ADFS/IdS 문제 해결 및 일반적인 문제

목차

소개

브라우저를 통한 Cisco IDs(Identity Service)와 AD FS(Active Directory Federation Services) 간의 SAML(Security Assertion Markup Language) 상호 작용은 SSO(Single-Sign On) 로그인 흐름의 핵심입니다. 이 문서는 Cisco IDs 및 AD FS의 구성과 관련된 문제를 해결하기 위한 권장 작업과 함께 디버깅하는 데 도움이 됩니다.

Cisco IDs 구축 모델

제품	구축
UCCX	공동 상주
PCCE	CUIC(Cisco Unified Intelligence Center) 및 LD(라이브 데이터)와 공동 상주
UCCE	2k 구축을 위해 CUIC 및 LD와 공동 상주 4k 및 12k 구축을 위한 독립형

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco Unified Contact Center Express(UCCX) 릴리스 11.5 또는 Cisco Unified Contact Center Enterprise 릴리스 11.5 또는 PCCE(Packaged Contact Center Enterprise) 릴리스 11.5가 해당됩니다.
- Microsoft Active Directory - Windows Server에 설치된 AD
- IdP(ID 공급자) - AD FS(Active Directory Federation Service) 버전 2.0/3.0

사용되는 구성 요소

이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

Cisco IdS와 AD FS 간에 신뢰 관계가 설정되면(자세한 내용은 UCCX 및 UCCE에 공통으로 참조) 관리자는 Identity Service Management의 설정 페이지에서 테스트 SSO 설정을 실행하여 Cisco IdS와 AD FS 간의 컨피그레이션이 제대로 작동하는지 확인해야 합니다. 테스트가 실패할 경우 이 가이드에 제공된 적절한 애플리케이션 및 제안을 사용하여 문제를 해결하십시오.

디버깅에 유용한 응용 프로그램 및 로그

애플리케이션/로그	세부 정보	도구를 찾을 위치
Cisco IdS 로그	Cisco IdS 로거는 Cisco IdS에서 발생한 모든 오류를 기록합니다.	RTMT를 사용하여 Cisco IdS 로그를 져옵니다.RTMT 사용 방법에 대한 자한 내용은 RTMT 사용 설명서 를 참십시오. RTMT 이름은 **Cisco Identity Servic니다**.로그를 찾으려면 **Cisco Identity Service > log**로 이동합니다.
플렛 로그	Fedlet 로그는 Cisco IdS에서 발생하는 SAML 오류에 대한 자세한 정보를 제공합니다.	RTMT를 사용하여 Fedlet 로그를 가니다. Fedlet 로그의 위치는 Cisco IdS 로그동일합니다. fedlet 로그는 접두사 fedlet -
Cisco IdS API 메	API 메트릭을 사용하여 Cisco IdS API에서 반환했	RTMT를 사용하여 API 메트릭을 가

트릭	을 수 있는 오류와 Cisco idS에서 처리된 요청 수를 확인하고 검증할 수 있습니다.	니다. RTMT 이름은 **Cisco Identity Servic** 니다. 이는 별도의 폴더 **메트릭** 아래에 나 니다.**saml_metrics.csv** 및 **authorize_metrics.csv**는 이 문서에 관련 메트릭입니다.
AD FS의 이벤트 뷰어	사용자가 시스템의 이벤트 로그를 볼 수 있습니다.SAML 요청을 처리하고 SAML 응답을 보내는 동안 AD FS에 오류가 발생하면 여기에 기록됩니다.	AD FS 컴퓨터에서 **Event Viewer(이벤트 뷰어) >Applications** and **Services Logs(애플리케이션 및 서비스 로그) >AdDFS 2.0 > Admin(관리)으로 이동합니다.** Windows 2008의 경우 **제어판 > 성능 유지 관리 > 관리 도구에서 이벤트 뷰어를 시작합니다.** Windows 2012에서 제어판\시스템 및 보안\관리 도구에서 시작합니다. 이벤트 뷰어를 찾을 위치를 보려면 Windows 설명서를 참조하십시오.
SAML 뷰어	SAML Viewer는 Cisco IdS에서/로 전송되는 SAML 요청 및 응답을 확인하는 데 도움이 됩니다. 이 브라우저 애플리케이션은 SAML 요청/응답 분석에 매우 유용합니다.	다음은 SAML 요청 및 응답을 확인하는 데 사용할 수 있는 몇 가지 권장 SAML 뷰어입니다. 1. 피들러 AD FS에서 파일을 사용하는 방법Fiddler Chrome 플러그인 2. SAML Tracer - Firefox 3. SAML Chrome 패널

디버깅 옵션이 있는 플로우 다이어그램

SSO 인증을 위한 다양한 단계가 이미지에 표시되고 해당 단계에서 장애가 발생할 경우 각 단계에서 아티팩트를 디버깅합니다.

이 표에서는 브라우저에서 SSO의 각 단계에서 실패를 식별하는 방법에 대한 세부 정보를 제공합니다.다른 도구 및 디버깅에 도움이 되는 방법도 지정합니다.

단계	브라우저에서 장애를 식별하는 방법	툴/로그	확인할 구성
Cisco ID에 의한 AuthCode 요청 처리	오류가 발생할 경우 브라우저가 SAML 엔드포인트 또는 AD FS로 리디렉션되지 않고 Cisco IdS에서 JSON 오류가 표시되며, 이는 클라이언트 ID 또는 리디렉션 URL이 잘못되었음을 나타냅니다.	Cisco IdS logs(Cisco IDs 로그) - authcode 요청이 검증되고 처리되는 동안 발생하는 오류를 나타냅니다. Cisco IdS API metrics - 처리 및 실패한 요청 수를 나타냅니다.	클라이언트 등록
Cisco ID로 SAML 요청 시작	실패 시 브라우저는 AD FS로 리디렉션되지 않으며 Cisco IdS에서 오류 페이지/메시지를 표시합니다.	Cisco IdS logs(Cisco IdS 로그) - 요청이 시작되는 동안 예외가 있는지 여부를 나타냅니다. Cisco IdS API metrics - 처리 및 실패한 요청 수를 나타냅니다.	NOT_CONFIGURED 상태의 Cisco ID입니다.
AD FS별 SAML 요청 처리	이 요청을 처리하지 못하면 로그인 페이지 대신 AD FS 서버에서 오류 페이지를 표시합니다.	AD FS의 이벤트 뷰어 - 요청이 처리되는 동안 발생하는 오류를 나타냅니다. SAML Browser Plugin - AD FS로 전송되는 SAML 요청을 볼 수 있습니다.	IdP의 당사자 트러스트 구성

AD FS로 SAML 응답 전송	응답을 보내지 못하면 유효한 자격 증명이 제출된 후 AD FS 서버에서 오류 페이지를 표시합니다.	AD FS의 이벤트 뷰어 - 요청이 처리되는 동안 발생하는 오류를 나타냅니다. AD FS의 이벤트 뷰어 - AD FS가 성공 상태 코드 없이 SAML 응답을 보내는 경우 오류를 나타냅니다.	• IdP의 당사자 트러스트 구성 • AD FS의 양식 인증 설정입니다 .
Cisco ID를 통한 SAML 응답 처리	Cisco IdS에 오류 사유와 빠른 확인 페이지가 포함된 500 오류가 표시됩니다.	SAML Browser Plugin - AD FS에서 보낸 SAML 응답을 확인하여 무엇이 잘못되었는지 확인할 수 있도록 도와줍니다. Cisco IdS 로그 - 처리 중 발생한 오류/예외를 나타냅니다. Cisco IdS API metrics - 처리 및 실패한 요청 수를 나타냅니다.	• 클레임 규칙 구성 • 메시지 및 어설션 서명

Cisco ID로 인증 코드 요청 처리

Cisco IdS에 관한 한 SSO 로그인의 시작점은 SSO 지원 애플리케이션의 권한 부여 코드 요청입니다.API 요청 검증이 완료되어 등록된 클라이언트의 요청인지 확인합니다.검증에 성공하면 브라우저가 Cisco IdS의 SAML 엔드포인트로 리디렉션됩니다.요청 유효성 검사에 오류가 발생하면 오류 페이지/JSON(JavaScript Object Notation)이 Cisco IdS에서 다시 전송됩니다.

이 프로세스 중에 발생한 일반적인 오류

1. 클라이언트 등록이 완료되지 않음

문제 요약 브라우저에서 401 오류가 발생하여 로그인 요청이 실패합니다.

오류 메시지

브라우저:

401 오류 메시지:{"error":"invalid_client","error_description":"잘못된 ClientId"}

Cisco IDs 로그:

```
2016-09-02 00:16:58.604 IST(+0530) [IdSEndPoints-51] WARN com.cisco.ccbu.ids IdSConfigImpl.java:
 ID:FB308a80050b2021f974f48a72ef9518a5e7ca69 2016-09-02 00:16:58.604 IST(+0530) [IdSE5] 1] ERROR
com.cisco.ccbu.ids IdSOAuthEndPoint.java:45 -
.org.apache.oltu.oauth2.common.exception.OAuthProblem:invalid_client,  ClientId
.com.cisco.ccbu.ids.auth.validator.IdSAuthorize.validator
org.apache.oltu.oauth2.common.exception.OAuthProblemException.error(OAuthProblem.java:59)
IdSAuthorizeValidator.validatorRequestParams(Id.cisco.cids.sa.Validator.Validator.Validator.SA5)
org.apache.oltu.oauth2.as.reQUEST.OAuthRequest.validate(OAuthRequest.java:63)
UnauthorizeValidator.validatorRequiredParameters(IdSAuthorizeValidator.java:70)
```

가능한 원인 Cisco ID로 클라이언트 등록이 완료되지 않았습니다.

권장 작업 Cisco IdS Management 콘솔로 이동하여 클라이언트가 성공적으로 등록되었는지 확인합니다.그렇지 않은 경우 SSO를 진행하기 전에 클라이언트를 등록합니다.

2. 사용자가 IP 주소/대체 호스트 이름을 사용하여 애플리케이션에 액세스합니다.

문제 요약 브라우저에서 401 오류가 발생하여 로그인 요청이 실패합니다.

오류 메시지

브라우저:

401 오류 메시지:{"error":"invalid_redirectUri","error_description":"잘못된 리디렉션 URI"}

가능한 사용자는 IP 주소/대체 호스트 이름을 사용하여 애플리케이션에 액세스합니다.

원인	SSO 모드에서는 애플리케이션이 IP를 사용하여 액세스하면 작동하지 않습니다.애플리케이션은 Cisco ID에 등록된 호스트 이름으로 액세스해야 합니다.이 문제는 사용자가 Cisco Id에 등록되지 않 대체 호스트 이름에 액세스한 경우 발생할 수 있습니다.
권장 작업	Cisco IdS Management Console로 이동하여 클라이언트가 올바른 리디렉션 URL로 등록되어 있고 일한 URL을 사용하여 애플리케이션에 액세스하는지 확인합니다.

Cisco ID로 SAML 요청 시작

Cisco IdS의 SAML 엔드포인트는 SSO 기반 로그인에서 SAML 흐름의 시작점입니다.Cisco IdS와 AD FS 간의 상호 작용 시작이 이 단계에서 트리거됩니다.이 단계가 성공하려면 Cisco IdS가 연결할 AD FS를 알고 있어야 합니다. 해당 IdP 메타데이터를 Cisco IdS에 업로드해야 합니다.

이 프로세스 중에 발생한 일반적인 오류

1. AD FS 메타데이터가 Cisco IdS에 추가되지 않았습니다.

문제 요약	브라우저에서 503 오류가 발생하여 로그인 요청이 실패합니다.
오류 메시지	**브라우저:** 503 오류 메시지:{"error":"service_unavailable","error_description":"SAML 메타데이터가 초기화 않았습니다."}
가능한 원인	Cisco ID에서는 IDP 메타데이터를 사용할 수 없습니다.Cisco IdS와 AD FS 간의 신뢰 설정이 완 지 않았습니다.
권장 작업	Cisco IdS Management Console로 이동하여 IdS가 구성되지 **않음** 상태에 있는지 확인합니다. IdP 메타데이터가 업로드되었는지 확인합니다. 그렇지 않은 경우 AD FS에서 다운로드한 IdP 메타데이터를 업로드합니다. 자세한 내용은 여기를 참조하십시오.

AD FS별 SAML 요청 처리

SAML Request Processing(SAML 요청 처리)은 SSO 흐름에서 AD FS의 첫 번째 단계입니다.Cisco IdS에서 보낸 SAML 요청은 이 단계에서 AD FS에서 읽고, 검증하고, 해독합니다.이 요청을 성공적으로 처리하면 두 가지 시나리오가 발생합니다.

1. 브라우저에서 새 로그인일 경우 AD FS는 로그인 양식을 표시합니다.기존 브라우저 세션에서 이미 인증된 사용자의 재로그인인 경우 AD FS는 SAML 응답을 직접 보내려고 시도합니다.

참고:이 단계의 기본 전제 조건은 AD FS가 회신 대상 트러스트를 구성하도록 하는 것입니다.

이 프로세스 중에 발생한 일반적인 오류

1. 최신 Cisco IdS SAML 인증서가 없는 AD FS

문제 요약	AD FS에서 로그인 페이지를 표시하지 않고 오류 페이지를 표시합니다.
오류 메시지	**브라우저** AD FS는 다음과 유사한 오류 페이지를 표시합니다. 사이트에 액세스하는 동안 문제가 발생했습니다.사이트를 다시 찾아보십시오. 문제가 계속되면 이 사이트의 관리자에게 문의하여 문제를 확인할 참조 번호를 제공하십시오. 참조 번호:1ee602be-382c-4c49-af7a-5b70f3a7bd8e

AD FS 이벤트 뷰어
SAML 인증 요청을 처리하는 동안 페더레이션 서비스에 오류가 발생했습니다.
추가 데이터

```
 :Microsoft.IdentityModel.Protocols.XmlSignature.SignatureVerificationFailedException:MSIS0038:S
:'myuccx.cisco.com'Microsoft.IdentityServer.Protocols.Saml.Contract.SamlContractUtility.CreateSa
message) at Microsoft.IdentityServer.Service.SamlProtocol.SamlProtocolService.CreateErrorMessage
Protocol.SamlProtocolService.ProcessRequest(Message requestMessage)
```

가능한 원인 신뢰 당사자 트러스트가 설정되지 않았거나 Cisco IdS 인증서가 변경되었지만 AD FS에 업로드되지

권장 작업 최신 Cisco IdS 인증서를 사용하여 AD FS와 Cisco IdS 간에 신뢰를 설정합니다.
Cisco IDs 인증서가 만료되지 않았는지 확인하십시오.Cisco Identity Service Management에서 상태
경우 설정 페이지에서 인증서를 다시 생성합니다.
ADFS 및 Cisco IdS 전반에 걸쳐 메타데이터 신뢰를 설정하는 방법에 대한 자세한 내용은 여기를 참

AD FS에서 보내는 SAML 응답

ADFS는 사용자가 성공적으로 인증되면 브라우저를 통해 SAML 응답을 Cisco IdS로 다시 전송합니다.ADFS는 Success 또는 Failure를 나타내는 상태 코드와 함께 SAML 응답을 다시 전송할 수 있습니다.양식 인증이 AD FS에서 활성화되지 않은 경우 실패 응답을 나타냅니다.

이 프로세스 중에 발생한 일반적인 오류

1. AD FS에서 양식 인증을 사용할 수 없습니다.

문제 요약 브라우저에 NTLM 로그인이 표시된 다음 Cisco IdS로 리디렉션하지 않고 실패합니다.
장애 단계 SAML 응답 전송
오류 메시지 **브라우저:**
브라우저에는 NTLM 로그인이 표시되지만, 로그인이 성공하면 많은 리디렉션이 실패하게 됩니
가능한 원인 Cisco IdS는 양식 기반 인증만 지원하며, 양식 인증은 AD FS에서 활성화되지 않습니다.
양식 인증을 활성화하는 방법에 대한 자세한 내용은 다음을 참조하십시오.
권장 작업
ADFS 2.0 양식 인증 설정
ADFS 3.0 양식 인증 설정

Cisco ID를 통한 SAML 응답 처리

이 단계에서는 Cisco IdS가 AD FS에서 SAML 응답을 받습니다.이 응답에는 성공 또는 실패를 나타내는 상태 코드가 포함될 수 있습니다.AD FS의 오류 응답이 오류 페이지로 이어지므로 동일한 내용을 디버깅해야 합니다.

성공적인 SAML 응답 중에 다음과 같은 이유로 요청 처리가 실패할 수 있습니다.

- 잘못된 AD FS(IdP) 메타데이터입니다.
- AD FS에서 필요한 발신 클레임을 검색하지 못했습니다.
- Cisco IdS 및 AD FS 클럭이 동기화되지 않습니다.

이 프로세스 중에 발생한 일반적인 오류

1. Cisco IdS의 AD FS 인증서가 최신 인증서가 아닙니다.

문제 요약 오류 코드가 invalidSignature로 표시된 브라우저에 500 오류가 발생하여 로그인 요청이 실패합니다
장애 SAML 응답 처리

단계	

오류 메시지	**브라우저:**
	브라우저에서 이 메시지에 대한 500 오류:
	오류 코드:유효하지 않은 서명
	메시지:서명 인증서가 엔터티 메타데이터에 정의된 것과 일치하지 않습니다.
	AD FS 이벤트 뷰어:
	오류 없음
	Cisco IDs 로그:
	`2016-04-13 12:42:15.896 IST(+0530)  [IdSEndPoints-0] com.cisco.ccbu.ids IdSEndPoint.java:102 - com.sun.identity.saml2.common.SAML2:`
	`.com.sun.identity.saml2.xmlsig.FMSigProvider.verify(FMSigProvider.java:331) at com.sun.identity.saml2.protocol.impl.StatusResponseImpl.isSignatureValid(StatusResponseImpl.java at com.sun.identity.profile.profile.SPACSUGetGetTiLS.GetResponSEFromFrom COM.SUN.IDENTITY.SAML2.PROFILE.SPACSUtils.getResponse(SPACSUtils.java:196) post(SPACSUtils.java:`

가능한 원인	IdP 인증서가 Cisco IdS에서 사용할 수 있는 것과 다르므로 SAML 응답 처리에 실패했습니다.
권장 작업	다음 위치에서 최신 AD FS 메타데이터를 다운로드합니다 .**https://<ADFSServer>/federationmetadata/2007-06/federationmetadata.xml** Identity Service Management 사용자 인터페이스를 통해 Cisco Id에 업로드합니다. 자세한 내용은 Cisco IdS 및 AD FS 구성을 참조하십시오.

2. Cisco IdS 및 AD FS 클럭이 동기화되지 않습니다.

문제 요약	브라우저에서 500 오류가 발생하여 로그인 요청이 실패하고 상태 코드가 표시됩니다.urn:oasis:nar
장애 단계	SAML 응답 처리
오류 메시지	**브라우저:** 500 오류 메시지: IdP 구성 오류:SAML 처리 실패 IdP에서 SAML 어설션이 실패했습니다(상태 코드:urn:oasis:names:tc:SAML:2.0:status:Success.Id **Cisco IDs 로그** `2016-08-24 18:46:56.780 IST(+0530) [IdSEndPoints-SAML-22] ERROR com.cisco.ccbu.ids IdSSAMLAsyncS .com.sun.identity.saml2.common.saml2Utils.isBearerSubjectConfirmation(SAML2Utils.java:766) at co com.sun.identity.saml2.profile.spacsuProcessResponse(SU1SUSU:SU11TILS:JAVA.stils1Response) com.cisco.ccbu.ids.auth.api.IdSSAMLAsyncServlet.getAttributesMapFromSAMLRonse(IdSSAMLAsyncSyncMa) 0) 2) com.cisco.ccbu.ids.auth.api.IdSSAMLAsyncServlet.processcom.cisco.ccbu.ids.auth.api.IdSSA java.util.concurrent.ThreadPoolExecutor.ThreadPoolWorker.runWorker(ThreadPoolExecutor.java:1145) java.lang.Thread.run(Thread.java:745)2016-08-24 18:24:20.510 IST(+0530) [pool-4-thread-1]` **SAML 뷰어:** NotBefore 및 NotOnOrAfter 필드를 찾습니다. <Conditions NotBefore="2016-08-28T14:45:03.325Z" NotOnOrAfter="2016-08-28T15:45:03.325Z"
가능한 원인	Cisco IdS 및 IdP 시스템의 시간이 동기화되지 않았습니다.
권장 작업	Cisco IdS 및 AD FS 시스템의 시간을 동기화합니다.AD FS 시스템 및 Cisco IdS는 NTP 서버를 사용

3. AD FS의 잘못된 서명 알고리즘(SHA256 vs SHA1)

문제 요약	브라우저에서 로그인 요청이 500 오류와 함께 실패함(상태 코드: urn:oasis:names:tc:SAML:2.0:sta AD FS 이벤트 보기 로그의 오류 메시지 - AD FS의 잘못된 서명 알고리즘(SHA256 vs SHA1)
장애 단계	SAML 응답 처리
오류 메시지	**브라우저** 500 오류 메시지: IdP 구성 오류:SAML 처리 실패

IdP에서 SAML 어설션이 실패했습니다(상태 코드:urn:oasis:names:tc:SAML:2.0:status:Responder
AD FS 이벤트 뷰어:
SAML 요청이 필요한 서명 알고리즘으로 서명되지 않았습니다.SAML 요청은 서명 알고리즘 http://w
필요한 서명 알고리즘은 http://www.w3.org/2000/09/xmldsig#rsa-sha1입니다.
Cisco IDs 로그:

```
 com.cisco.ccbu.ids IdSSAMLAsyncServlet.java:298 - com.sun.identity.saml2.common.SAML2Exception
.com.sun.identity.saml2.common.saml2Utils.verifyResponse(SAML2Utils.java:425) at com.sun.identit
com.sun.identity.saml2.profile.SPACSUtils.processResponseForFedlet(SPACTILSSPACES.SPACES.SPACES2
) COM.CISCO.CCBU.IDS.AUTH.API.IdSSAMLAsyncServlet.getAttributesMapFromSAMLResponse(IdSSAMLAsyncS
```

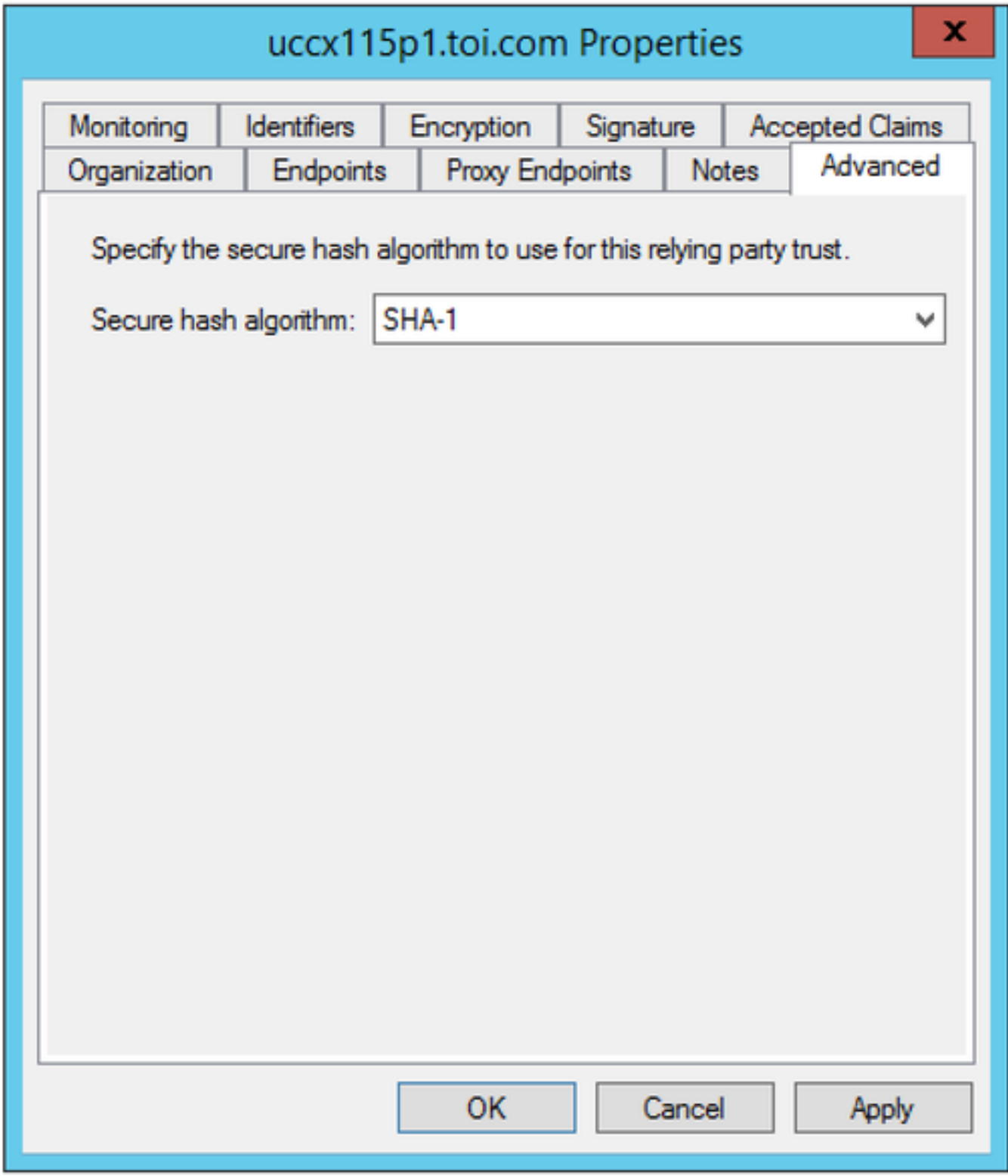
가능한 원인

AD FS는 SHA-256을 사용하도록 구성되어 있습니다.

권장 작업

서명 및 암호화에 SHA-1을 사용하도록 AD FS를 업데이트합니다.

1. AD FS 시스템에 대한 RDP입니다.
2. AD FS 콘솔을 엽니다.
3. 당사자 **신뢰** 당사자 **트러스트를** 선택하고 **속성**을 클릭합니다.
4. 고급 탭을 **선택합니다**.
5. 드롭다운 목록에서 SHA-1을 선택합니다.



4. 발신 클레임 규칙이 올바르게 구성되지 않음

문제 요약	브라우저에 "Could not retrieve user identifier from SAML response./Could not retrieve user princip 검색할 수 없음)"라는 500 오류가 발생하여 로그인 요청이 실패합니다. uid 및/또는 user_principal이 발신 클레임에 설정되지 않았습니다.
장애 단계	SAML 응답 처리
오류 메시지	**브라우저:** 500 오류 메시지: IdP 구성 오류:SAML을 처리하지 못했습니다. SAML 응답에서 사용자 식별자를 검색할 수 없습니다./SAML 응답에서 사용자 계정을 검색할 수 없

AD FS 이벤트 뷰어:
오류 없음
Cisco IDs 로그:

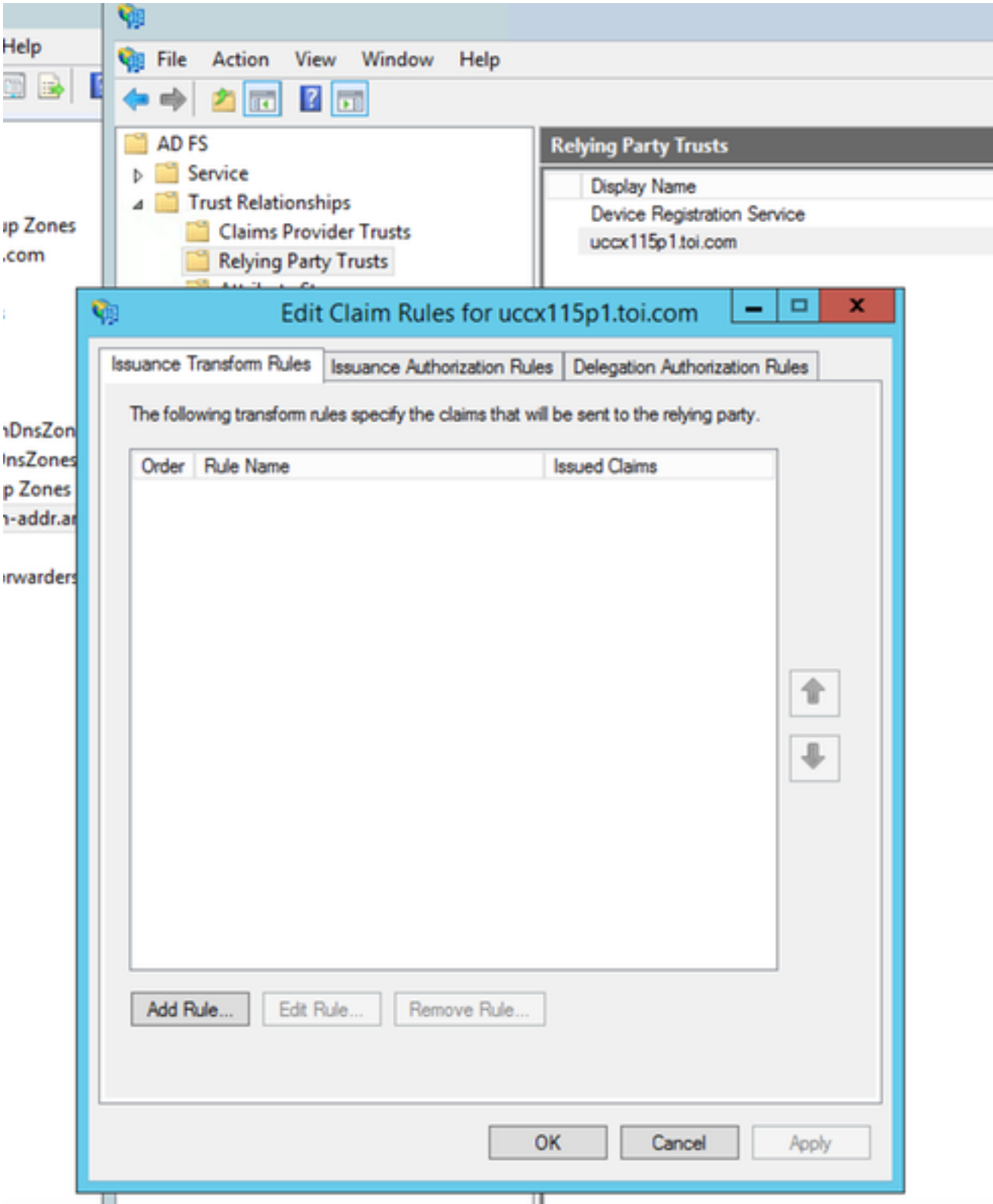
```
 com.cisco.ccbu.ids IdSSAMLAsyncServlet.java:294 - com.sun.identity.saml.common.SAMLException
.com.cisco.ccbu.ids.auth.api.IdSSAMLAsyncServlet.validateSAMLAttributes(IdSSAMLAsyncServlet.java
com.cisco.ccbu.ids.auth.api.IdSSAMLAsyncServlet.processSamlPostResponse(IdSSAMLAsyncSyncServlet.
)
```

가능한 원인

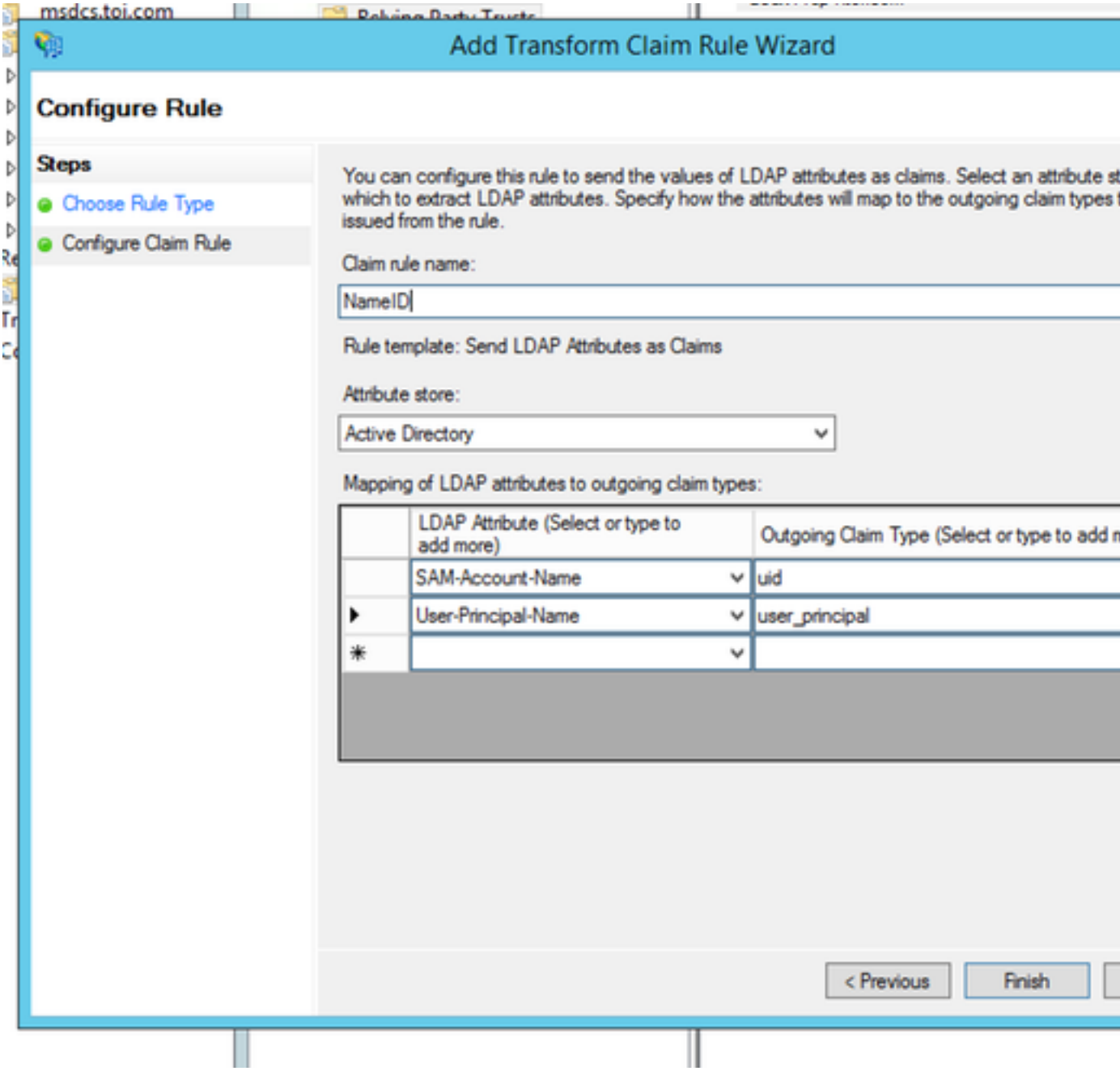
필수 발신 클레임(uid 및 user_principal)이 클레임 규칙에서 올바르게 구성되지 않았습니다.
NameID 클레임 규칙을 구성하지 않았거나 uid 또는 user_principal이 제대로 구성되지 않은 경우
NameID 규칙이 구성되지 않았거나 user_principal이 올바르게 매핑되지 않은 경우 Cisco IdS는 use
uid가 올바르게 매핑되지 않은 경우 Cisco IdS는 uid가 검색되지 않음을 나타냅니다.
AD FS 클레임 규칙에서 "user_principal" 및 "uid"에 대한 특성 매핑이 IdP 컨피그레이션 가이드(다음

권장 작업

1. AD FS 시스템에 대한 RDP.
2. 신뢰 당사자 트러스트에 대한 클레임 규칙을 편집합니다.



3. user_principal 및 uid가 올바르게 매핑되었는지 확인합니다.



5. 송신 클레임 규칙이 페더레이션 AD FS에 올바르게 구성되지 않았습니다.

문제 요약	브라우저에 "Could not retrieve user identifier from SAML response(SAML 응답에서 사용자 식별자 검색할 수 없습니다." AD FS가 페더레이션 AD FS인 경우
장애 단계	SAML 응답 처리
오류 메시지	**브라우저** 500 오류 메시지: IdP 구성 오류:SAML 처리 실패 SAML 응답에서 사용자 식별자를 검색할 수 없습니다./ SAML 응답에서 사용자 계정을 검색할 수 없 **AD FS 이벤트 뷰어:** 오류 없음 **Cisco IDs 로그:** `com.cisco.ccbu.ids IdSSAMLAsyncServlet.java:294 - com.sun.identity.saml.common.SAMLException .com.cisco.ccbu.ids.auth.api.IdSSAMLAsyncServlet.validateSAMLAttributes(IdSSAMLAsyncServlet.java com.cisco.ccbu.ids.auth.api.IdSSAMLAsyncServlet.processSamlPostResponse(IdSSAMLAsyncSyncServlet. )`
가능한	페더레이션된 AD FS에는 누락된 구성이 더 필요합니다.

원인 권장 작업 페더레이션 AD의 AD FS 컨피그레이션이 Configure Cisco IdS and AD FS(Cisco ID 및 AD FS 구성

6. 사용자 지정 클레임 규칙이 올바르게 구성되지 않음

문제 요약 브라우저에 "Could not retrieve user identifier from SAML response./Could not retrieve user princip
./SAML 응답에서 사용자 계정을 검색할 수 없음)"라는 500 오류가 발생하여 로그인 요청이 실패합
uid 및/또는 user_principal이 발신 클레임에 설정되지 않았습니다.

장애 단계 SAML 응답 처리

오류 메시지
브라우저
500 오류 메시지:
IdP에서 SAML 어설션이 실패했습니다(상태 코드:urn:oasis:names:tc:**SAML:2.0:status:Requester/**
다시 시도하십시오.

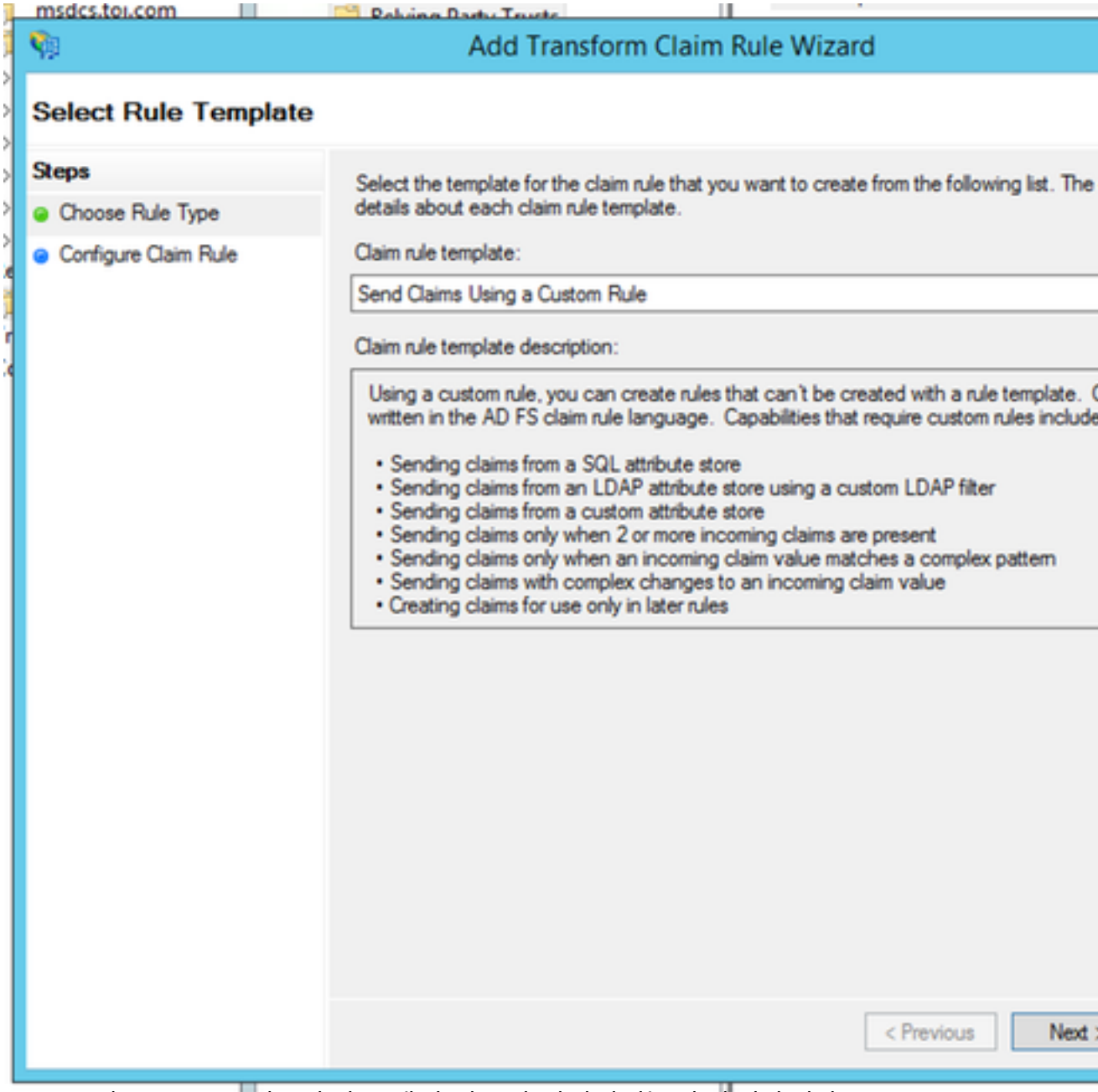
AD FS 이벤트 뷰어:
SAML 인증 요청에 NameID 정책이 충족되지 않았습니다.
요청자:myids.cisco.com
이름 식별자 형식:urn:oasis:names:tc:SAML:2.0:nameid-format:transient
SPName한정자:myids.cisco.com
예외 정보:
MSIS1000:SAML 요청에 발급된 토큰에 의해 충족되지 않은 NameIDPolicy가 포함되어 있습니다.요
:urn:oasis:names:tc:SAML:2.0:nameid-format:transient SPNameQualifier:myids.cisco.com. 실제 Na
이 요청이 실패했습니다.
사용자 작업
AD FS 2.0 관리 스냅인을 사용하여 필요한 이름 식별자를 생성하는 컨피그레이션을 구성합니다.
Cisco IdS 로그:

```
2016-08-30 09:45:30.471 IST(+0530) [IdSEndPoints-SAML-82] INFO com.cisco.ccbu.ids SAML2SPAdapter
Value="urn:oasis:names:tc:SAML:2.0:status:Requester"> <samlp:StatusCode Value="urn:oasis:names:t
</samlp:StatusStatusCode> </samlp:StatusStatusRequestStatusStatusStatusStatusStatus> </samlp Sta
</saml:StatusRequestStatusStatus> </StatusStatus>:  2016-08-30 09:45:30.471 IST(+0530) [IdSEndPo
( com.sun.identity.common.SAML.SAML.common.ID.SAML.common.SAML.SAML2.SAML.ID.common.SAML.ISL). :
.com.sun.identity.saml2.common.saml2Utils.verifyResponse(SAML2Utils.java:425) at com.sun.identit
com.sun.identity.saml2.profile.SPACSUtils.processResponseForFedlet(SPACTILSSPACES.SPACES.SPACES2
) JAVA:2038)
```

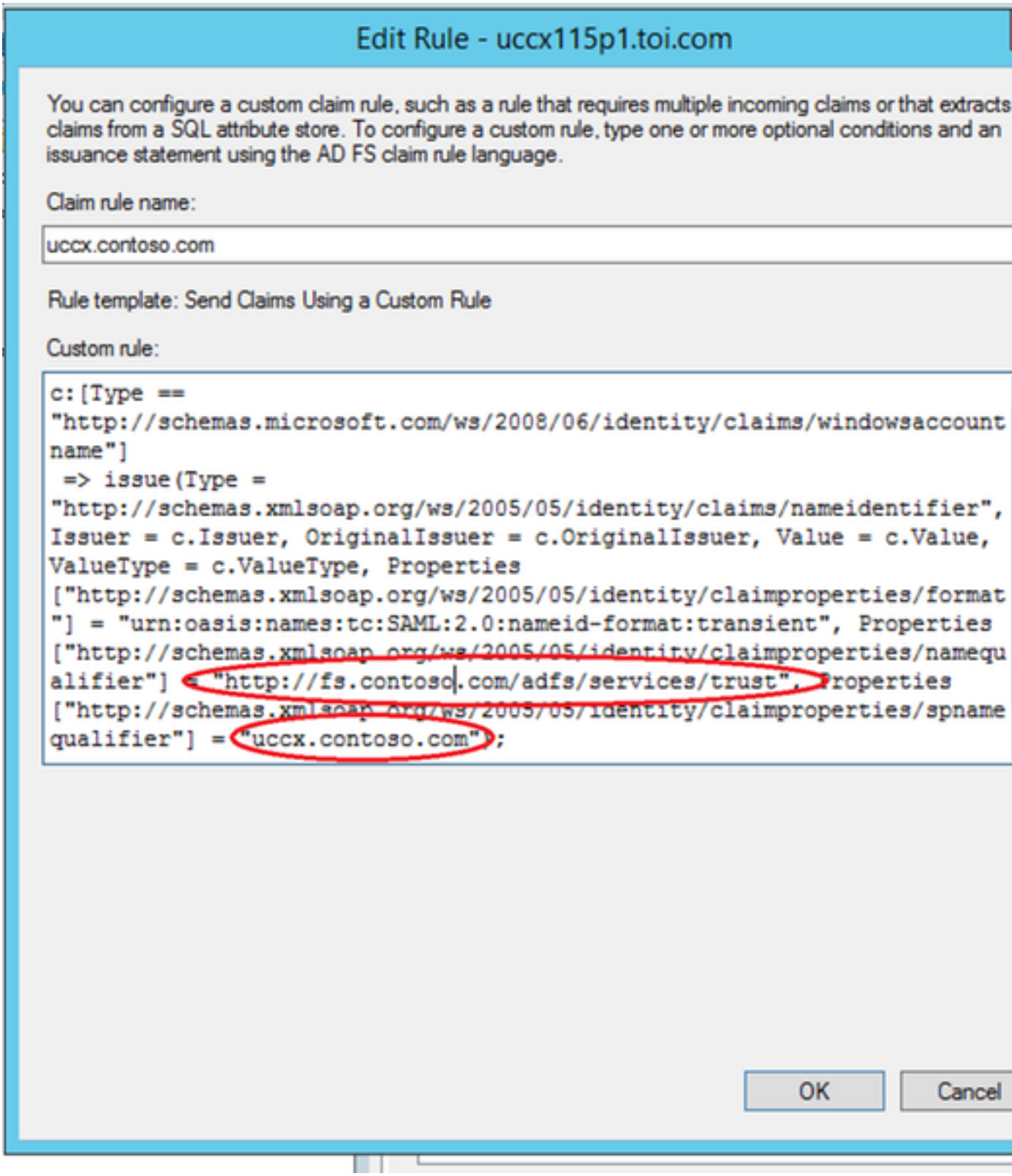
가능한 원인 사용자 지정 클레임 규칙이 올바르게 구성되지 않았습니다.

권장 작업 AD FS 클레임 규칙에서 "user_principal" 및 "uid"에 대한 특성 매핑이 컨피그레이션 가이드(다음 가

1. AD FS 시스템에 대한 RDP.
2. 사용자 지정 클레임 규칙에 대한 클레임 규칙을 수정합니다.



3. AD FS 및 Cisco IdS 정규화된 도메인 이름이 지정되었는지 확인합니다.



7. AD FS에 대한 요청이 너무 많습니다.

문제 요약 브라우저에서 로그인 요청이 500 오류와 함께 실패함(상태 코드: urn:oasis:names:tc:SAML:2.0:sta
AD FS 이벤트 보기 로그의 오류 메시지는 AD FS에 대한 요청이 너무 많음을 나타냅니다.

장애 단계 SAML 응답 처리

오류 메시지
브라우저
500 오류 메시지:
IdP 구성 오류:SAML 처리 실패
IdP에서 SAML 어설션이 실패했습니다(상태 코드:urn:oasis:names:tc:SAML:2.0:status:Responder
AD FS 이벤트 뷰어:

Microsoft.IdentityServer.Web.InvalidRequestException:
MSIS7042:**동일한 클라이언트 브라우저 세션이 마지막 단계에서 '6' 요청을 수행함 '16'초자세한 내용은 관리자에게 문의하십시오.**
Microsoft.IdentityServer.Web.FederationPassiveAuthentication.UpdateLoopDetectionCookie()
Microsoft.IdentityServer.Web.FederationPassiveAuthentication.SendSignInResponse(MSISSign

```
 XML:<Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event"> <System> <Provider Na
<EventID>364</EventID> version>0</Version> <Level>2</Level> <Task>0</Task> <Opcode>0</Opcode> <K
19T12:12:15:14:14:14:14.474662600Z" /> <EventRecordID>29385</EventRecordID> <Correlation Activit
ThreadID="392" /> <Channel>AD FS 2.0/Admin</Channel> <Computer>myadfs.cisco.com</Computer> <Secu
<UserData> <Event xmlns:auto-ns2="http://schemas.microsoft.com/win/2004/08/events" xmlns="http:/
<EventData>Microsoft.IdentityServer.Web.InvalidRequestException:MSIS7042: 16      '6'  .
.Microsoft.IdentityServer.Web.FederationPassiveAuthentication.UpdateLoopDetectionCookie()(Micros
</Data> </EventData> </Event> </UserData> </Event>
```

Cisco IDs 로그

```
2016-04-15 16:19:01.220 EDT(-0400)   [IdSEndPoints-1] com.cisco.ccbu.ids IdSEndPoint.java:102 -
.com.sun.identity.saml2.common.saml2Utils.verifyResponse(SAML2Utils.java:425) at com.sun.identit
com.sun.identity.saml2.profile.SPACSUtils.processResponseForFedlet(SPACTILSSPACES.SPACES.SPACES2
) COM.CISCO.CCBU.IDS.AUTH.API.IdSSAMLAsyncServlet.getAttributesMapFromSAMLResponse(IdSSAMLAsyncS
```

가능한 원인 동일한 브라우저 세션에서 AD FS로 들어오는 요청이 너무 많습니다.

일반적으로 프로덕션 환경에서는 이러한 일이 발생하지 않습니다.그러나 이러한 문제가 발생하면

권장 작업

1. AD FS Windows 이벤트 뷰어를 선택합니다.
2. 신뢰 당사자 트러스트 설정을 다시 확인하십시오.자세한 내용은 Cisco IdS 및 AD FS 구성을
3. 다시 로그인합니다.

8. AD FS가 어설션과 메시지를 모두 서명하도록 구성되지 않았습니다.

문제 요약 브라우저에서 500 오류가 발생하여 로그인 요청이 실패하고 오류 코드: invalidSignature

장애 단계 SAML 응답 처리

브라우저
500 오류 메시지:
오류 코드:invalidSignature
메시지:ArtifactResponse에 잘못된 서명이 있습니다.

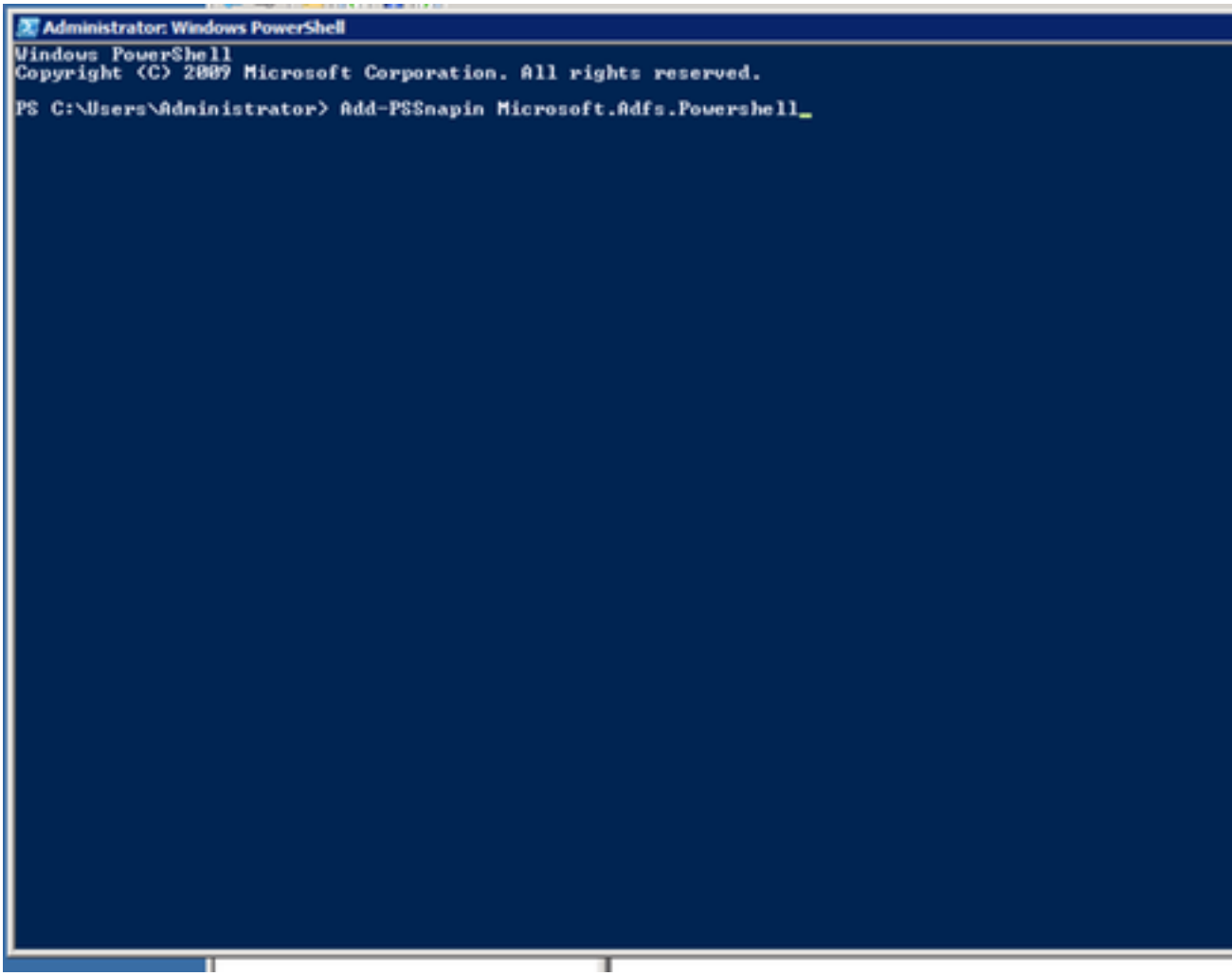
오류 메시지 **Cisco IDs 로그:**

```
2016-08-24 10:53:10.494 IST(+0530) [IdSEndPoints-SAML-241] INFO saml2error.jsp.java:75 - SAML
.2016-08-24 10:53:10.494 IST(+0530) [IdSEndPoints-SAML-241] ERROR com.cisco.ccbu.ids IdSSAMLAsyn
com.sun.identity.common.SAML.SAML2.common.SAML.SAML.common.SAML). :
.com.sun.identity.saml2.profile.SPACSUtils.getResponseFromPost(SPACSUtils.java:994)(com.sun.iden
com.sun.identity.saml2.profile.SPACSUtsu.processResponse(ForFedlet)
com.cisco.ccbu.ids.auth.api.IdSSAMLAsyncServlet.getAttributesMapFromSAMLResponse(IdSSAMLAsyncSer
```

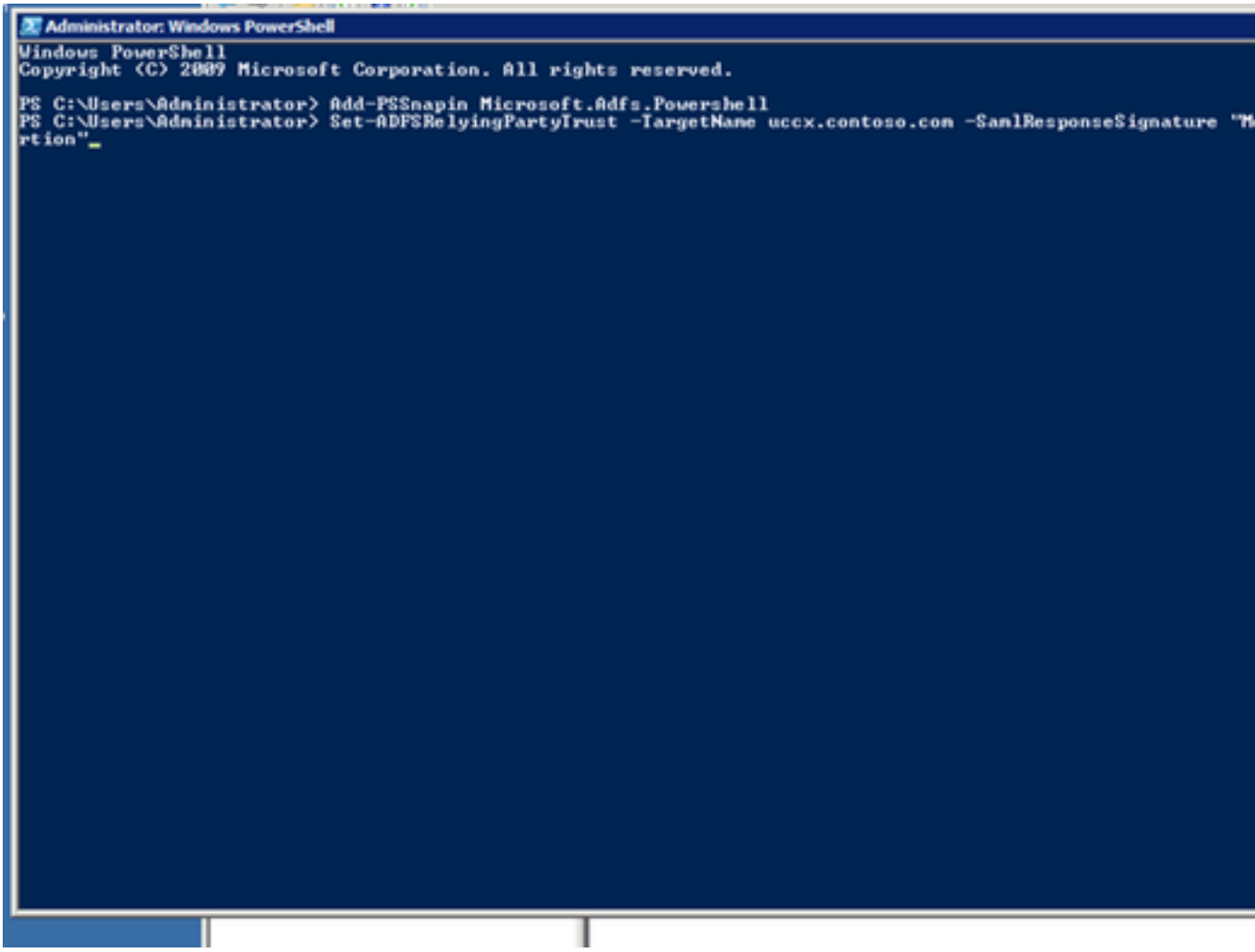
가능한 원인 AD FS가 어설션과 메시지를 모두 서명하도록 구성되지 않았습니다.

권장 작업

1. AD FS Powershell 명령을 실행합니다. Set-ADFSRelyingPartyTrust **-TargetName <Relying P SamlResponseSignature "MessageAndAssertion"**
2. AD 시스템에 대한 RDP.
3. Powershell을 **엽니다**.
4. 현재 세션에 Windows PowerShell 스냅인을 추가합니다.CmdLet이 역할 및 기능 추가의 일부 사용하는 경우에는 이 단계가 필요하지 않을 수 있습니다.



5. 메시지 및 어설션에 대해 AD FS 신뢰 당사자 트러스트를 추가합니다.



관련 정보

이는 다음 문서에 설명된 ID 제공자 컨피그레이션과 관련이 있습니다.

- https://www.cisco.com/c/en/us/support/docs/customer-collaboration/unified-contact-center-express/200612-Configure-the-Identity-Provider-for-UCCX.html
- 기술 지원 및 문서 – Cisco Systems