ADFS/IDs-probleemoplossing en gemeenschappelijke problemen

Inhoud

Inleiding

De interactie Security Association Markup Language (SAML) tussen Cisco Identity Service (IDS) en Active Directory Federation Services (AD FS) via een browser is de kern van het Single-aanmelding (SSO)-logbestand in flow. Dit document helpt u bij het oplossen van problemen met betrekking tot configuraties in Cisco IDs en AD FS, samen met de aanbevolen actie om deze op te lossen.

Cisco IDs-implementatiemodule

Product	Plaatsing
UCCX	Medeingezetene
PCCE	Gelijktijdige inwoner met CUIC (Cisco Unified Intelligence Center) en LD (Live Data)
UCCES	Gelijktijdige inwoner met CUIC en LD voor 2k implementaties. Standalone voor 4k- en 12k-implementaties.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco Unified Contact Center Express (UCCX) release 11.5 of Cisco Unified Contact Center Enterprise release 11.5 of Packaged Contact Center Enterprise (PCCE) release 11.5 indien van toepassing.
- Microsoft Active Directory - AD geïnstalleerd op Windows Server
- IDP (Identity Provider) - Active Directory Federation Service (AD FS) versie 2.0/3.0

Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Achtergrondinformatie

Nadat de vertrouwensrelatie tussen Cisco IDS en AD FS is ontstaan (zie hier voor details, gebruikelijk voor UCCX en UCCE), wordt van de beheerder verwacht dat hij Test SSO uitvoert dat is ingesteld in de pagina Instellingen van Identity Services Management om te verzekeren dat de configuratie tussen Cisco IDS en AD FS prima werkt. Als de test mislukt, gebruikt u de juiste toepassingen en suggesties die in deze handleiding zijn gegeven om het probleem op te lossen.

Toepassingen en logbestanden die handig kunnen zijn in het fouilleren

Toepassings-/logbestand	Details	Waar u het gereedschap vindt
Cisco IDs-logbestand	De logger van Cisco IDS zal om het even welke fout registreren die in Cisco IDs is gebeurd.	Gebruik RTMT om Cisco IDs-logboek halen. Zie voor informatie over het ge van RTMT de Guide voor gebruik var RTMT Let op dat de RTMT-naam **Cisco Ider Services** is. Om de logbestanden te vinden, navigeer dan naar **Cisco Iden**

Fedlet Logs	Lettertypen geven meer informatie over fouten van SAML die bij Cisco IDs optreden	**Service > log** Gebruik RTMT om Fedlet-logbestand krijgen. De locatie voor het Fedlet-logbestand dezelfde als de Cisco IDS-logboeken De fedlet-logboeken beginnen met he voorvoegsel **fedlet-**fedlet
Cisco IDs API-metriek	API-metriek kan worden gebruikt om fouten in te zien en te valideren die Cisco IDs API's mogelijk hebben teruggegeven en aantal verzoeken dat wordt verwerkt door Cisco idS	Gebruik RTMT om API-parameters te verkrijgen. Let op dat de RTMT-naam **Cisco Ider Services** is Dit wordt weergegeven onder een ap **map**. Let erop dat **saml_metrics.csv** e **autorze_metrics.csv** de relevante parameters voor dit document zijn.
Event Viewer in AD	Hiermee kunnen gebruikers de eventlogbestanden in het systeem bekijken. Elke fout in AD FS tijdens de verwerking van de SAML-aanvraag/het verzenden van de SAML-respons wordt hier geregistreerd.	In AD FS-machine, navigeer naar **Eve Viewer > Toepassingen** en **Servicesl >AdDFS 2.0 > Admin** In Windows 2008, start het evenemer **Configuratiescherm > Prestaties en onderhoud > Administratieve hulpmid** In Windows 2012 kunt u het starten v Control Panel\System en Security\Administration Tools. Bekijk uw Windows-documentatie om zien waar u het Event Viewer kunt vir
SAML Viewer	Een SAML Viewer zal helpen bij het bekijken van het SAML verzoek en de respons die van/naar Cisco IDs worden verzonden. Deze browser toepassing is zeer nuttig voor de analyse van SAML aanvraag/respons.	Dit zijn enkele voorgestelde SAML-kij die u kunt gebruiken om naar het SAM verzoek en de SAML-respons te kijke 1. Fiddler Hoe wordt Fidler gebrui AD FSFiddler Chrome Plugin 2. SAML Tracer - Firefox 3. SAML Chrome Panel

Stroomdiagram met afvoeropties

De verschillende stappen voor SSO-authenticatie worden in het beeld getoond, samen met en zuiverend artefacten bij elke stap in het geval van een storing in die stap.

In deze tabel worden de details gegeven over de manier waarop storingen bij elke stap van de SSO in de browser kunnen worden geïdentificeerd. De verschillende gereedschappen en hoe ze kunnen helpen bij het fouilleren worden ook gespecificeerd.

Stap	Hoe de fout in de browser te identificeren	Gereedschappen/logboek	Configuraties om te bekijken
Auditcodeaanvraag verwerken door Cisco-idS	In het geval van een fout wordt de browser niet opnieuw gericht naar het SAML-eindpunt of de AD FS, dan wordt een JSON-fout weergegeven	Cisco IDS-logbestanden - Geeft de fouten aan die optreden terwijl het registratieverzoek is gevalideerd en verwerkt. Cisco IDS API-metriek - Geeft het aantal	Clientregistratie

	door Cisco IDS, die aangeeft dat de client-ID of de URL omleiden ongeldig is.	verwerkte en mislukte verzoeken aan.	
SAML-aanvraag - initiatie door Cisco IDs	Tijdens het uitvallen wordt de browser niet opnieuw gericht naar AD FS en wordt een foutpagina/bericht weergegeven door Cisco IDS.	Cisco IDS-logbestanden - Geeft aan of er een uitzondering is of niet terwijl het verzoek is gestart. Cisco IDS API-metriek - Geeft het aantal verwerkte en mislukte verzoeken aan.	Cisco IDs in NIET_CONFIGURED-status.
SAML-aanvraag - verwerking door AD-FS	Wanneer u dit verzoek niet verwerkt, wordt er een foutpagina weergegeven door de AD FS-server in plaats van de inlogpagina.	Event Viewer in AD-FS - Geeft de fouten aan die optreden terwijl het verzoek wordt verwerkt. SAML browser plug-in - helpt het SAML-verzoek te zien dat naar de AD FS wordt verzonden.	Configuratie van leden van vertrouwen in IDP
Sending SAML-respons door AD-FS	Elke fout bij het verzenden van de respons resulteert in een foutpagina die wordt weergegeven door een AD FS-server nadat de geldige aanmeldingsgegevens zijn ingediend.	Event Viewer in AD-FS - Geeft de fouten aan die optreden terwijl het verzoek wordt verwerkt.	• Configuratie van leden van vertrouwen in IDP • Instelling van formulierverificatie in AD FS.
SAML-responsverwerking door Cisco IDs	Cisco IDS geeft een fout van 500 weer met de foutreden en een pagina voor snelle controle.	Event Viewer in AD-FS - Geeft de fout aan als AD FS een SAML-respons verstuurt zonder een succesvolle statuscode. SAML browser plug-in - helpt de SAML respons te zien die door AD FS wordt verstuurd om te identificeren wat fout is. Cisco IDS-logbestand - Geeft de fout/uitzondering aan die tijdens de verwerking is opgetreden. Cisco IDS API-metriek - Geeft het aantal verwerkte en mislukte verzoeken aan.	• Configuratie van Claimregels • Bericht- en bevestiging-signalering

Auteur-aanvraag verwerking door Cisco-idS

Het beginpunt van de SSO-inlognaam is, wat Cisco IDS betreft, het verzoek om een vergunningscode van een SSO-enabled-toepassing. De validatie van het API-verzoek wordt uitgevoerd om te controleren of het een verzoek van een geregistreerde cliënt betreft. Een succesvolle valideringsresultaten in de browser die wordt omgeleid naar het SAML-eindpunt van Cisco IDS. Elke mislukking in de aanvraag validatie resulteert in een foutpagina/JSON (JavaScript Notes) die wordt teruggestuurd van Cisco IDS.

Gemeenschappelijke fouten die tijdens dit proces zijn gemaakt

1. Clientregistratie is niet voltooid

Probleemsamenvatting	Aanmelden mislukt met 401 fout in de browser.

Foutbericht	**browser:**
	401 fout met dit bericht: {"error":"ongeldige_client", "error_Description": "Ongeldig
	Log Cisco IDs:
	`2016-09-02 00:16:58.604 IST(+0530) [IDSEndPoint-51] WARN com.cisco.cbu.ids IDSCo`
	`fb308a80050b2021f974f48a72ef9518a5e7ca69 bestaat niet (+0530) [IDSEandPoint-51]`
	`com.cisco.cbu.idSOAuthEndPoint.java:45 - verzoek om een vergunning voor het verw`
	`org.apache.oltu.oauth2.common.uitzondering.OAuthProblemException: ongeldige_clie`
	`org.apache.oltu.oauth2.common.uitzondering.OAuthProblemmException.error(OAuthPro`
	`com.cisco.cbu.ids.auth.validator.IDSAuthorizeGeliquam(IDSAuthorizeGeliquam ator.`
	`com.cisco.cbu.ids.auth.validator.IDSAuthorizeGeldigheidsator.validerendParameter`
	`op org.apache.oltu.oauth2.as.request.OAuthrequest.validering(OAuthrequest.java:6`

Mogelijke oorzaak	De client-registratie met Cisco IDS is niet voltooid.
Aanbevolen actie	Navigeren in naar Cisco IDS Management-console en bevestigen of de client is g dan de cliënten alvorens met de SSO te gaan.

2. Gebruikerstoegang op een applicatie met IP-adres/alternatieve hostnaam

Probleemsamenvatting	Aanmelden mislukt met 401 fout in de browser.
Foutbericht	**browser:** 401 fout met dit bericht: {"error":"ongeldige_redirectUri", "error_Description":"Indire Uri"}
Mogelijke oorzaak	Gebruiker heeft toegang tot de toepassing met IP Address/Alternate Host Name. In SSO-modus, als de toepassing benaderd wordt met IP, werkt deze niet. De toepassingen zouden door de hostname moeten worden benaderd waardoor zij in Cisco IDS zijn geregistreerd. Dit probleem kan voorkomen als de gebruiker toega heeft tot een alternatieve host-naam die niet bij Cisco IDS is geregistreerd.
Aanbevolen actie	Navigeer naar Cisco IDS Management-console en bevestig als de client is geregistreerd met de juiste URL en hetzelfde wordt gebruikt om de toepassing te benaderen.

SAML-aanvraag - initiatie door Cisco IDs

SAML-eindpunt van Cisco IDS is het beginpunt van de SAML-stroom in SSO-gebaseerde inlognaam. De initiatie van de interactie tussen Cisco IDS en AD FS wordt in deze stap geactiveerd. Voorwaarde is dat de Cisco IDS de AD-FS moet kennen om verbinding te maken met de corresponderende IDP-metagegevens die naar Cisco IDS moeten worden geüpload om deze stap te laten slagen.

Gemeenschappelijke fouten die tijdens dit proces zijn gemaakt

1. AAD FS-metagegevens die niet aan Cisco IDS zijn toegevoegd

Probleemsamenvatting	Aanmelden mislukt met 503 fout in de browser.
Foutbericht	**browser:** 503 fout met dit bericht: {"error":"service_niet"," error_Description": "SAML Metagegevens zijn niet geïnitialiseerd"}
Mogelijke oorzaak	IP-metagegevens zijn niet beschikbaar in Cisco IDS. De inrichting van het vertrou tussen Cisco IDS en ADs is niet volledig. Navigeer naar de console van het beheer van Cisco IDS en zie of IDS in **niet gevo** staat is.
Aanbevolen actie	Controleer of de IDP-metadata al dan niet geüpload zijn. Indien niet, uploadde de IDP-metadata van AD FS. Zie hier voor meer informatie.

SAML-aanvraag - verwerking door AD-FS

De verwerking van SAML-aanvragen is de eerste stap in de AD FS in de SSO-stroom. Het SAML-verzoek dat door Cisco IDS wordt verzonden, wordt in deze stap gelezen, gevalideerd en ontcijferd door AD-FS. Een succesvolle behandeling van dit verzoek leidt tot twee scenario's:

1. Als het om een nieuw logbestand in een browser gaat, toont AD FS het inlogformulier.Als het gaat om een herinloggen van een reeds geauthentiseerde gebruiker van een bestaande browser sessie, probeert AD FS de SAML reactie direct terug te sturen.

   Opmerking: De belangrijkste voorwaarde voor deze stap is dat de AD FS het vertrouwen van de responderende partij heeft ingesteld.

Gemeenschappelijke fouten die tijdens dit proces zijn gemaakt

1. AD-FS heeft niet het laatste SAML-certificaat van Cisco IDs.

Probleemsamenvatting	AD FS toont de loginpagina niet, maar toont een foutpagina.

Foutbericht	**browser**
	AD FS toont een fout pagina vergelijkbaar:
	Er was een probleem met toegang tot de site. Probeer nogmaals naar de website
	Als het probleem zich blijft voordoen, neemt u contact op met de beheerder van d referentienummer om het probleem te identificeren.
	Referentienummer: 1e602be-382c-4c49-af7a-5b70f3a7bd8e
	AD FS-Event Viewer
	De Federatiedienst vond een fout tijdens de verwerking van de SAML-verificatieaa
	Aanvullende gegevens
	`Uitzonderingsgegevens: Microsoft.IdentityModel.Protocols.XmlSignature.SignatureV`
	`SAML Message heeft een verkeerde handtekening. Afgever: 'myuccx.cisco.com'. Bij`
	`Microsoft.IdentityServer.Protocols.Saml.contract.SamlContractUtility.CreateSamlM`
	`bij Microsoft.IdentityServer.Service.SamlProtocol.SamlProtocolService.CreateErro`
	`Microsoft.IdentityServer.Service.SamlProtocol.Protocol ProtocolService.Procesaan`

Mogelijke oorzaak	Het vertrouwen van een betrouwbare partij wordt niet gevestigd of het certificaat v hetzelfde wordt niet geüpload naar de AD FS.
Aanbevolen actie	Voer vertrouwen in tussen AD en Cisco IDs met het nieuwste Cisco IDS-certificaa Zorg ervoor dat het Cisco-idS-certificaat niet is verlopen. U kunt het statusdashbo Management. Reinig het certificaat in de pagina Instellingen als dit het geval is. Voor meer informatie over het instellen van metagegevensvertrouwen tussen ADF

SAML-respons verzonden door AD-FS

De ADFS stuurt de SAML-respons terug naar de Cisco IDs via de browser nadat de gebruiker is geauthentiseerd. ADFS kan een SAML-respons terugsturen met een statuscode die succes of falen aangeeft. Indien de formulierverificatie niet in AD FS is ingeschakeld, duidt dit op een mislukkingsreactie.

Gemeenschappelijke fouten die tijdens dit proces zijn gemaakt

1. Formulierverificatie is niet ingeschakeld in AD FS

Probleemsamenvatting	browser toont NTLM inloggen, en faalt dan zonder dat u deze opnieuw naar Cisco hebt gericht.
Stap met fouten	Sending SAML-respons
Foutbericht	**browser:** browser toont inloggen NTLM, maar na succesvol inloggen faalt het met veel omleidingen.
Mogelijke oorzaak	Cisco IDS ondersteunt alleen op formulieren gebaseerde verificatie, formulierverif is niet ingeschakeld in ADFS.
Aanbevolen actie	Zie voor meer informatie over het mogelijk maken van een vorm van authenticatie ADFS 2.0-instelling voor formulierverificatie ADFS 3.0 Formulierverificatie-instelling

SAML-responsverwerking door Cisco IDs

In deze fase krijgt Cisco IDs een SAML-respons van ADs. Deze reactie kan een statuscode bevatten die succes of falen aangeeft. Een foutreactie van AD FS resultaten in een foutpagina en hetzelfde moet worden gezuiverd.

Tijdens een succesvolle SAML-respons kan de behandeling van het verzoek om deze redenen niet volstaan:

- Onjuiste IDP (AD FS)-metagegevens.
- Geen verwachte uitgaande claims van AD FS terug te winnen.
- Cisco IDs en AD FS-klokken zijn niet gesynchroniseerd.

Gemeenschappelijke fouten die tijdens dit proces zijn gemaakt

1. AD-FS-certificaat in Cisco-idS is niet het laatste.

Probleemsamenvatting	Aanmelden mislukt met 500 fout in de browser met foutcode als ongeldige handte
Stap met fouten	SAML-responsverwerking
Foutbericht	**browser:** 500 fout met dit bericht in de browser: Foutcode: ongeldige handtekeningen Bericht: Het ondertekeningscertificaat komt niet overeen met wat in de metagegev wordt gedefinieerd. **Viewer voor AD FS-gebeurtenissen:** Geen fout **Log Cisco IDs:** `2016-04-13 12:42:15.896 IST(+0530) defaultwachtwoord [IDSEndPoint-0] com.cisco.c IDSEndPoint.java:102 - Exception Processing request com.sun.Identity.saml2 Commo Het ondertekeningscertificaat komt niet overeen met wat in de metagegevens van d gedefinieerd. op com.sun.Identity.saml2.xmlsig.FMSigProvider.verify(FMSigProvide`

	com.sun.identiteit.saml2.protocol.impl.StatusResponseImpl.isSignatureValid(Statu op com.sun.Identity.saml2.profile SPACSUtils.getResponseFromPost (SPACSUtils.jav com.sun.identiteit.saml2.profile.SPACSUtils.getResponse (SPACSUtils.java:196)
Mogelijke oorzaak	De verwerking van SAML-respons is mislukt omdat het IDP-certificaat anders is d beschikbaar is.
Aanbevolen actie	Downloadt de laatste AD FS-metagegevens van: **https://<ADSL>/federationmetac 06/federationmetadata.xml** En uploaden het naar Cisco IDS via de gebruikersinterface voor identiteitsbeheer. Zie Cisco IDs en AD voor meer informatie configureren

2. Cisco IDS- en AD FS-klokken zijn niet gesynchroniseerd.

Probleemsamenvatting	Aanmelden mislukt met 500 fout in de browser met de statuscode: urn:oasis:namen:tc:SAML:2.0:status:Succes
Stap met fouten	SAML-responsverwerking
Foutbericht	**browser:** 500 fout met dit bericht: Fout in configuratie IDP: SAML-verwerking mislukt SAML-bewering mislukt bij IDP met statuscode: urn:oasis:namen:tc:SAML:2.0:sta Controleer de IDP-configuratie en probeer het opnieuw. **Cisco-idS-logboek** 2016-08-24 18:46:56.780 IST(+0530) [IDSEndPoint-SAML-22] FOUT com.cisco.cbu.ids IDSSAMLAsyncServlet.java:298 - SML-responsverwerking met uitzondering van com.sun.Identity.saml2.common.SAML2Exception: De tijd in ObjectConfirmationData com.sun.Identity.saml2.common.SAML2Utils.isBeonderSubfirmation(SAML2Utils.java:7 com.sun.identiteit.saml2.common.SAML2Utils.verifyResponse (SAML2Utils.java:609) com.sun.Identity.saml2.profile. SPACSUtils.processResponse (SPACSUtils.java:1050 com.sun.identiteit.saml2.profile.SPACSUtils.processResponseForFedlet (SPACSUtils com.cisco.cbu.ids.auth.api IDSSAMLAsyncServlet.getAttributesFromSAMLResponse (IDSSAMLAsyncServlet.java:472) op com.cisco.cbu.ids.auth.api.IDSSAMLAsyncServlet.processSamlPostResponse (IDSSAMLA syncServlet.java:258) op com.cisco.cbu.ids.auth.api.idSSAMLAsyncServlet.processIDSEndPointrequest(IDSSAML op com.cisco.cbu.ids.auth.api.i IDSEndPoint$1.run (IDSEndPoint.java:269) op java.util.parallelle.ThreadPoolExec.run(ThreadPoolExec.java:1145) op java.util.tegelijkertijd.ThreadPoolExec$Worker.run(Thread) PoolExecteur.java:615 java.lang.Thread.run(Thread.java:745)2016-08-24 18:24:20.510 IST (+0530) [pool-4 **Viewer:** Bekijk de velden nietVoor en nietOnorAfter <VOORWAARDEN NIETVoordat="2016-08-28T14:45:03.325Z" NotOnORAfter=" 28T15:45:03.325Z">
Mogelijke oorzaak	De tijd in het systeem van Cisco IDs en IDP is niet sync.
Aanbevolen actie	synchroniseer de tijd in Cisco IDS en AD FS systeem. Aanbevolen wordt dat het A Cisco IDS tijd gesynchroniseerd zijn met behulp van NTP-server.

3. Fout Signature Algorithm (SHA256 vs SHA1) in AD FS

Probleemsamenvatting	Aanmelden fout bij 500 fout in browser met statuscode:urn:oasis:namen:tc:SAML:2.0:status:Responder Foutbericht in AD FS Event View Log - fout Signature Algorithm (SHA256 vs SHA
Stap met fouten	SAML-responsverwerking
Foutbericht	**browser** 500 fout met dit bericht: Fout in configuratie IDP: SAML-verwerking mislukt SAML-bewering mislukt bij IDP met statuscode: urn:oasis:namen:tc:SAML:2.0:sta Controleer de IDP-configuratie en probeer het opnieuw. **Viewer voor AD FS-gebeurtenissen:**

SAML-aanvraag is niet ondertekend met het verwachte algoritme voor handteken
is ondertekend met algoritme voor handtekening http://www.w3.org/2001/04/xmld
sha256.
Verwacht algoritme voor handtekening is http://www.w3.org/2000/09/xmldsig#rsa-

Log Cisco IDs:

```
FOUT op com.cisco.cbu.ids IDSSAMLAsyncServlet.java:298 - SAML-responsverwerking
op com.sun.Identity.saml2.common.SAML2Exception: Ongeldige statuscode in respons
com.sun.Identity.saml2.common.SAML2Utils.verifyResponse (SAML2Utils.java:425) op
com.sun.identiteit.saml2.profile.SPACSUtils.processResponse (SPACSUtils.java:105
com.sun.Identity.saml2.profile.SPACSES Utils.processResponseForFedlet (SPACSUtil
com.cisco.cbu.ids.auth.api.IDSSAMLAsyncServlet.getAttributesMapFromSAMLAsyncServ
```

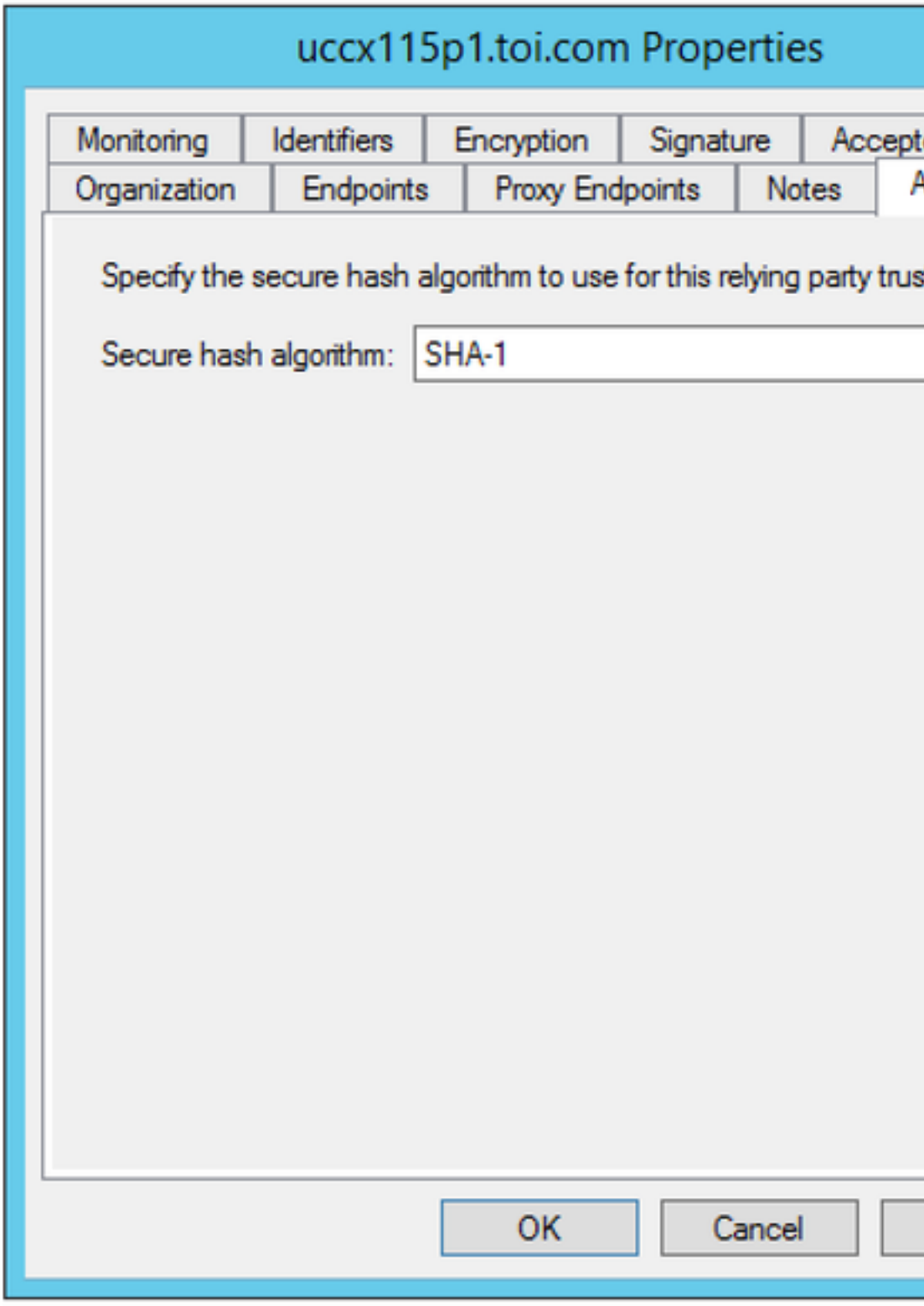
Mogelijke oorzaak

AD FS is ingesteld op SHA-256.

Update AD om SHA-1 te gebruiken voor het tekenen en coderen.

1. RDP naar het AD FS-systeem.
2. Open AD FS-console.
3. Selecteer het **vertrouwen** van de **Relay Party** en klik op **Properties**
4. Selecteer het tabblad **Geavanceerd**.
5. Selecteer SHA-1 in de vervolgkeuzelijst.

Aanbevolen actie



4. Aflopende claimregel is niet correct ingesteld

Probleemsamenvatting	Login request werkt niet met 500 fout op de browser met bericht "Kan gebruiker id terugkrijgen./Kon gebruiker main niet van SAML respons terugkrijgen." uid en/of user_main niet ingesteld in de vertrekkende claims.
Stap met fouten	SAML-responsverwerking
Foutbericht	**browser:** 500 fout met dit bericht: Fout in configuratie IDP: SAML-verwerking is mislukt. Het kon geen gebruiker identifier terugkrijgen van de SAML respons./Kon geen ge terugkrijgen van de SAML respons.

Viewer voor AD FS-gebeurtenissen:

Geen fout

Log Cisco IDs:

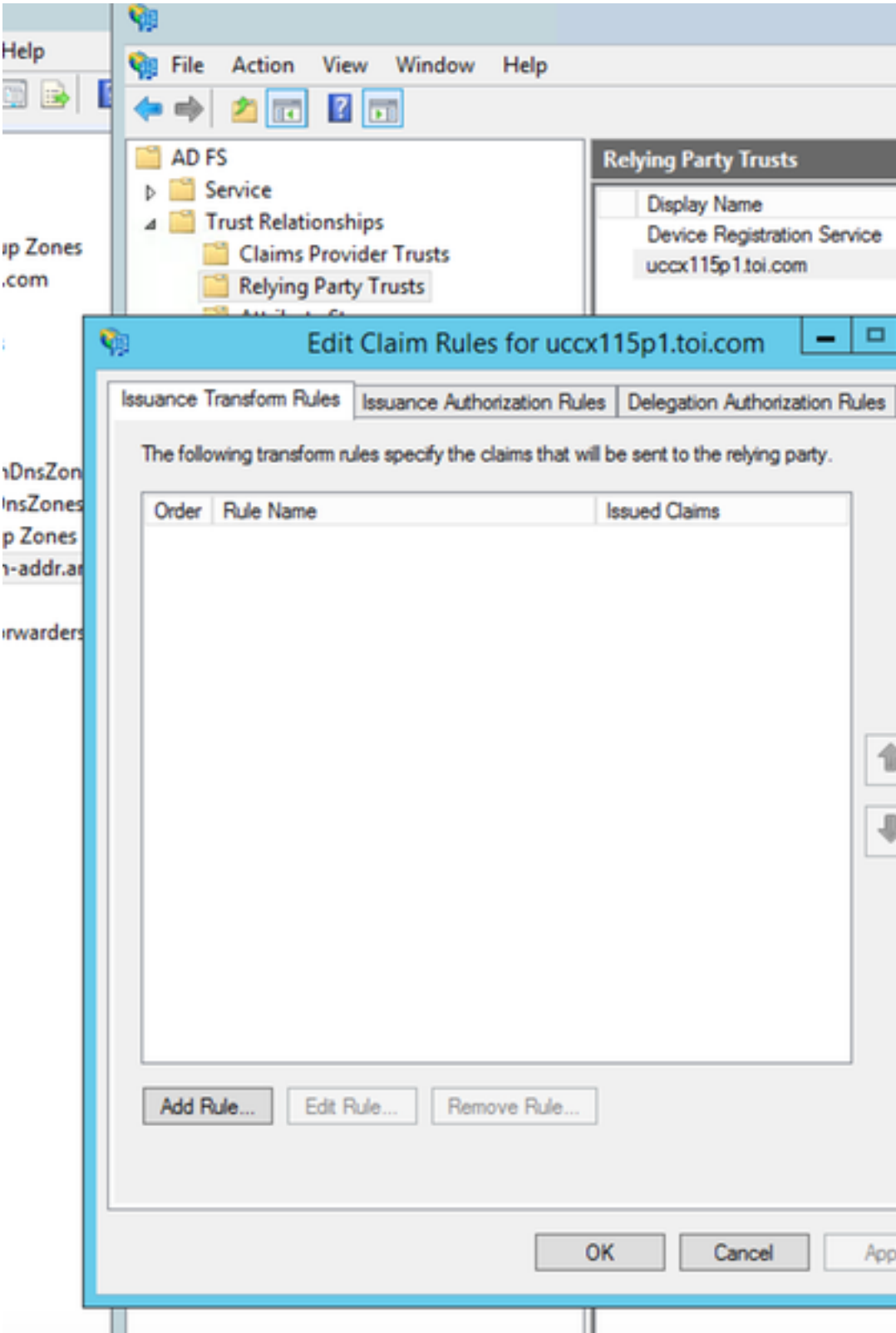
```
FOUT op com.cisco.cbu.ids IDSSAMLAsyncServlet.java:294 - SAML-responsverwerking
com.sun.Identity.saml.common.SAMLException: Geen identificatie van gebruiker doo
com.cisco.cbu.ids.auth.api.IDSSAMLAsyncServlet.valideringsrapportSAMLAttributes
op com.cisco.cbu.ids.auth.api.IDSSAMLAsyncServlet.procedureSaml PostResponse (ID
com.cisco.cbu.ids.auth.api.IDSSAMLAsyncServlet.procedureIDSEndPointApplication(I
```

Mogelijke oorzaak

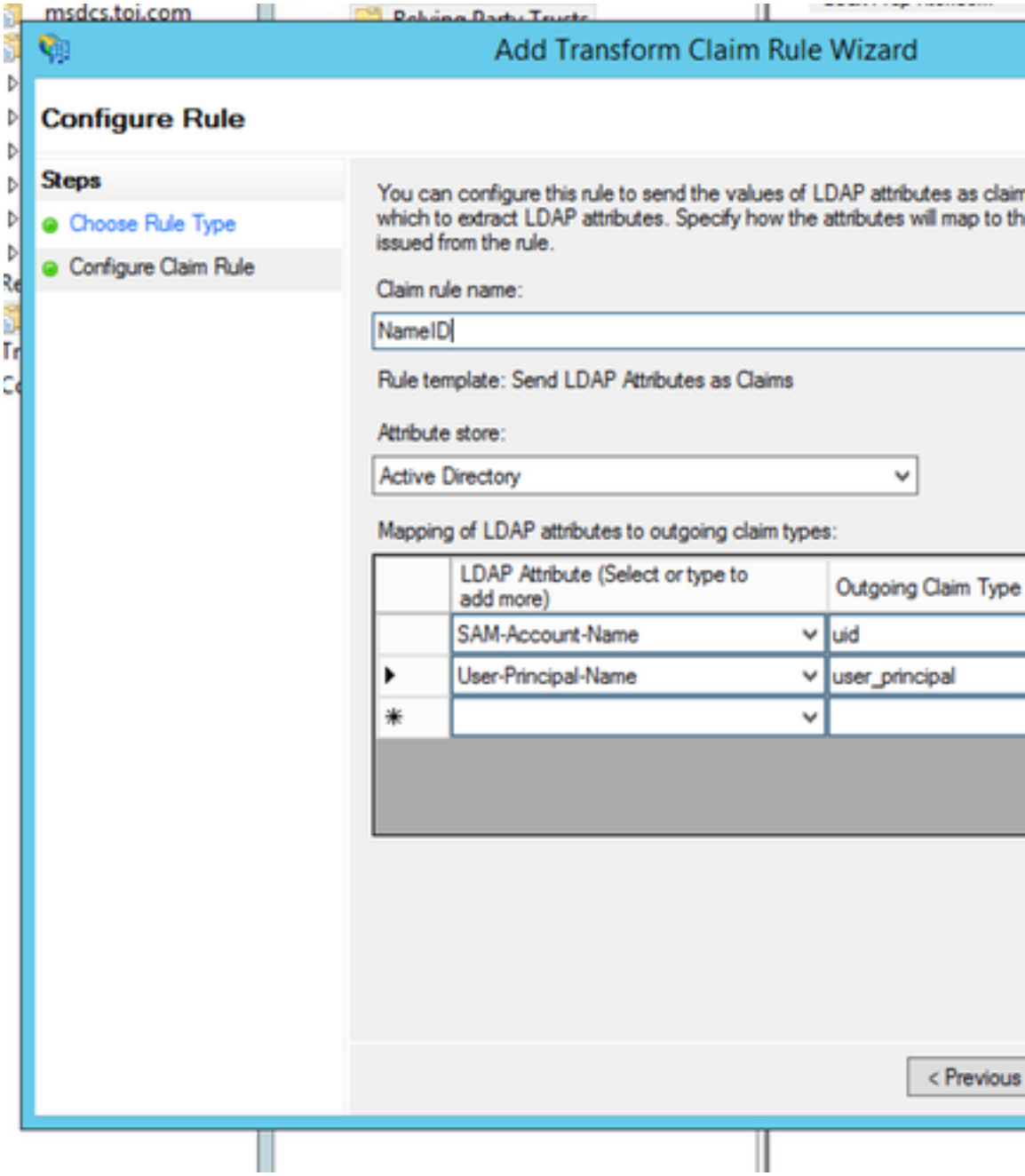
De verplichte uitgaande claims (uid en user_main) worden niet correct ingesteld ir
Als u de NameID claimregel niet hebt ingesteld of uid of user_main wordt niet goe
Als NameID regel niet wordt ingesteld of user_main niet correct in kaart wordt geb
user_main niet wordt opgehaald aangezien dit de eigenschap is die Cisco IDS zo
Als uid niet correct in kaart is gebracht, geeft Cisco IDS aan dat uid niet opgehaal
Zorg er onder AD FS claimregels voor dat attributenmapping voor "user_main" en
in de IDP Configuration-gids (welke gids?).

1. RDP naar AD FS-systeem.
2. Bewerk de claimregels voor het vertrouwen van de betrouwbare partij.

Aanbevolen actie



3. Controleer of de user_main en uid correct in kaart zijn gebracht



5. De aflopende schuldregel is in een federaal personeelsbestand niet correct ingesteld

Probleemsamenvatting	Aanmelden mislukt met 500 fout in de browser met bericht "Kan gebruiker identifi respons ophalen. of kon het hoofd van de gebruiker niet uit de SAML respons hal Federated AD FS is.
Stap met fouten	SAML-responsverwerking
Foutbericht	**browser** 500 fout met dit bericht: Fout in configuratie IDP: SAML-verwerking mislukt Het kon geen gebruiker identifier terugkrijgen van de SAML respons./ Het kon de gebruiker niet terugkrijgen van de SAML respons. **Viewer voor AD FS-gebeurtenissen:** Geen fout **Log Cisco IDs:** `FOUT op com.cisco.cbu.ids IDSSAMLAsyncServlet.java:294 - SAML-responsverwerking com.sun.Identity.saml.common.SAMLException: Geen identificatie van gebruiker doo com.cisco.cbu.ids.auth.api.IDSSAMLAsyncServlet.valideringsrapportSAMLAttributes (IDSSAMLAsyncServlet.java:231) op com.cisco.cbu.ids.auth.api.IDSSAMLAsyncServlet (IDSSAMLAsyncServlet.java:263) op`

```
com.cisco.cbu.ids.auth.api.IDSSAMLAsyncServlet.procedureIDSEndPointApplication(I
```

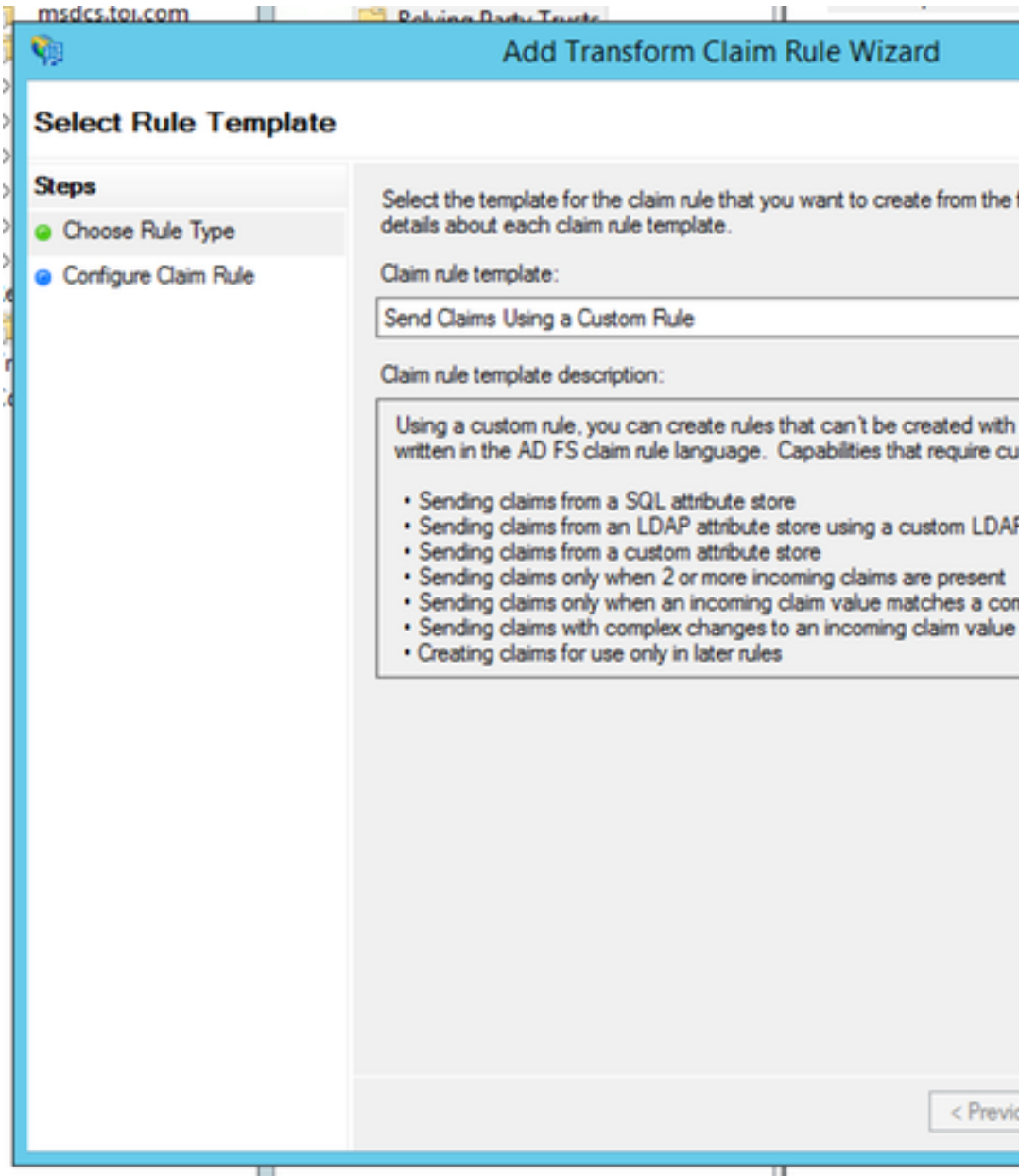
Mogelijke oorzaak	In een Federated AD FS zijn meer configuraties vereist die zouden kunnen ontbre
Aanbevolen actie	Controleer of de AD FS-configuratie in Federated AD is uitgevoerd zoals in het ge **met meerdere domeinen voor Federated AD FS** in Cisco IDS en AD FS instellen

6. Aangepaste setup-regels zijn niet correct ingesteld

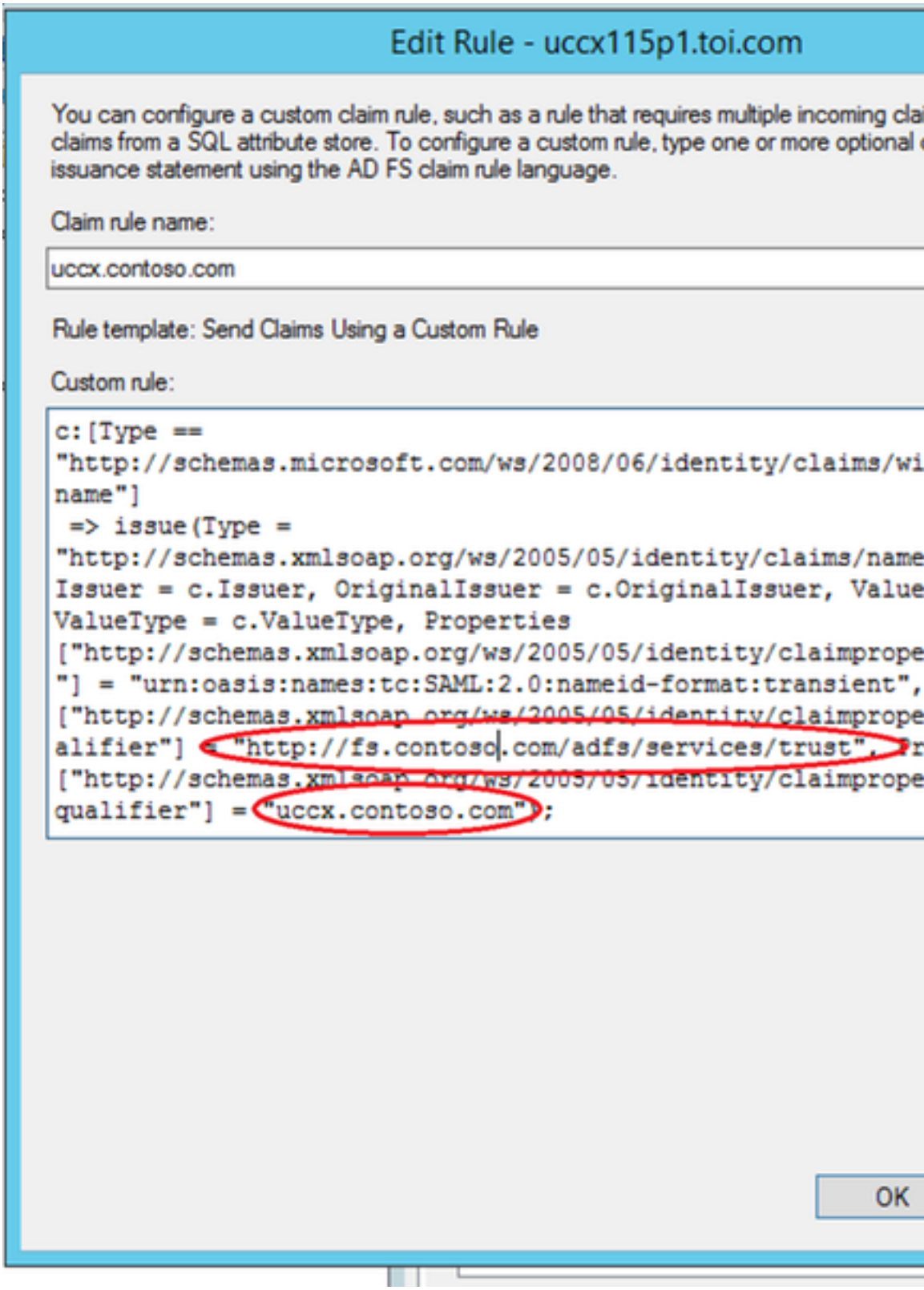
Probleemsamenvatting	Login request werkt niet met 500 fout op de browser met bericht "Kan gebruiker id terugkrijgen./Kon gebruiker main niet van SAML respons terugkrijgen." uid en/of user_main niet ingesteld in de vertrekkende claims.
Stap met fouten	SAML-responsverwerking **browser** 500 fout met dit bericht: SAML-bewering mislukt bij IDP met statuscode: urn:oasis:namen:tc:**SAML:2.0:status:requester/urn:oasis:namen:tc:SAML:2.0:statu** Controleer de IDP-configuratie en probeer het opnieuw.

Foutbericht	**Viewer voor AD FS-gebeurtenissen:**
	De SAML-authenticatieaanvraag had een NameID-beleid dat niet kon worden vol
	Aanvrager: myids.cisco.com
	Identificatiecode naam: urn:oasis:namen:tc:SAML:2.0:naamdicht:transient
	SPNameQualifier: myids.cisco.com
	Uitzonderingsgegevens:
	MSIS 1000: Het SAML-verzoek bevatte een naambeleid dat niet door de afgegev
	naamIDP-beleid: Laat maken: True Format: urn:oasis:namen:tc:SAML:2.0:naamID
	SPNameQualifier: myids.cisco.com. Feitelijke naamID eigenschappen: ongeldig.
	Dit verzoek is mislukt.
	Gebruikersactie
	Gebruik het AD FS 2.0 Management magnetisch-in om de configuratie te configur
	identifier geeft.
	Log van Cisco IDs:
	`2016-08-30 09:45:30.471 IST(+0530) [IDSEndPoint-SAML-82] INFO com.cisco.cbu.ids`
	`mislukt met code: 1. Antwoordstatus: <samlp:Status> <samlp:StatusCode`
	`Value="urn:oasis:namen:tc:SAML:2.0:status:requester"> <samlp:StatusCode`
	`Value="urn:oasis:namen:tc:SAML:2.0:status:OngeldigNameIDPPolicy"> </samlp:Status`
	`</min:Status> voor Auteur-aanvraag: n.v.t. 2016-08-30 09:45:30.471 IST(+0530) [I`
	`com.cisco.cbu.idSSAMLAsyncServlet.java:299 - SAML reageerverwerking is mislukt m`
	`com.sun.Identity.saml2.common.SAML2Exception: Ongeldige statuscode in respons. o`
	`com.sun.Identity.saml2.common.SAML2Utils.verifyResponse (SAML2Utils.java:425) op`
	`com.sun.identiteit.saml2.profile.SPACSUtils.processResponse (SPACSUtils.java:105`
	`com.sun.Identity.saml2.profile.SPACSES Utils.procesResponseForFedlet (SPACSUtils`

Mogelijke oorzaak	De regel Aangepaste claim wordt niet correct ingesteld. Zorg er onder AD FS claimregels voor dat de attributenmapping voor "user_main" in de configuratiegids (welke gids?). 1. RDP naar AD FS-systeem. 2. Bewerk de claimregels voor aangepaste claimregels.
Aanbevolen actie	



3. Controleer dat de AD FS- en Cisco IDS-domeinnamen volledig zijn gekwalifi



7. Te veel verzoeken om een antisubsidieaanvraag.

Probleemsamenvatting	Aanmelden fout bij 500 fout in browser met statuscode:urn:oasis:namen:tc:SAML Foutbericht in het logbestand voor de weergave van AD FS-gebeurtenissen geef verzoeken zijn om naar AD FS te gaan.
Stap met fouten	SAML-responsverwerking **browser**
Foutbericht	500 fout met dit bericht: Fout in configuratie IDP: SAML-verwerking mislukt SAML-bewering mislukt bij IDP met statuscode: urn:oasis:namen:tc:SAML:2.0:sta Controleer de IDP-configuratie en probeer het opnieuw.

Viewer voor AD FS-gebeurtenissen:
Microsoft.IdentityServer.Web.OngeldigeApplicationException:
MSIS 7042: **Dezelfde client browser sessie heeft '6' verzoeken gedaan in de laats**
16 seconden. Neem voor meer informatie contact op met de beheerder.
op Microsoft.IdentityServer.Web.FederationPassiveAuthentication.UpdateLoopD
bij Microsoft.IdentityServer.Web.FederationPassiveAuthentication.SendSignInR
(MSISSingInResponse)

```
Event Xml: <Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event">
Name="AD FS 2.0" Guid="{20E25DDB-09E5-404B-8A56-EDAE2F12EE81}" /> <EventID>364</
<versie>0</versie> <niveau>2</niveau> <taak>0</taak> <Opcode>0</opcode>
<Trefwoorden>0x800000000000001</Trefwoorden> <Trefwoorden>Tijd gecreëerd systeem
9T12:14:58.474662600Z" /> <EventRecordID>29385</EventRecordID> <Correlactiviteit
4DD5-B3B-0 565AC17BFE}"/> <UitvoeringsprocesID="2264" ThreadID="392" /> <Channel
2.0/Admin</Channel> <Computer>myadfs.cisco.com</Computer> <Security UserID="S-1-
129527365-1502263146-1105"/> </systeem> <UserData> <Event xmlns:auto-
ns2="http://schemas.microsoft.com/win/2004/08/events"
xmlns="http://schemas.microsoft.com/ActiveDirectoryFederationServices/2.0/Events
<Data>Microsoft.IdentityServer.Web.OngeldigeApplicationException: MSIS 7042: Dez
sessie heeft '6' verzoeken gedaan in de laatste '16' seconden. Neem voor meer in
met de beheerder. op
Microsoft.IdentityServer.Web.FederationPassiveAuthentication.UpdateLoopDetection
Microsoft.IdentityServer.Web.FederationPassiveAuthentication.VerzendSignInRespon
</Data> </Event> </Event> </UserData> </Event>
```

Cisco-idS-logboek

```
2016-04-15 16:19:01.220 EDT(-0400) defaultwachtwoord [IDSEndPoint-1] com.cisco.c
IDSEndPoint.java:102 - Exception Processing request com.sun.Identity.saml2 Commo
Ongeldige statuscode in respons. op com.sun.Identity.saml2.common.SAML2Utils.ver
(SAML2Utils.java:425) op com.sun.identiteit.saml2.profile.SPACSUtils.processResp
(SPACSUtils.java:1050) op com.sun.Identity.saml2.profile.SPACSES Utils.processRe
(SPACSUtils.java:2038) op
com.cisco.cbu.ids.auth.api.IDSSAMLAsyncServlet.getAttributesMapFromSAMLAsyncServ
```

Mogelijke oorzaak Er komen te veel verzoeken van dezelfde browser-sessie naar AD FS.
Dit zou normaal niet moeten gebeuren in de productie. Maar als je dit tegenkomt,

Aanbevolen actie

1. Controleer het AD FS Windows Event Viewer.
2. Controleer de instellingen van het vertrouwen van de Relying Partij. Zie Cisc informatie configureren en Cisco-*id* en ABBYY FS configureren
3. Reloïne.

8. AD FS is niet ingesteld voor zowel de bevestiging als het bericht.

Probleemsamenvatting Aanmelden mislukt met 500 fout in de browser met foutcode:ongeldigeSignature
Stap met fouten SAML-responsverwerking
browser
500 fout met dit bericht:
Foutcode:ongeldigeHandtekening
Bericht:Ongeldige handtekening in ArtifactResponse.
Log Cisco IDs:

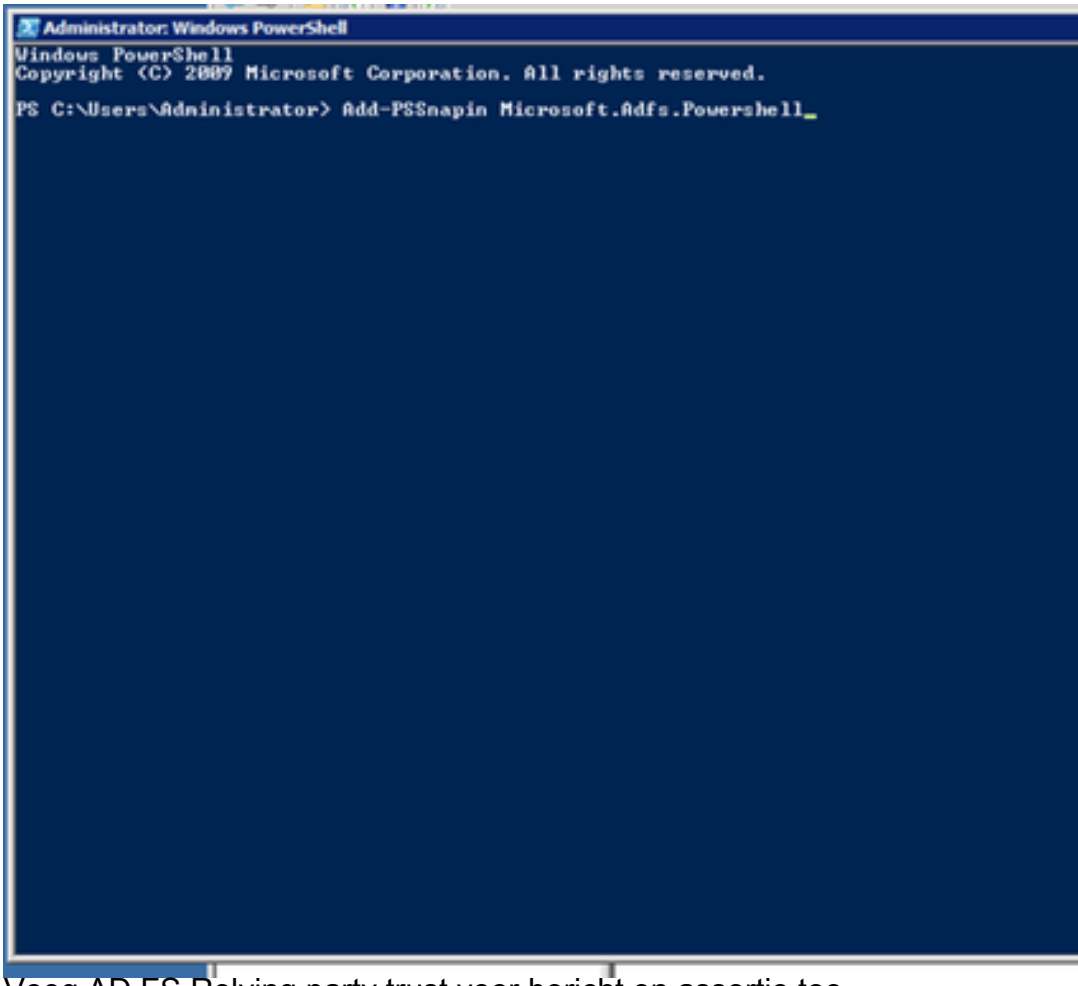
Foutbericht

```
2016-08-24 10:53:10.494 IST(+0530) [IDSEndPoints-SAML-241] INFO saml2error.jsp.
SAML-responsverwerking mislukt met code: ongeldigeHandtekening; bericht : Ongeld
ArtifactResponse. 2016-08-24 10:53:10.494 IST(+0530) [IDSEndPoints-SAML-241] FOU
com.cisco.cbu.idSSAMLAsyncServlet.java:298 - SAML respons verwerking mislukt met
com.sun.Identity.saml2.common.SAML2Exception: Ongeldige handtekening in antwoord
com.sun.Identity.saml2.profile.SPACSUtils.getResponseFromPost (SPACSUtils.java:9
com.sun.identiteit.saml2.profile.SPACSUtils.getResponse (SPACSUtils.java:196) op
com.sun.identiteit.saml2.profile 1.SPACSUtils.processResponseForFedlet (SPACSUti
com.cisco.cbu.ids.auth.api.IDSSAMLAsyncServlet.getAttributesMapFromSAMLResponse
```

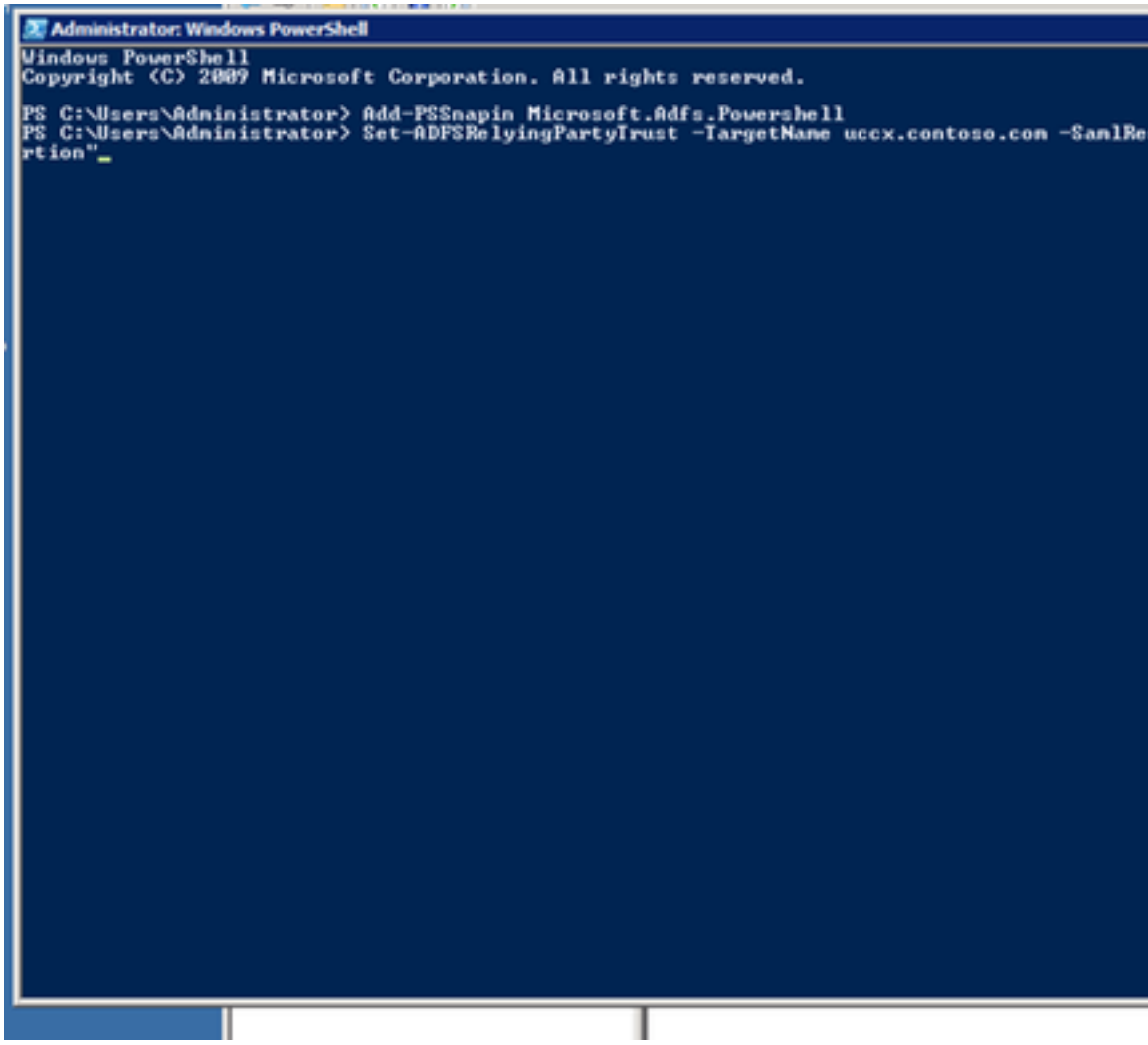
Mogelijke oorzaak AD FS is niet ingesteld voor zowel bevestiging als bericht.

Aanbevolen actie

1. Start de opdracht AD FS PowerShell: **Set-ADFSRelyingPartyTrust-TargetNa**
   Identifier> -SamlResponseSignature "MessageandAssertion" (Berichtmeldin
2. RDP naar AD-systeem.
3. Open **PowerShell**.
4. Voeg de haakjes van Windows PowerShell aan de huidige sessie toe. Deze
   het geval dat u ADFS 3.0 gebruikt omdat CmdLet al geïnstalleerd is als onde
   de rollen en functies.



5. Voeg AD FS Relying party trust voor bericht en assertie toe.



Gerelateerde informatie

Dit houdt verband met de configuratie van de in het artikel beschreven identiteitsaanbieder:

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