с 500 ошибками на браузере с кодом ст urn:oasis:names:tc:SAML:2.0:status:Success
Шаг сбоя	Обработка Ответа SAML **Браузер:** 500 ошибок с этим сообщением: Ошибка конфигурации IdP: обработка SAML отказала Утверждение SAML отказало от IdP с кодом статуса: urn:oasis:names:tc:SAML:2.0:s Проверяют конфигурацию IdP и попробовали еще раз. **Журнал Cisco IDS** `2016-08-24 18:46:56.780 IST(+0530) [IdSEndPoints-SAML-22] ERROR com.cisco.ccbu.ids IdSSAMLAsyncServlet.java:298 - SAML response processing failed with exception com.sun.identity.saml2.common.SAML2Exception: The time in SubjectConfirmationData is i com.sun.identity.saml2.common.SAML2Utils.isBearerSubjectConfirmation(SAML2Utils.java:7 com.sun.identity.saml2.common.SAML2Utils.verifyResponse(SAML2Utils.java:609) at com.sun.identity.saml2.profile.SPACSUtils.processResponse(SPACSUtils.java:1050) at com.sun.identity.saml2.profile.SPACSUtils.processResponseForFedlet(SPACSUtils.java:203 com.cisco.ccbu.ids.auth.api.IdSSAMLAsyncServlet.getAttributesMapFromSAMLResponse(IdSSA`

	at com.cisco.ccbu.ids.auth.api.IdSSAMLAsyncServlet.processSamlPostResponse(IdSSAMLAsyn com.cisco.ccbu.ids.auth.api.IdSSAMLAsyncServlet.processIdSEndPointRequest(IdSSAMLAsync com.cisco.ccbu.ids.auth.api.IdSEndPoint$1.run(IdSEndPoint.java:269) at java.util.concurrent.ThreadPoolExecutor.runWorker(ThreadPoolExecutor.java:1145) at java.util.concurrent.ThreadPoolExecutor$Worker.run(ThreadPoolExecutor.java:615) at java.lang.Thread.run(Thread.java:745)2016-08-24 18:24:20.510 IST(+0530) [pool-4-thread **Средство просмотра SAML:** Ищите поля NotBefore и NotOnOrAfter <Условия NotBefore = "2016-08-28T14:45:03.325Z" NotOnOrAfter = "2016-08-28T15:4
Возможная причина	Время в Cisco IDS и системе IdP вне синхронизования.
Рекомендуемое действие	Синхронизируйте Время в Cisco IDS и AD системе FS. Рекомендуется, чтобы AD с были время, синхронизировал Сервер NTP использования.

3. Неправильный алгоритм сигнатуры (SHA256 по сравнению с SHA1) в AD FS

Краткое описание проблемы	Запрос регистрации в системе отказывает с 500 ошибками на браузере со статусо code:urn:oasis:names:tc:SAML:2.0:status:Responder Сообщение об ошибках в AD Просмотре журнала события FS – неправильный алг (SHA256 по сравнению с SHA1) в AD FS
Шаг сбоя	Обработка Ответа SAML **Браузер** 500 ошибок с этим сообщением: Ошибка конфигурации IdP: обработка SAML отказала Утверждение SAML отказало от IdP с кодом статуса: urn:oasis:names:tc:SAML:2.0:s Проверьте конфигурацию IdP и попробуйте еще раз. **AD просмотр событий FS:** Запрос SAML не подписан с алгоритмом контрольной сигнатуры. Запрос SAML под сигнатуры http://www.w3.org/2001/04/xmldsig-more#rsa-sha256. Алгоритм контрольной сигнатуры является http://www.w3.org/2000/09/xmldsig#rsa-s **Журнал Cisco IDS:** ERROR com.cisco.ccbu.ids IdSSAMLAsyncServlet.java:298 - SAML response processing faile com.sun.identity.saml2.common.SAML2Exception: Invalid Status code in Response. at com.sun.identity.saml2.common.SAML2Utils.verifyResponse(SAML2Utils.java:425) at com.sun.identity.saml2.profile.SPACSUtils.processResponse(SPACSUtils.java:1050) at com.sun.identity.saml2.profile.SPACSUtils.processResponseForFedlet(SPACSUtils.java:203 com.cisco.ccbu.ids.auth.api.IdSSAMLAsyncServlet.getAttributesMapFromSAMLResponse(IdSSA
Возможная причина	AD FS настроен для использования SHA 256.
Рекомендуемое действие	Обновите AD FS для использования SHA-1 для подписания и шифрования. 1. RDP к AD системе FS. 2. Откройте AD консоль FS. 3. Выберите **Relying Party Trust** и нажмите **Properties** 4. **Откройте вкладку Advanced (Дополнительно).** 5. Выберите SHA-1 от выпадающего списка.



4. Исходящее Правило Требования, не Настроенное Правильно

Краткое описание проблемы	Сбои запроса регистрации в системе с 500 ошибками на браузере с сообщением " идентификатор пользователя из SAML response./Could не, получают пользовательь ответа SAML". uid и/или user_principal "not set" в исходящих требованиях.
Шаг сбоя	Обработка Ответа SAML **Браузер:** 500 ошибок с этим сообщением: Ошибка конфигурации IdP: обработка SAML отказала. Невозможно получить идентификатор пользователя из SAML response./Could не, п

пользовательский принципал из ответа SAML.

AD просмотр событий FS:

Никакая ошибка

Журнал Cisco IDS:

```
ERROR com.cisco.ccbu.ids IdSSAMLAsyncServlet.java:294 - SAML response processing faile
com.sun.identity.saml.common.SAMLException: Could not retreive user identifier from SA
com.cisco.ccbu.ids.auth.api.IdSSAMLAsyncServlet.validateSAMLAttributes(IdSSAMLAsyncSer
com.cisco.ccbu.ids.auth.api.IdSSAMLAsyncServlet.processSamlPostResponse(IdSSAMLAsyncSe
com.cisco.ccbu.ids.auth.api.IdSSAMLAsyncServlet.processIdSEndPointRequest(IdSSAMLAsync
```

Возможная причина

Обязательные исходящие требования (uid и user_principal) не настроены правильн
Требования.

Если вы не настроили правило требования NameID, или или uid или user_principal
образом.

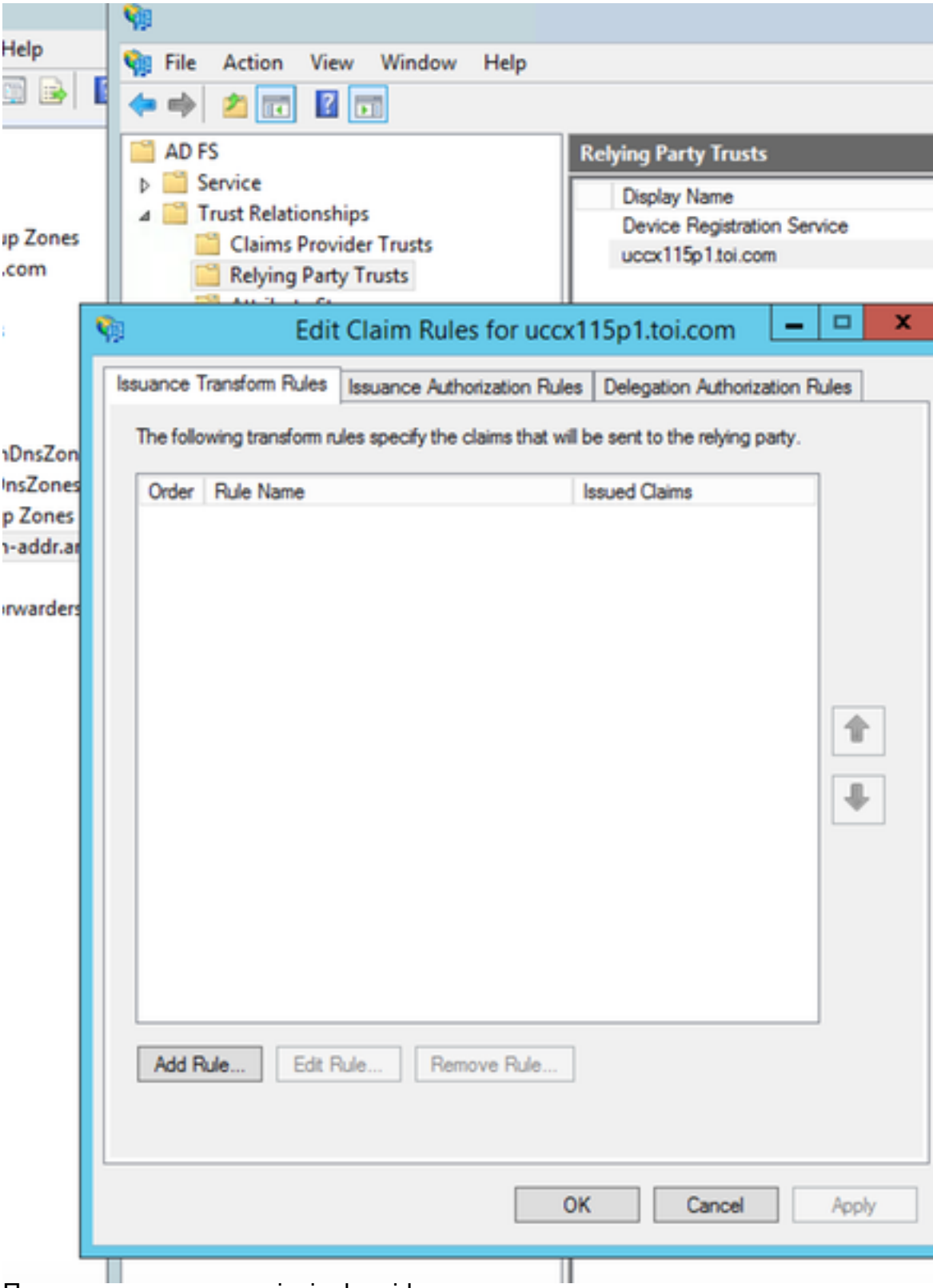
Если правило NameID не настроено , или user_principal не сопоставлен правильно,
что user_principal не получен, так как это - свойство, которое ищет Cisco IDS.

Если uid не сопоставлен правильно, Cisco IDS указывает, что не получен uid.

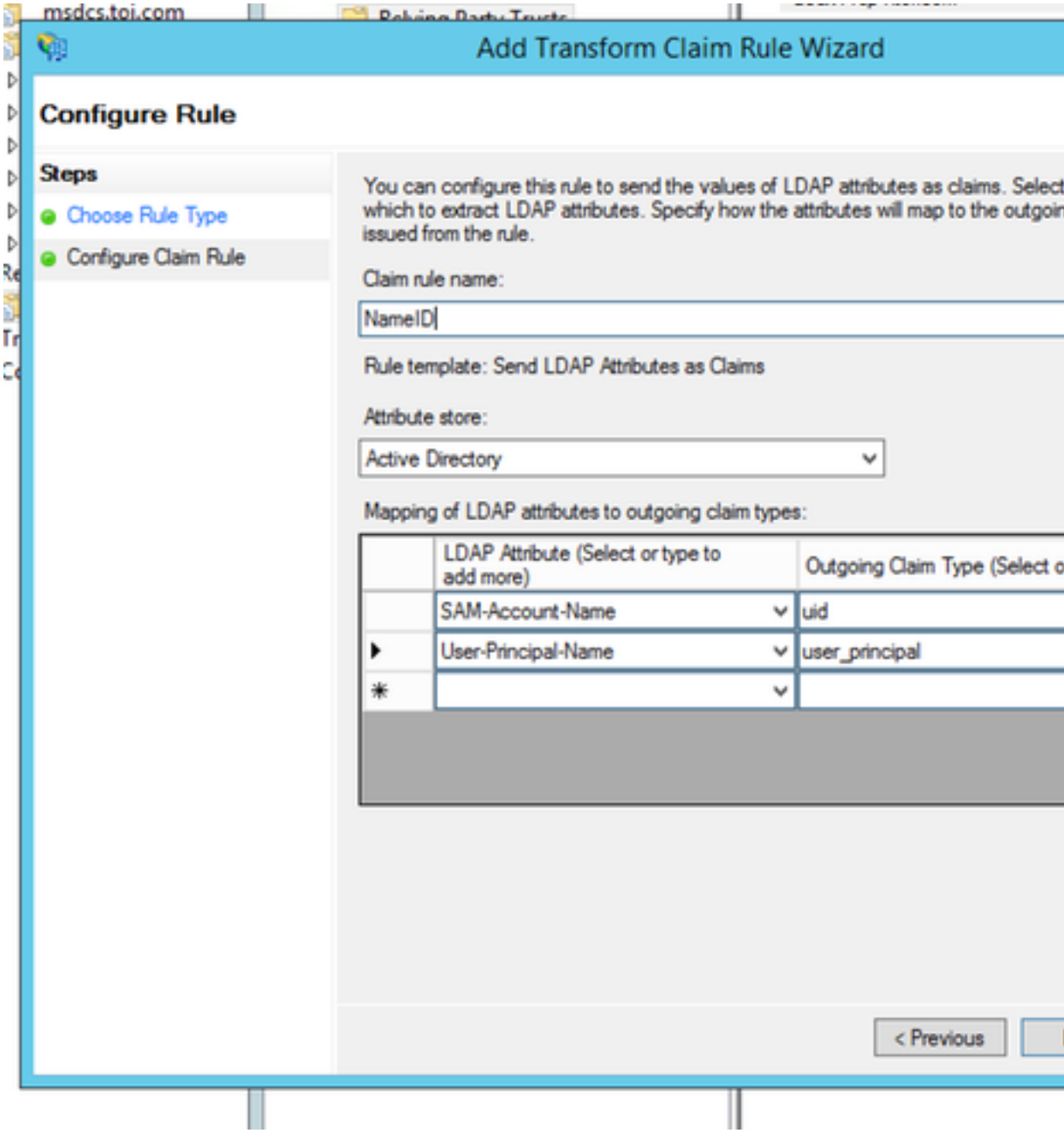
По AD правилам требования FS гарантируйте, что сопоставление атрибутов для "
определено как в Руководстве по конфигурации IdP (которые ведут?).

1. RDP к AD системе FS.
2. Отредактируйте Правила Требования для полагающегося партийного довери

Рекомендуемое действие



3. Проверьте, что user_principal и uid сопоставлены правильно



5. Исходящее Правило Требования не настроено правильно в Федеративном AD FS

Краткое описание проблемы Сбои запроса регистрации в системе с 500 ошибками на браузере с сообщением " получить идентификатор пользователя из ответа SAML. или не Мог получить поль принципал из ответа SAML". когда AD FS является Федеративный AD FS.

Шаг сбоя Обработка Ответа SAML

Браузер

500 ошибок с этим сообщением:

Ошибка конфигурации IdP: обработка SAML отказала

Невозможно получить идентификатор пользователя из SAML response./, не Мог по пользовательский принципал из ответа SAML.

AD просмотр событий FS:

Никакая ошибка

Журнал Cisco IDS:

```
ERROR com.cisco.ccbu.ids IdSSAMLAsyncServlet.java:294 - SAML response processing faile
com.sun.identity.saml.common.SAMLException: Could not retreive user identifier from SA
com.cisco.ccbu.ids.auth.api.IdSSAMLAsyncServlet.validateSAMLAttributes(IdSSAMLAsyncSer
com.cisco.ccbu.ids.auth.api.IdSSAMLAsyncServlet.processSamlPostResponse(IdSSAMLAsyncSe
at
```

```
com.cisco.ccbu.ids.auth.api.IdSSAMLAsyncServlet.processIdSEndPointRequest(IdSSAMLAsync
```

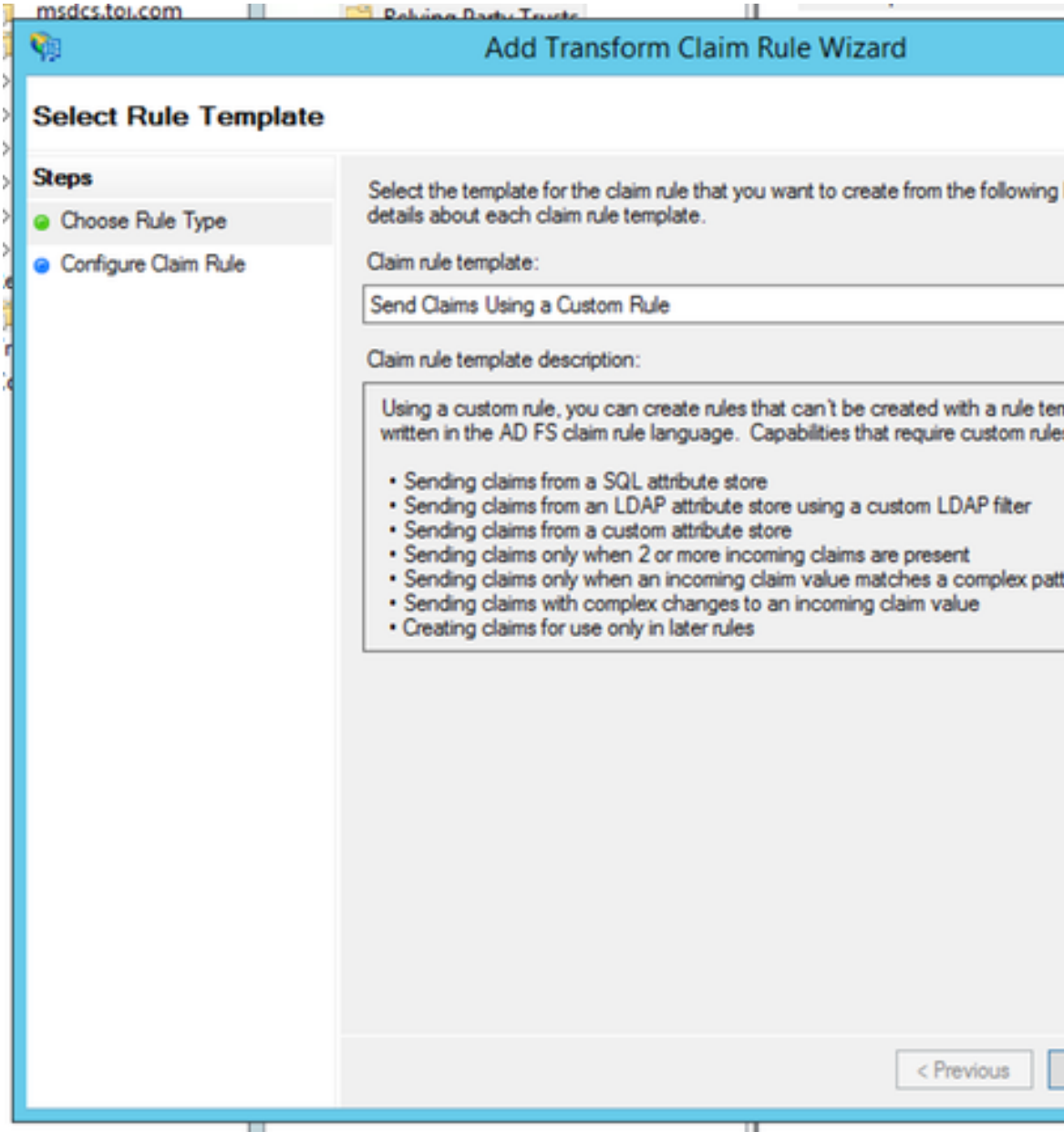
Возможная причина	В Федеративном AD FS существует больше конфигураций, требуемых, что это мог отсутствовать.
Рекомендуемое действие	Проверьте, реализована ли AD конфигурация FS в Федеративном AD согласно раз **Мультидоменной Конфигурации для Федеративного AD FS** в, Настраивают Cisco II

6. Пользовательские Правила Требования, не Настроенные Правильно

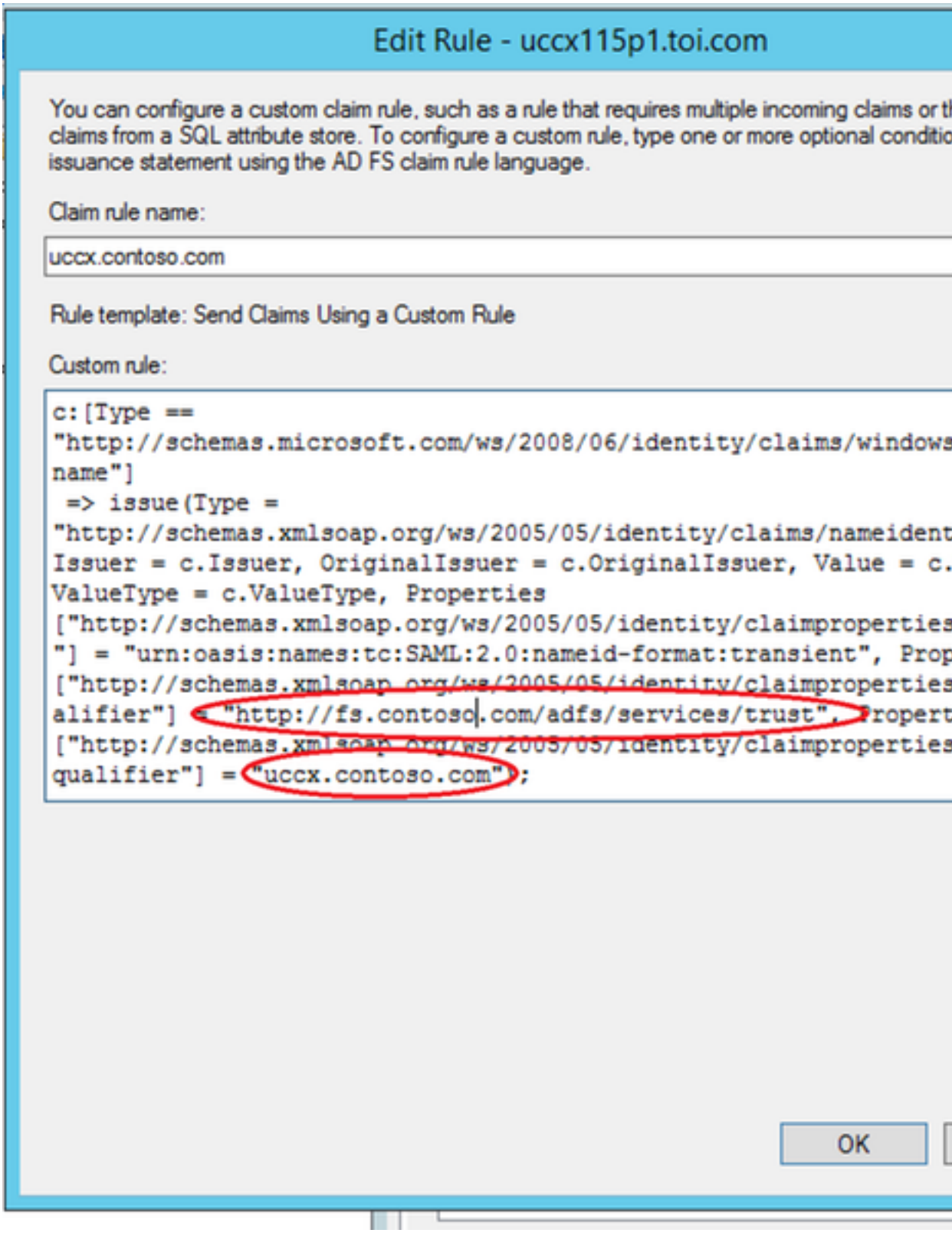
Краткое описание проблемы	Сбои запроса регистрации в системе с 500 ошибками на браузере с сообщением " идентификатор пользователя из SAML response./Could не, получают пользователь ответа SAML". uid и/или user_principal "not set" в исходящих требованиях.
Шаг сбоя	Обработка Ответа SAML **Браузер** 500 ошибок с этим сообщением: Утверждение SAML отказало от IdP с кодом статуса: **urn:oasis:names:tc:SAML:2.0:status:Requester/urn:oasis:names:tc:SAML:2.0:status:Inv** Проверьте конфигурацию IdP и попробуйте еще раз. **AD просмотр событий FS:** **Запрос аутентификации SAML имел Политику NameID, которая не могла быть удо** Проситель: myids. cisco . com Формат идентификатора названия: urn:oasis:names:tc:SAML:2.0:nameid-format:trans SPNameQualifier: myids. cisco . com Подробные данные исключения: MSIS1000: запрос SAML содержал NameIDPolicy, который не был удовлетворен вы Запрошенный NameIDPolicy: AllowCreate: Истинный Формат: urn:oasis:names:tc:SA format:transient SPNameQualifier: myids. cisco . com. Фактические свойства NameID: Этот запрос отказал. Действие пользователя Используйте моментальный снимок менеджмента AD FS 2.0 - в настроить конфигу испускает требуемый идентификатор названия. **Журнал Cisco IDS**:

```
2016-08-30 09:45:30.471 IST(+0530) [IdSEndPoints-SAML-82] INFO com.cisco.ccbu.ids SAML
failed with code: 1. Response status: <samlp:Status> <samlp:StatusCode
Value="urn:oasis:names:tc:SAML:2.0:status:Requester"> <samlp:StatusCode
Value="urn:oasis:names:tc:SAML:2.0:status:InvalidNameIDPolicy"> </samlp:StatusCode> </
</samlp:Status> for AuthnRequest: n/a 2016-08-30 09:45:30.471 IST(+0530) [IdSEndPoints
com.cisco.ccbu.ids IdSSAMLAsyncServlet.java:299 - SAML response processing failed with
com.sun.identity.saml2.common.SAML2Exception: Invalid Status code in Response. at
com.sun.identity.saml2.common.SAML2Utils.verifyResponse(SAML2Utils.java:425) at
com.sun.identity.saml2.profile.SPACSUtils.processResponse(SPACSUtils.java:1050) at
com.sun.identity.saml2.profile.SPACSUtils.processResponseForFedlet(SPACSUtils.java:203
```

Возможная причина	Пользовательское правило требования не настроено правильно.
Рекомендуемое действие	По AD правилам требования FS гарантируйте, что сопоставление атрибутов для "u определено как в руководстве по конфигурации (которые ведут?). 1. RDP к AD системе FS. 2. Отредактируйте Правила Требования для пользовательских правил требован



3. Проверьте, что даны AD FS и полные доменные имена Cisco IDS.



7. Слишком много запросов к AD FS.

Краткое описание проблемы	Запрос регистрации в системе отказывает с 500 ошибками на браузере со статусо code:urn:oasis:names:tc:SAML:2.0:status:Responder Сообщение об ошибках в AD Просмотре журнала События FS указывает, что сущ много запросов к AD FS.
Шаг сбоя	Обработка Ответа SAML **Браузер** 500 ошибок с этим сообщением: Ошибка конфигурации IdP: обработка SAML отказала Утверждение SAML отказало от IdP с кодом статуса: urn:oasis:names:tc:SAML:2.0:s

Проверьте конфигурацию IdP и попробуйте еще раз.
AD просмотр событий FS:
Microsoft. IdentityServer. Сеть. InvalidRequestException:
MSIS7042: **тот же сеанс клиентского браузера сделал '6' запросы в последнем '16' секунды. Свяжитесь со своим администратором для подробных данных.**
в Microsoft. IdentityServer. Сеть. FederationPassiveAuthentication. UpdateLoopDetec
в Microsoft. IdentityServer. Сеть. FederationPassiveAuthentication. SendSignInRespo
MSISSignInResponse)

```
Event Xml: <Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event"> <Syst
FS 2.0" Guid="{20E25DDB-09E5-404B-8A56-EDAE2F12EE81}" /> <EventID>364</EventID> <Versi
<Level>2</Level> <Task>0</Task> <Opcode>0</Opcode> <Keywords>0x8000000000000001</Keywo
SystemTime="2016-04-19T12:14:58.474662600Z" /> <EventRecordID>29385</EventRecordID> <C
ActivityID="{98778DB0-869A-4DD5-B3B6-0565AC17BFFE}"/> <Execution ProcessID="2264" Thre
<Channel>AD FS 2.0/Admin</Channel> <Computer>myadfs.cisco.com</Computer> <Security Use
1680627477-1295527365-1502263146-1105"/> </System> <UserData> <Event xmlns:auto-
ns2="http://schemas.microsoft.com/win/2004/08/events"
xmlns="http://schemas.microsoft.com/ActiveDirectoryFederationServices/2.0/Events"> <Ev
<Data>Microsoft.IdentityServer.Web.InvalidRequestException: MSIS7042: The same client
'6' requests in the last '16' seconds. Contact your administrator for details. at
Microsoft.IdentityServer.Web.FederationPassiveAuthentication.UpdateLoopDetectionCookie
Microsoft.IdentityServer.Web.FederationPassiveAuthentication.SendSignInResponse(MSISSi
</Data> </EventData> </Event> </UserData> </Event>
```

Журнал Cisco IDS

```
2016-04-15 16:19:01.220 EDT(-0400) default ERROR [IdSEndPoints-1] com.cisco.ccbu.ids I
Exception processing request com.sun.identity.saml2.common.SAML2Exception: Invalid Sta
com.sun.identity.saml2.common.SAML2Utils.verifyResponse(SAML2Utils.java:425) at
com.sun.identity.saml2.profile.SPACSUtils.processResponse(SPACSUtils.java:1050) at
com.sun.identity.saml2.profile.SPACSUtils.processResponseForFedlet(SPACSUtils.java:203
com.cisco.ccbu.ids.auth.api.IdSSAMLAsyncServlet.getAttributesMapFromSAMLResponse(IdSSA
```

Возможная причина

Существует слишком много запросов, достигающих AD FS от того же сеанса через

Рекомендуемое действие

Это не должно, как правило, происходить в производстве. Но если вы встречаетес

1. Проверьте AD Windows Event Viewer FS.
2. Перепроверьте Полагающиеся Партийные Параметры доверия. Для получен информации *посмотрите*, Настраивают Cisco IDS и AD FS
3. Перевход в систему.

8. AD FS не Настроен для Подписания и Утверждения и сообщения.

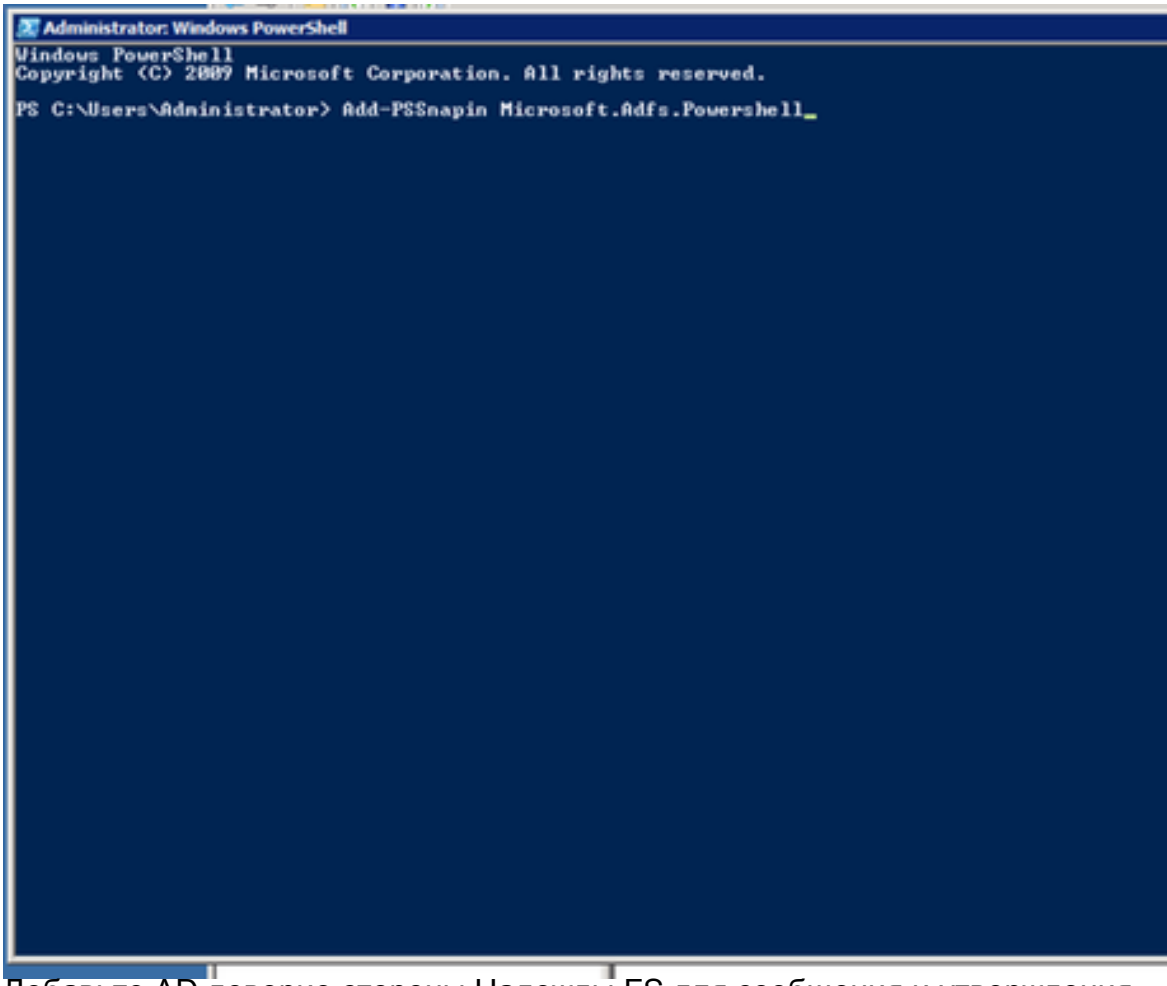
Краткое описание проблемы

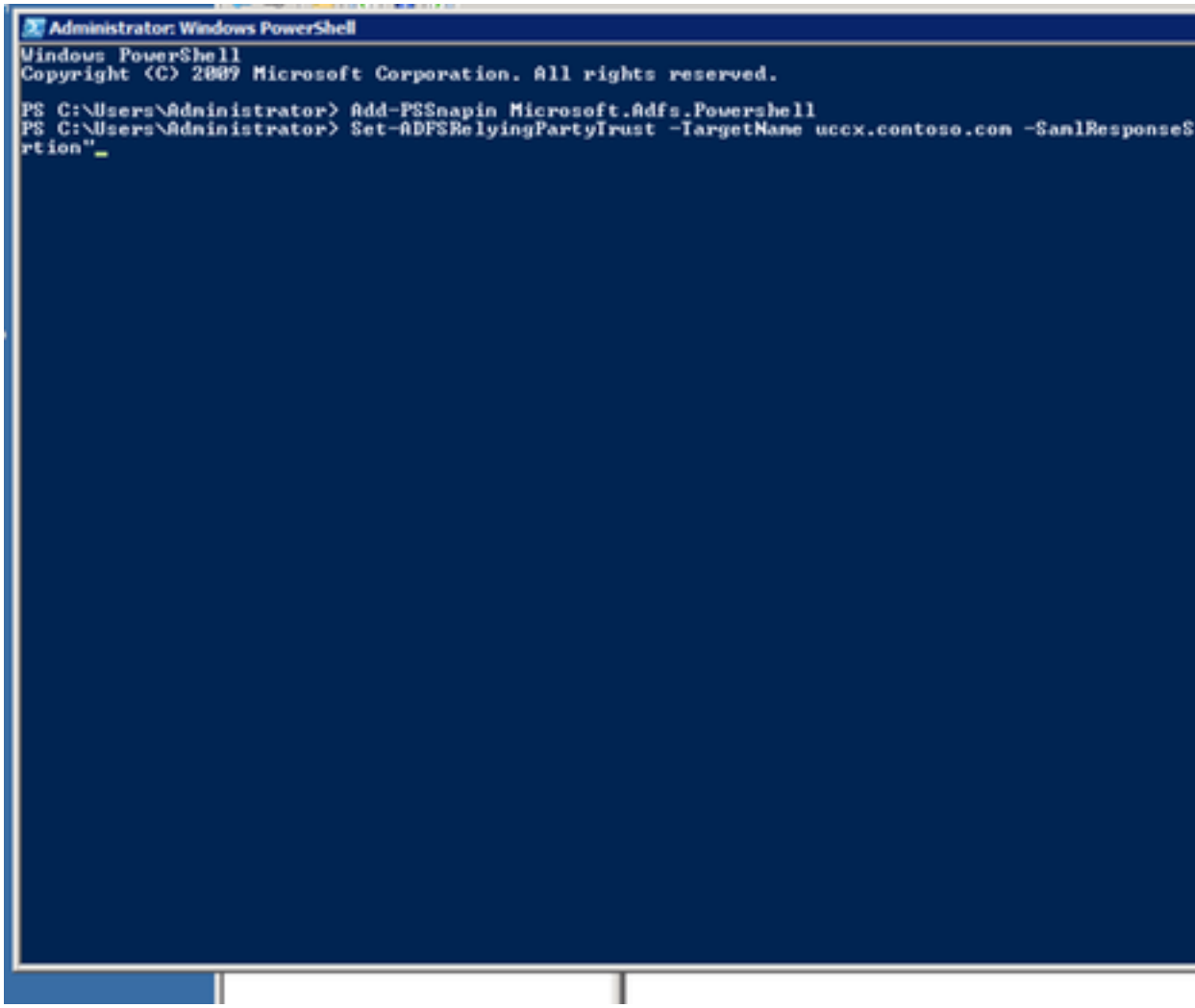
Запрос регистрации в системе отказывает с 500 ошибками на браузере с Ошибкой

Шаг сбоя

Обработка Ответа SAML
Браузер
500 ошибок с этим сообщением:
Код ошибки: invalidSignature
Подпись Message:Invalid в ArtifactResponse.
Журнал Cisco IDS:

```
2016-08-24 10:53:10.494 IST(+0530) [IdSEndPoints-SAML-241] INFO saml2error.jsp saml2er
response processing failed with code: invalidSignature; message: Invalid signature in
08-24 10:53:10.494 IST(+0530) [IdSEndPoints-SAML-241] ERROR com.cisco.ccbu.ids IdSSAML
SAML response processing failed with exception com.sun.identity.saml2.common.SAML2Exce
in Response. at com.sun.identity.saml2.profile.SPACSUtils.getResponseFromPost(SPACSUti
com.sun.identity.saml2.profile.SPACSUtils.getResponse(SPACSUtils.java:196) at
com.sun.identity.saml2.profile.SPACSUtils.processResponseForFedlet(SPACSUtils.java:202
com.cisco.ccbu.ids.auth.api.IdSSAMLAsyncServlet.getAttributesMapFromSAMLResponse(IdSSA
```

Возможная причина	AD FS не настроен для подписания и Утверждения и сообщения.
Рекомендуемое действие	1. Выполните AD FS powershell команда: **набор-ADFSRelyingPartyTrust-TargetNa Партийный Трастовый Идентификатор>-SamlResponseSignature "MessageAnd** 2. RDP к AD системе. 3. Открытый **Powershell**. 4. Добавьте моментальный-снимок-ins Windows PowerShell к текущему сеансу. 3 требоваться в том, если вы используете ADFS 3.0, так как CmdLet уже устано добавления ролей и функций.  5. Добавьте AD доверие стороны Надежды FS для сообщения и утверждения.



Дополнительные сведения

Это отнесено к конфигурации Идентификационного Поставщика, описанного в статье:

- https://www. cisco . com/c/en/us/support/docs/customer-collaboration/unified-contact-center-express/200612-Configure-the-Identity-Provider-for-UCCX .html
- Cisco Systems – техническая поддержка и документация