Fehlerbehebung und häufige Probleme mit ADFS/IDs

Inhalt

Einführung

Die SAML-Interaktion (Security Assertion Markup Language) zwischen Cisco Identity Service (IdS) und Active Directory Federation Services (AD FS) über einen Browser ist der Kern des Single-Sign-on (SSO)-Login-Flows. Dieses Dokument unterstützt Sie beim Debuggen von Problemen im Zusammenhang mit Konfigurationen in Cisco IDs und AD FS sowie bei der empfohlenen Vorgehensweise, um diese zu beheben.

Cisco IDS-Bereitstellungsmodelle

Produkt	Bereitstellung
UCCX	Co-Resident
PCCE	Co-Resident mit CUIC (Cisco Unified Intelligence Center) und LD (Live-Daten)
UCCE	Resident gemeinsam mit CUIC und LD für 2.000 Bereitstellungen. Standalone für 4.000- und 12.000-Bereitstellungen.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Cisco Unified Contact Center Express (UCCX) Version 11.5 oder Cisco Unified Contact Center Enterprise Release 11.5 oder Packaged Contact Center Enterprise (PCCE) Release 11.5.
- Microsoft Active Directory - AD installiert auf Windows Server
- IdP (Identity Provider) - Active Directory Federation Service (AD FS) Version 2.0/3.0

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardwareversionen beschränkt.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Hintergrundinformationen

Nachdem die Vertrauensbeziehung zwischen Cisco IdS und AD FS hergestellt wurde (für UCCX und UCCE übliche Informationen finden Sie hier), sollte der Administrator Test SSO Set (SSO-Einrichtung) auf der Seite Einstellungen des Identity Service Management (Identitätsservicemanagements) ausführen, um sicherzustellen, dass die Konfiguration zwischen Cisco IDS und AD FS funktioniert. Wenn der Test fehlschlägt, verwenden Sie die entsprechenden Anwendungen und Vorschläge in diesem Leitfaden, um das Problem zu beheben.

Anwendungen und Protokolle, die beim Debuggen nützlich sein können

Anwendung/Protokoll	Details	Wo finde ich das Tool?
Cisco IDs-Protokoll	Die Cisco IDs-Protokollierung protokolliert alle Fehler, die in Cisco IDs aufgetreten sind.	Verwenden Sie RTMT, um Cisco IDs abzuruf Informationen zur Verwendung von RTMT finden Sie im Benutzerhandbuch für RTMT. Bitte beachten Sie, dass der RTMT-Name **Cis Identity Service** ist. Um die Protokolle zu finde navigieren Sie zu **Cisco Identity Service > log**

Fedlet-Protokolle	Fedlet-Protokolle enthalten weitere Details zu SAML-Fehlern, die in Cisco IDs auftreten.	Verwenden Sie RTMT, um Fedlet-Protokolle abzurufen. Der Speicherort für das Fedlet-Protokoll ist identisch mit den Cisco IDs-Protokollen. Die Fedlet-Protokolle beginnen mit dem Präfi **fedlet-**
Kennzahlen der Cisco IDS API	Anhand von API-Metriken können Fehler, die von Cisco IDs zurückgegeben wurden, sowie die Anzahl der von Cisco IDs verarbeiteten Anforderungen geprüft und validiert werden.	Verwenden Sie RTMT, um API-Metriken abzurufen. Bitte beachten Sie, dass der RTMT-Name **Cis Identity Service** ist. Dies wird unter einer separaten **Ordnermetrik** angezeigt. Bitte beachten Sie, dass **saml_metrics.csv** und **autorize_metrics.csv** di relevanten Metriken für dieses Dokument sin
Ereignisanzeige in AD FS	Ermöglicht Benutzern, die Ereignisprotokolle im System anzuzeigen. Jeder Fehler in AD FS bei der Verarbeitung der SAML-Anforderung/beim Senden der SAML-Antwort wird hier protokolliert.	Navigieren Sie im AD FS-Rechner zu **Event Viewer >Applications** and **Services Logs >AdDFS 2.0 > Admin** Starten Sie in Windows 2008 die Ereignisanzeige über **Systemsteuerung > Leistung und Wartung > Verwaltung.** Starten Sie es in Windows 2012 über Systemsteuerung\System und Sicherheit\Verwaltung. In der Dokumentation zu Ihrem Fenster könn Sie sehen, wo Sie die Ereignisanzeige finden können.
SAML-Viewer	Ein SAML-Viewer hilft Ihnen dabei, die SAML-Anforderung und -Antwort zu betrachten, die von/an Cisco IDs gesendet werden. Diese Browseranwendung ist sehr nützlich für die Analyse von SAML Request/Response.	Dies sind einige empfohlene SAML-Viewer, n denen Sie die SAML-Anforderung und -Antwo betrachten können. 1. Fiddler Verwendung von Filddler mit AD FSChrome-Plugin 2. SAML Tracer - Firefox 3. SAML-Chrome-Panel

Flussdiagramm mit Debugoptionen

Die verschiedenen Schritte für die SSO-Authentifizierung werden im Bild zusammen mit den Artefakten und dem Debuggen in jedem Schritt angezeigt, falls in diesem Schritt ein Fehler auftritt.

In dieser Tabelle finden Sie Details zum Identifizieren von Ausfällen in jedem Schritt der SSO im Browser. Die verschiedenen Tools und wie sie beim Debuggen helfen können, sind ebenfalls spezifiziert.

Schritt	So identifizieren Sie den Fehler im Browser	Tools/Protokoll	Konfigurationen fü Überprüfung
AuthCode-Anforderungsverarbeitung mit Cisco IDs	Im Fehlerfall wird der Browser nicht an den SAML-Endpunkt oder AD FS umgeleitet, und Cisco IDs zeigen einen JSON-Fehler	Cisco IDs-Protokolle - gibt die Fehler an, die beim Validieren und Verarbeiten der Authentifizierungsanfrage auftreten.	Client-Registrierur

	an, der anzeigt, dass die Client-ID oder die Redirect-URL ungültig ist.	Cisco IDS API-Metriken - gibt die Anzahl der verarbeiteten und fehlgeschlagenen Anfragen an.	
SAML-Anforderungsinitiierung durch Cisco IDS	Bei einem Ausfall wird der Browser nicht an AD FS umgeleitet, und Cisco IDs zeigen eine Fehlerseite bzw. eine Fehlermeldung an.	Cisco IdS-Protokolle - Gibt an, ob eine Ausnahme vorliegt oder nicht, während die Anforderung initiiert wird. Cisco IDS API-Metriken - gibt die Anzahl der verarbeiteten und fehlgeschlagenen Anfragen an.	Cisco IDs im Statu NOT_CONFIGUR
SAML-Anforderungsverarbeitung durch AD FS	Wenn diese Anforderung nicht bearbeitet wird, wird eine Fehlerseite vom AD FS-Server anstatt der Anmeldeseite angezeigt.	Ereignisanzeige in AD FS: gibt die Fehler an, die bei der Verarbeitung der Anforderung auftreten. SAML-Browser-Plugin - Hilft, die SAML-Anfrage anzuzeigen, die an die AD FS gesendet wird.	Konfiguration von Gruppenvertrauen
Senden der SAML-Antwort durch AD FS	Wenn die Antwort nicht gesendet wird, wird eine Fehlerseite vom AD FS-Server angezeigt, nachdem die gültigen Anmeldeinformationen übermittelt wurden.	Ereignisanzeige in AD FS - gibt die Fehler an, die bei der Verarbeitung der Anforderung auftreten.	• Konfiguration Gruppenvertra IDs • Einstellung fü Formularauthe rung in AD FS
SAML-Antwortverarbeitung durch Cisco IDS	Die Cisco IDs zeigen einen 500-Fehler mit dem Fehlergrund und eine schnelle Überprüfungsseite an.	Ereignisanzeige in AD FS - gibt den Fehler an, wenn AD FS eine SAML-Antwort ohne erfolgreichen Statuscode sendet. SAML-Browser-Plugin - Hilft, die SAML-Antwort zu sehen, die von AD FS gesendet wurde, um zu erkennen, was falsch ist. Cisco IdS-Protokoll - gibt den Fehler/die Ausnahme an, die während der Verarbeitung aufgetreten sind. Cisco IDS API-Metriken - gibt die Anzahl der verarbeiteten und fehlgeschlagenen	• Konfiguration Forderungsreg • Signierung vo Nachrichten u Assertionen

Anfragen an.

Bearbeitung von Autcode-Anfragen durch Cisco IDS

Der Ausgangspunkt für die SSO-Anmeldung bei der Cisco IDs ist die Anforderung eines Autorisierungscodes von einer SSO-aktivierten Anwendung. Bei der API-Anforderungsvalidierung wird überprüft, ob es sich um eine Anforderung eines registrierten Clients handelt. Eine erfolgreiche Validierung führt dazu, dass der Browser an den SAML-Endpunkt der Cisco IDS umgeleitet wird. Wenn bei der Anforderungsvalidierung ein Fehler auftritt, wird eine Fehlerseite/JSON (JavaScript Object Notation) von der Cisco IDS zurückgesendet.

Häufige Fehler, die während dieses Prozesses aufgetreten sind

1. Client-Registrierung nicht durchgeführt

Problemübersicht	Die Anmeldeanforderung schlägt im Browser mit dem Fehler 401 fehl.

Fehlermeldung	**Browser:**
	Fehler 401 mit dieser Meldung: {"error":"invalid_client","error_description":"Invalid Clien
	Cisco IDs-Protokoll:
	`2016-09-02 00:16:58.604 IST(+0530) [IdSEndPoints-51] WARN com.cisco.ccbu.ids IdSConfig`
	`fb308a80050b2021f974f48a72ef9518a5e7ca69 gibt es 2016-09-02 00:16:58.604 IST nicht. +`
	`ERROR com.cisco.ccbu.ids IdSOAuthEndPoint.java:45 - Ausnahmeverarbeitungs-Authentifizi`
	`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`
	`unter`
	`com.cisco.ccbu.ids.auth.validator.IdSAuthorizeValidator.validateRequiredParameters(IdS`
	`unter org.apache.oltu.oauth2.as.request.OAuthRequest.validate(OAuthRequest.java:63)`

Mögliche Ursache	Die Client-Registrierung bei Cisco IDs ist unvollständig.
Empfohlene Aktion	Navigieren Sie zur Cisco IDS Management Console, und überprüfen Sie, ob der Client wurde. Falls nicht, registrieren Sie die Clients, bevor Sie mit der SSO fortfahren.

2. Benutzer greift mithilfe der IP-Adresse/des alternativen Hostnamens auf die Anwendung zu.

Problemübersicht	Die Anmeldeanforderung schlägt im Browser mit dem Fehler 401 fehl.
Fehlermeldung	**Browser:** Fehler 401 mit dieser Meldung: {"error":"invalid_redirectUri","error_description":"Invlalid Redirect Uri"} Der Benutzer greift mithilfe der IP-Adresse/des alternativen Hostnamens auf die Anwen zu.
Mögliche Ursache	Wenn im SSO-Modus auf die Anwendung über IP zugegriffen wird, funktioniert sie nich Der Zugriff auf Anwendungen sollte über den Hostnamen erfolgen, über den sie in Cisc registriert sind. Dieses Problem kann auftreten, wenn der Benutzer auf einen alternative Hostnamen zugreift, der nicht bei Cisco IDs registriert ist.
Empfohlene Aktion	Navigieren Sie zur Cisco IDS-Managementkonsole, und überprüfen Sie, ob der Client r der richtigen Umleitungs-URL registriert ist und dieselbe URL für den Zugriff auf die Anwendung verwendet wird.

SAML-Anforderungsinitiierung durch Cisco IDS

SAML-Endpunkt der Cisco IDS ist der Ausgangspunkt des SAML-Flusses bei der SSO-basierten Anmeldung. In diesem Schritt wird die Interaktion zwischen Cisco IdS und AD FS ausgelöst. Voraussetzung hierfür ist, dass die Cisco IDs die AD FS für die Verbindung kennen, da die

entsprechenden IdP-Metadaten für diesen Schritt an die Cisco IDs hochgeladen werden müssen.

Häufige Fehler, die während dieses Prozesses aufgetreten sind

1. AD FS-Metadaten wurden Cisco IDs nicht hinzugefügt

Problemübersicht	Die Anmeldeanforderung schlägt im Browser mit dem Fehler 503 fehl.
Fehlermeldung	**Browser:** Fehler 503 mit dieser Meldung: {"error":"service_unavailable","error_description":"SAML Metadaten sind nicht initialisiert"}
Mögliche Ursache	In Cisco IDs sind keine IP-Metadaten verfügbar. Die Vertrauensstellung zwischen Cisco und AD FS ist nicht vollständig.
Empfohlene Aktion	Navigieren Sie zur Cisco IDS-Managementkonsole, und prüfen Sie, ob die IDs **nicht konfiguriert** sind. Bestätigen Sie, ob IDP-Metadaten hochgeladen wurden. Falls nicht, laden Sie die von AD FS heruntergeladenen IdP-Metadaten hoch. Weitere Informationen finden Sie hier.

SAML-Anforderungsverarbeitung durch AD FS

SAML Request Processing ist der erste Schritt im AD FS im SSO-Fluss. Die von der Cisco IDs gesendete SAML-Anfrage wird in diesem Schritt von AD FS gelesen, validiert und entschlüsselt. Die erfolgreiche Verarbeitung dieser Anforderung führt zu zwei Szenarien:

1. Wenn es sich um eine neue Anmeldung in einem Browser handelt, zeigt AD FS das Anmeldeformular an.Wenn es sich um eine erneute Anmeldung eines bereits authentifizierten Benutzers aus einer bestehenden Browsersitzung handelt, versucht AD FS, die SAML-Antwort direkt zurück zu senden.

   Hinweis: Die wichtigste Voraussetzung für diesen Schritt ist, dass die AD FS die Vertrauenswürdigkeit der antwortenden Partei konfiguriert.

Häufige Fehler, die während dieses Prozesses aufgetreten sind

1. AD FS verfügt nicht über das neueste SAML-Zertifikat der Cisco IDS.

Problemübersicht	AD FS zeigt die Anmeldeseite nicht an, sondern zeigt eine Fehlerseite an.

Fehlermeldung	**Browser**
	AD FS zeigt eine Fehlerseite ähnlich der folgenden an:
	Beim Zugriff auf die Website ist ein Problem aufgetreten. Versuchen Sie erneut, die We
	Wenn das Problem weiterhin besteht, wenden Sie sich an den Administrator dieser We
	Referenznummer an, um das Problem zu identifizieren.
	Referenznummer: 1ee602be-382c-4c49-af7a-5b70f3a7bd8e
	AD FS Event Viewer
	Beim Verarbeiten der SAML-Authentifizierungsanfrage ist beim Federation Service ein
	Zusätzliche Daten
	`Ausnahmedetails: Microsoft.IdentityModel.Protocols.XmlSignature.SignatureVerificationF`
	`SAML-Nachricht hat eine falsche Signatur. Emittent: 'myuccx.cisco.com'. unter`
	`Microsoft.IdentityServer.Protocols.Saml.Contract.SamlContractUtility.CreateSamlMessage`
	`unter Microsoft.IdentityServer.Service.SamlProtocol.SamlProtocolService.CreateErrorMes`
	`createErrorMessageRequest) unter Microsoft.IdentityServer.Service.SamlProtocol.`

	`SamlProtocolService.ProcessRequest(Message requestMessage)`
Mögliche Ursache	Die Vertrauenswürdigkeit der zugrunde liegenden Partei wurde nicht eingerichtet oder geändert, aber das gleiche Zertifikat wird nicht in das AD FS hochgeladen.
Empfohlene Aktion	Mit dem neuesten Cisco IDS-Zertifikat können Sie eine Vertrauensstellung zwischen Al Stellen Sie sicher, dass das Cisco IDS-Zertifikat nicht abgelaufen ist. Das Status-Dashb Service Management angezeigt. Wenn ja, generieren Sie das Zertifikat auf der Seite Ei Weitere Informationen zum Einrichten von Metadaten-Vertrauenswürdigkeit für ADFS u

SAML-Antwortsenden durch AD FS

Das ADFS sendet die SAML-Antwort über den Browser an die Cisco IDs zurück, nachdem der Benutzer erfolgreich authentifiziert wurde. ADFS kann eine SAML-Antwort mit einem Statuscode zurücksenden, der auf Erfolgreich oder Fehler hinweist. Wenn die Formularauthentifizierung in AD FS nicht aktiviert ist, gibt dies eine Failure-Antwort an.

Häufige Fehler, die während dieses Prozesses aufgetreten sind

1. Die Formularauthentifizierung ist in AD FS nicht aktiviert.

Problemübersicht	Der Browser zeigt die NTLM-Anmeldung an und schlägt dann fehl, ohne erfolgreich zur Cisco ID umzuleiten.
Fehlerschritt	SAML-Antwort senden
Fehlermeldung	**Browser:** Der Browser zeigt die NTLM-Anmeldung an, schlägt aber nach erfolgreicher Anmeldun vielen Umleitungen fehl.
Mögliche Ursache	Cisco IDs unterstützen nur die formbasierte Authentifizierung, die Formularauthentifizie ist in AD FS nicht aktiviert.
Empfohlene Aktion	Weitere Informationen zum Aktivieren der Formularauthentifizierung finden Sie unter: ADFS 2.0-Formularauthentifizierungseinstellungen ADFS 3.0-Formularauthentifizierungseinstellungen

SAML-Antwortverarbeitung durch Cisco IDS

In dieser Phase erhält Cisco IDS eine SAML-Antwort von AD FS. Diese Antwort kann einen Statuscode enthalten, der auf Erfolg oder Fehler hinweist. Eine Fehlerantwort von AD FS führt zu einer Fehlerseite, und dasselbe muss gedebuggt werden.

Während einer erfolgreichen SAML-Antwort kann die Verarbeitung der Anforderung aus folgenden Gründen fehlschlagen:

- Falsche IDP (AD FS)-Metadaten.
- Fehler beim Abrufen der erwarteten ausgehenden Ansprüche von AD FS.
- Cisco IDs und AD FS-Uhren werden nicht synchronisiert.

Häufige Fehler, die während dieses Prozesses aufgetreten sind

1. Das AD FS-Zertifikat in Cisco IDs ist nicht das neueste.

Problemübersicht	Die Anmeldeanforderung schlägt im Browser mit dem Fehler "Error Code as invalidSign (Fehlercode als ungültige Signatur) mit dem Fehler 500 fehl.
Fehlerschritt	SAML-Antwortverarbeitung
Fehlermeldung	**Browser:**

	500 Fehler mit dieser Meldung im Browser:
	Fehlercode: ungültige Signatur
	Nachricht: Das Signaturzertifikat stimmt nicht mit dem überein, was in den Entitätsmeta
	ist.
	AD FS Event Viewer:
	Kein Fehler
	Cisco IDs-Protokoll:
	`2016-04-13 12:42:15.896 IST(+0530) Standard-FEHLER [IdSEndPoints-0] com.cisco.ccbu.ids`
	`IdSEndPoint.java:102 - Ausnahmeverarbeitungsanfrage com.sun.saml2.common SAML2Ausnahme`
	`Signaturzertifikat stimmt nicht mit dem überein, was in den Entitätsmetadaten definie`
	`com.sun.identity.saml2.xmlsig.FMSigProvider.verify(FMSigProvider.java:331) unter`
	`com.sun.identity.saml2.protocol.impl.StatusResponseImpl.isSignatureValid(StatusRespons`
	`unter com.sun.identity.saml2.profile SPACSUtils.getResponseFromPost(SPACSUtils.java:9`
	`com.sun.identity.saml2.profile.SPACSUtils.getResponse(SPACSUtils.java:196)`

Mögliche Ursache	Die SAML-Antwortverarbeitung ist fehlgeschlagen, da das IdP-Zertifikat von dem in Cis verfügbaren Zertifikat abweicht.
Empfohlene Aktion	Laden Sie die neuesten AD FS-Metadaten herunter: **https://<ADFSServer>/federationm** **06/federationmetadata.xml** Upload auf Cisco IDs über die Benutzeroberfläche für das Identity Service Managemen Weitere Informationen finden Sie unter Konfigurieren von Cisco IDs und AD FS.

2. Cisco IDs und AD FS-Uhren werden nicht synchronisiert.

Problemübersicht	Die Anmeldeanforderung schlägt im Browser mit dem Statuscode 500 fehl: urn:oasis:names:tc:SAML:2.0:status:Success
Fehlerschritt	SAML-Antwortverarbeitung

Fehlermeldung	**Browser:**
	500 Fehler mit dieser Meldung:
	IDP-Konfigurationsfehler: SAML-Verarbeitung fehlgeschlagen
	SAML Assertion fehlgeschlagen von IdP mit Statuscode: urn:oasis:names:tc:SAML:2.0
	Überprüfen Sie die IDP-Konfiguration, und versuchen Sie es erneut.
	Cisco IDs-Protokoll
	`2016-08-24 18:46:56.780 IST(+0530) [IdSEndPoints-SAML-22] ERROR com.cisco.ccbu.ids`
	`IdSSAMLAsyncServlet.java:298 - SAML-Antwortverarbeitung fehlgeschlagen exception`
	`com.sun.identity.saml2.common.SAML2Ausnahme: Die Zeit in SubjectConfirmationData ist`
	`com.sun.identity.saml2.common.SAML2Utils.isBearerSubjectConfirmation(SAML2Utils.java:`
	`com.sun.identity.saml2.common.SAML2Utils.verifyResponse(SAML2Utils.java:609) unter`
	`com.sun.saml2.profile SPACSUtils.processResponse(SPACSUtils.java:1050) unter`
	`com.sun.identity.saml2.profile.SPACSUtils.processResponseForFedlet(SPACSUtils.java:20`
	`com.cisco.ccbu.ids.auth.api.`
	`SSAMLAsyncServlet.getAttributesMapFromSAMLResponse(IdSSAMLAsyncServlet.java:472) at`
	`com.cisco.ccbu.ids.auth.api.IdSSAMLAsyncServlet.processSamlPostResponse(IdSSAMLASyncS`
	`unter`
	`com.cisco.ccbu.ids.auth.api.IdSSAMLAsyncServlet.processIdSEndPointRequest(IdSSAMLAsync`
	`unter com.cisco.ccbu.ids.auth.api.IdSE ndPoint$1.run(IdSEndPoint.java:269) unter`
	`java.util.Gleichzeitig.ThreadPoolExecutor.runWorker(ThreadPoolExecutor.java:1145) unte`
	`java.util.Gleichzeitig.ThreadPoolExecutor$Worker.run(ThreadPoolExecutor.java:6 15) be`
	`java.lang.Thread.run(Thread.java:745)2016-08-24 18:24:20.510 IST(+0530) [pool-4-thread`
	SAML-Viewer:
	Suchen Sie die Felder NotBefore und NotOnOrAfter.
	<Bedingungen nichtvor="2016-08-28T14:45:03.325Z" NotOnOrAfter="2016-08-28T15:4

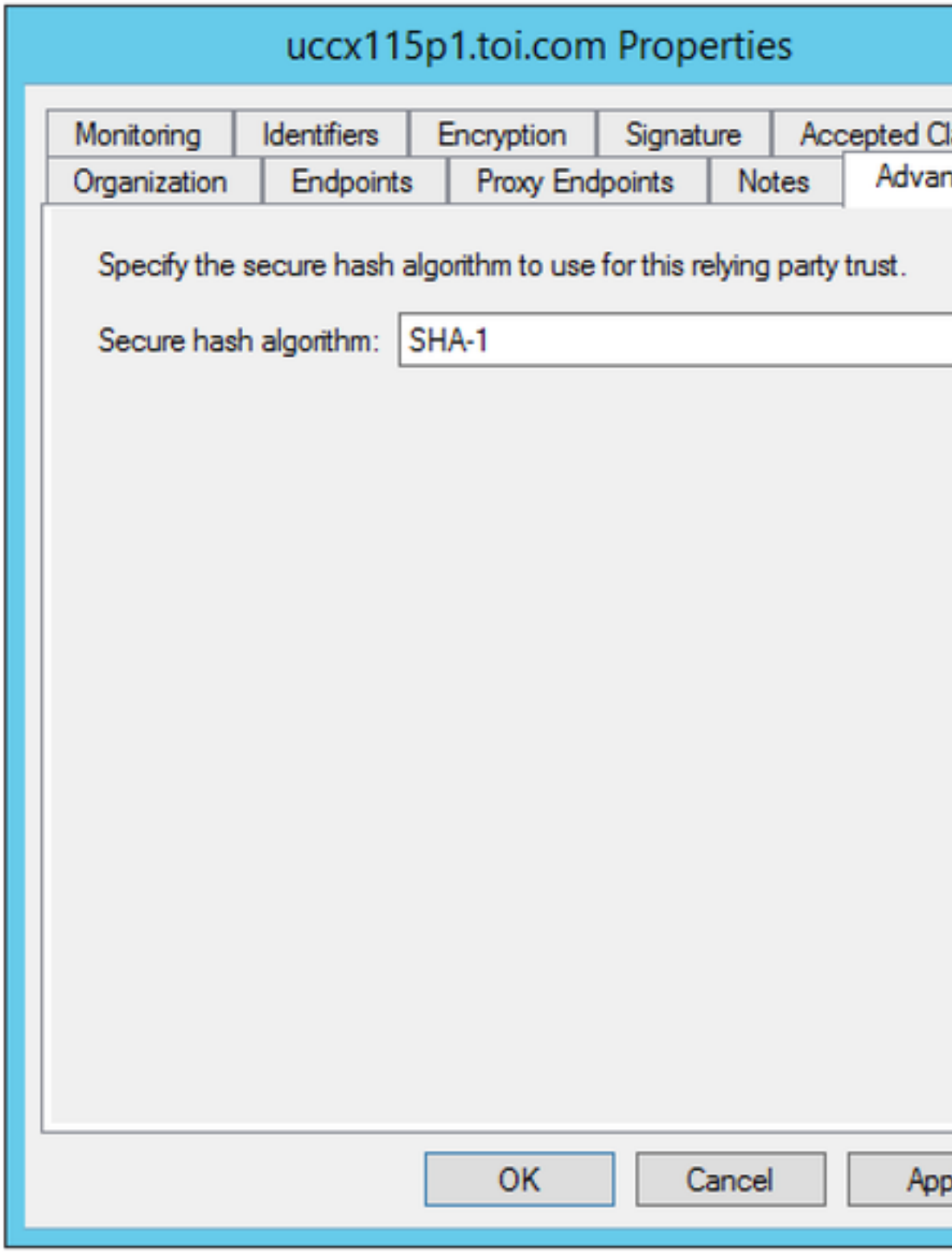
Mögliche Ursache	Die Uhrzeit im Cisco IDS- und IdP-System ist nicht synchronisiert.
Empfohlene Aktion	Synchronisieren Sie die Zeit im Cisco IDS- und AD FS-System. Es wird empfohlen, das und die Cisco IDs mithilfe des NTP-Servers zu synchronisieren.

3. Falscher Signature-Algorithmus (SHA256 im Vergleich zu SHA1) in AD FS

Problemübersicht	Die Anmeldeanforderung schlägt im Browser mit dem Statuscode 500 fehl:urn:oasis:names:tc:SAML:2.0:status:Responder Fehlermeldung im AD FS Event View Log - Wrong Signature Algorithm (SHA256 vs SH
Fehlerschritt	SAML-Antwortverarbeitung

Fehlermeldung	**Browser**
	500 Fehler mit dieser Meldung:
	IDP-Konfigurationsfehler: SAML-Verarbeitung fehlgeschlagen
	SAML Assertion fehlgeschlagen von IdP mit Statuscode: urn:oasis:names:tc:SAML:2.0
	Überprüfen Sie die IDP-Konfiguration, und versuchen Sie es erneut.
	AD FS Event Viewer:
	Die SAML-Anforderung wird nicht mit dem erwarteten Signaturalgorithmus signiert. Die
	wird mit dem Signaturalgorithmus http://www.w3.org/2001/04/xmldsig-more#rsa-sha256
	Der erwartete Signaturalgorithmus lautet http://www.w3.org/2000/09/xmldsig#rsa-sha1.
	Cisco IDs-Protokoll:
	`ERROR com.cisco.ccbu.ids IdSSAMLAsyncServlet.java:298 - Die SAML-Antwortverarbeitung`
	`com.sun.identity.saml2.common.SAML2Exception fehlgeschlagen: Ungültiger Statuscode als`
	`com.sun.identity.saml2.common.SAML2Utils.verifyResponse(SAML2Utils.java:425) unter`
	`com.sun.identity.saml2.profile.SPACSUtils.processResponse(SPACSUtils.java:1050) unter`
	`com.sun.identity.saml2.profile.SPACSZ Utils.processResponseForFedlet(SPACSUtils.java:`
	`com.cisco.ccbu.ids.auth.api.IdSSAMLAsyncServlet.getAttributesMapFromSAMLResponse(IdSSA`
	`72)`

Mögliche Ursache	AD FS ist für die Verwendung von SHA-256 konfiguriert.
Empfohlene Aktion	Aktualisieren Sie AD FS, um SHA-1 für Signierung und Verschlüsselung zu verwenden 1. RDP zum AD FS-System. 2. Öffnen Sie die AD FS-Konsole. 3. Wählen Sie die **Vertrauenswürdigkeit der vertraulichen Partei aus**, und klicken Sie 4. Wählen Sie die Registerkarte **Erweitert** aus. 5. Wählen Sie in der Dropdown-Liste SHA-1 aus.



4. Ausgehende Anspruchsregel nicht korrekt konfiguriert

Problemübersicht	Die Anmeldeanforderung schlägt im Browser mit dem Fehler 500 fehl, und es wird die M Benutzerkennung konnte nicht aus der SAML-Antwort abgerufen werden./Der Benutzer aus der SAML-Antwort abgerufen werden."
Fehlerschritt	uid und/oder user_capital nicht in den ausgehenden Ansprüchen festgelegt. SAML-Antwortverarbeitung
Fehlermeldung	**Browser:** 500 Fehler mit dieser Meldung: IDP-Konfigurationsfehler: SAML-Verarbeitung fehlgeschlagen. Die Benutzer-ID konnte nicht aus der SAML-Antwort abgerufen werden./Der Benutzer-I

der SAML-Antwort abgerufen werden.

AD FS Event Viewer:

Kein Fehler

Cisco IDs-Protokoll:

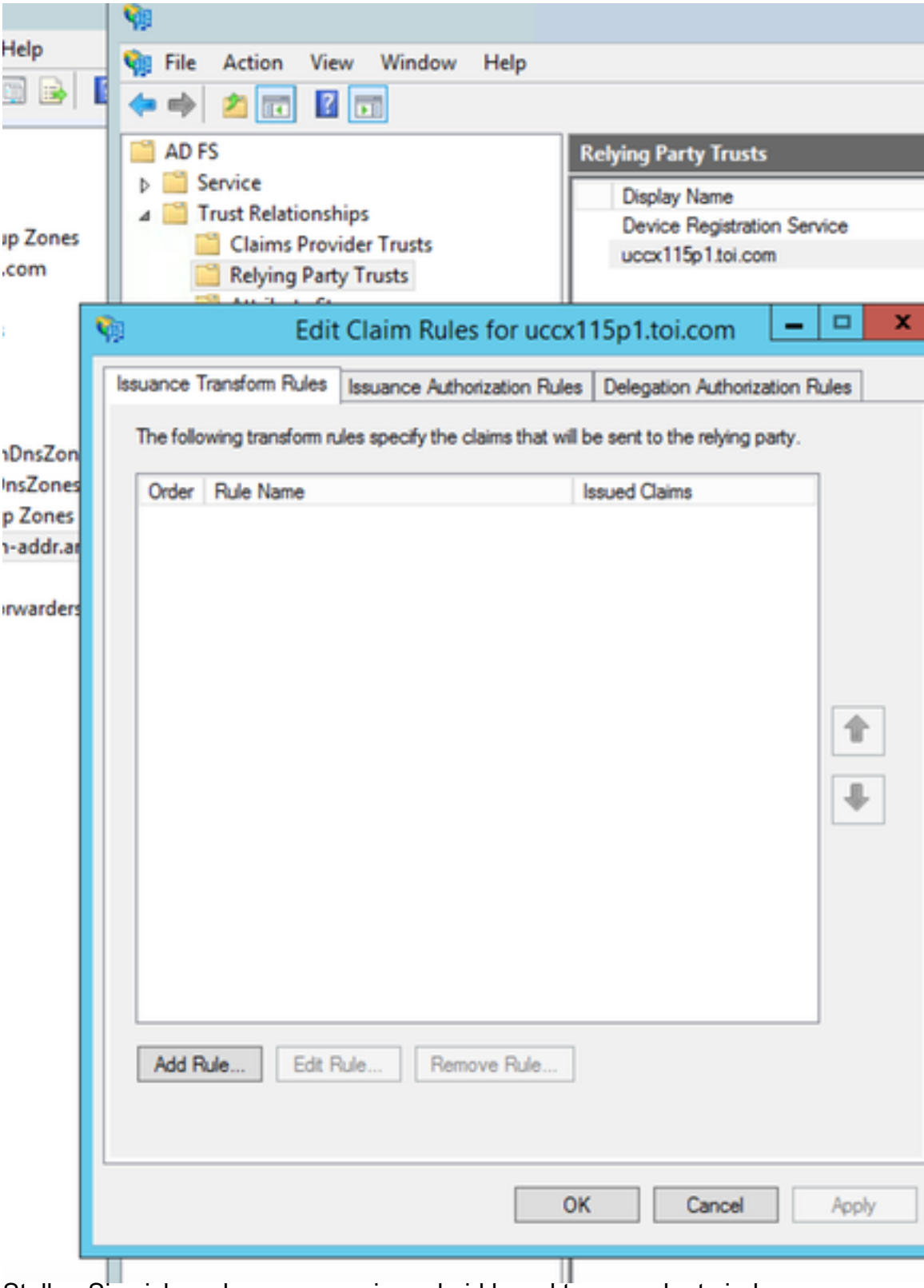
```
ERROR com.cisco.ccbu.ids IdSSAMLAsyncServlet.java:294 - Die SAML-Antwortverarbeitung
com.sun.identity.saml.common.SAMLException fehlgeschlagen: Die Benutzer-ID konnte aus
abgerufen werden. unter
com.cisco.ccbu.ids.auth.api.IdSSAMLAsyncServlet.validateSAMLAttributes(IdSSAMLAsyncSe
com.cisco.ccbu.ids.auth.api.IdSSAMLAsyncServlet.processSaml PostResponse(IdSSAMLAsync
com.cisco.ccbu.ids.auth.api.IdSSAMLAsyncServlet.processIdSEndPointRequest(IdSSAMLAsyn
```

Mögliche Ursache

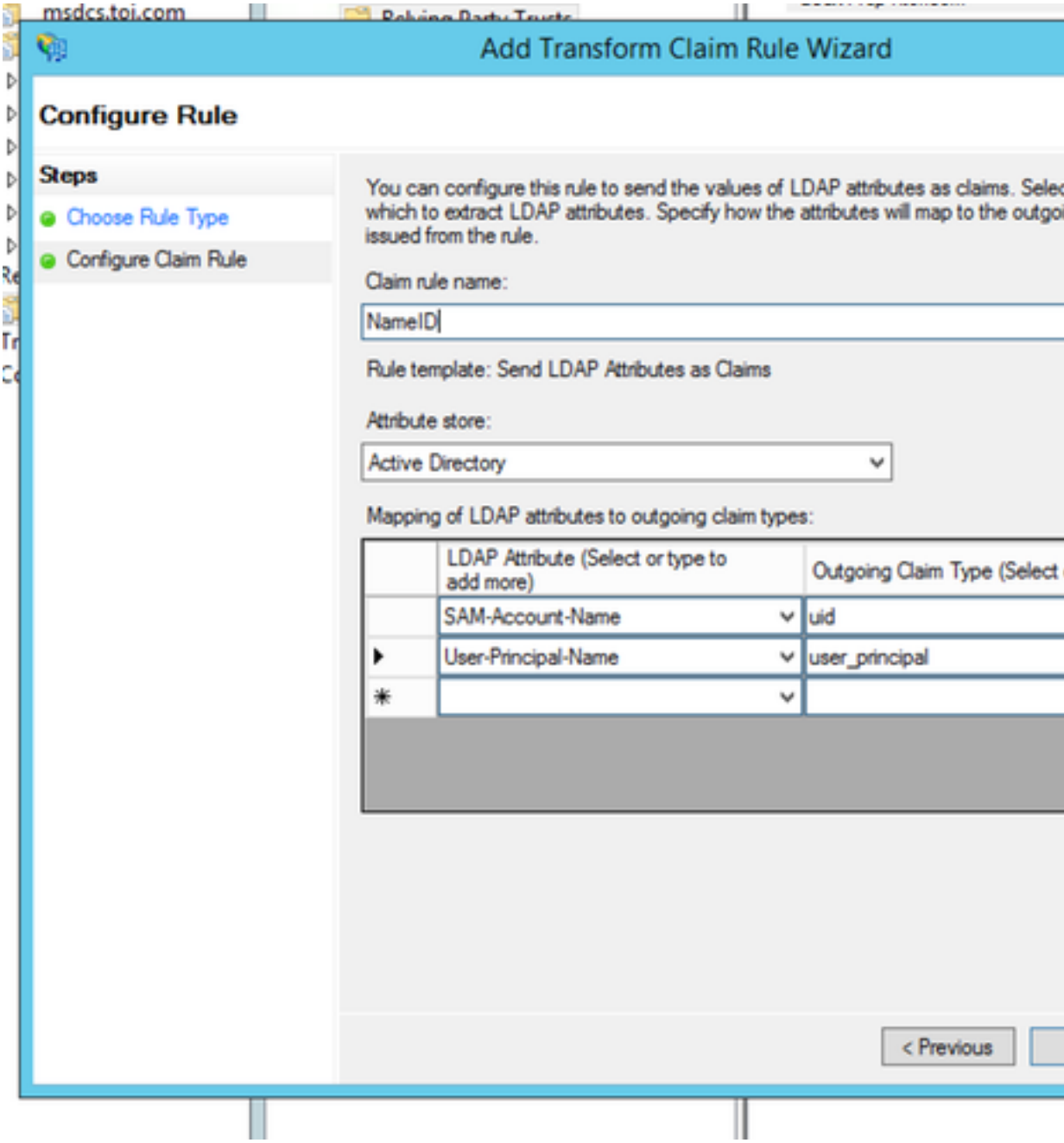
Obligatorische ausgehende Ansprüche (uid und user_main) sind in den Anspruchsrege
konfiguriert.
Wenn Sie die NamensID-Anspruchsregel nicht konfiguriert haben oder uid oder user_m
konfiguriert sind.
Wenn die NameID-Regel nicht konfiguriert ist oder user_main nicht korrekt zugeordnet
dass user_main nicht abgerufen wird, da dies die Eigenschaft ist, nach der Cisco IdS su
Wenn uid nicht korrekt zugeordnet ist, gibt Cisco IdS an, dass uid nicht abgerufen wird.
Stellen Sie unter AD FS-Anspruchsregeln sicher, dass die Attributzuordnung für "user_
IDP-Konfigurationsleitfaden (welcher Leitfaden?) definiert ist.

1. RDP an AD FS-System.
2. Bearbeiten Sie die Anspruchsregeln für die Vertrauenswürdigkeit der vertrauende

Empfohlene Aktion



3. Stellen Sie sicher, dass user_main und uid korrekt zugeordnet sind.



5. Ausgehende Anspruchsregel ist in einem Federated AD FS nicht korrekt konfiguriert

Problemübersicht	Die Anmeldeanforderung schlägt im Browser mit dem Fehler 500 fehl, und es wird die M konnte keine Benutzerkennung aus der SAML-Antwort abgerufen werden. oder Der Be den Principal der SAML-Antwort nicht abrufen." wenn das AD FS ein Federated AD FS
Fehlerschritt	SAML-Antwortverarbeitung

Fehlermeldung	**Browser**
	500 Fehler mit dieser Meldung:
	IDP-Konfigurationsfehler: SAML-Verarbeitung fehlgeschlagen
	Die Benutzer-ID konnte nicht aus der SAML-Antwort abgerufen werden./ Der Benutzer
	Principal aus der SAML-Antwort abrufen.
	AD FS Event Viewer:
	Kein Fehler
	Cisco IDs-Protokoll:
	`ERROR com.cisco.ccbu.ids IdSSAMLAsyncServlet.java:294 - Die SAML-Antwortverarbeitung`
	`com.sun.identity.saml.common.SAMLException fehlgeschlagen: Die Benutzer-ID konnte aus`
	`nicht abgerufen werden. unter`
	`com.cisco.ccbu.ids.auth.api.IdSSAMLAsyncServlet.validateSAMLAttributes(IdSSAMLAsyncSe`
	`unter com.cisco.ccbu.ids.auth.api.IdSSAMLAsyncServlet.processSaml`

```
PostResponse(IdSSAMLAsyncServlet.java:263) unter
com.cisco.ccbu.ids.auth.api.IdSSAMLAsyncServlet.processIdSEndPointRequest(IdSSAMLAsync
```

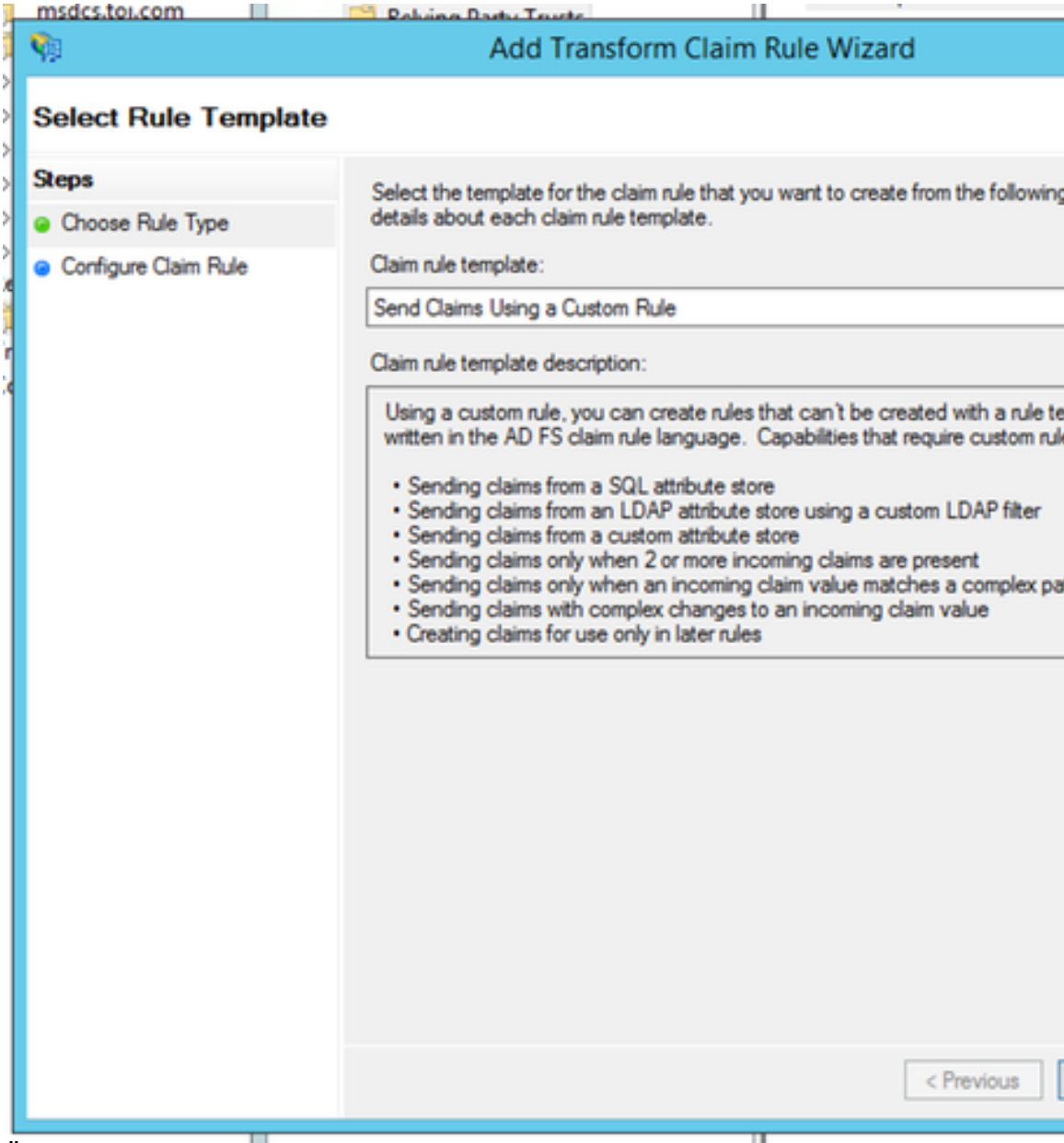
Mögliche Ursache	In einer Federated AD FS sind weitere Konfigurationen erforderlich, die möglicherweise
Empfohlene Aktion	Überprüfen Sie, ob die AD FS-Konfiguration in Federated AD wie im Abschnitt **Für eine Konfiguration für Federated AD FS** in Configure Cisco IDS and AD FS erfolgt.

6. Benutzerdefinierte Anspruchsregeln nicht korrekt konfiguriert

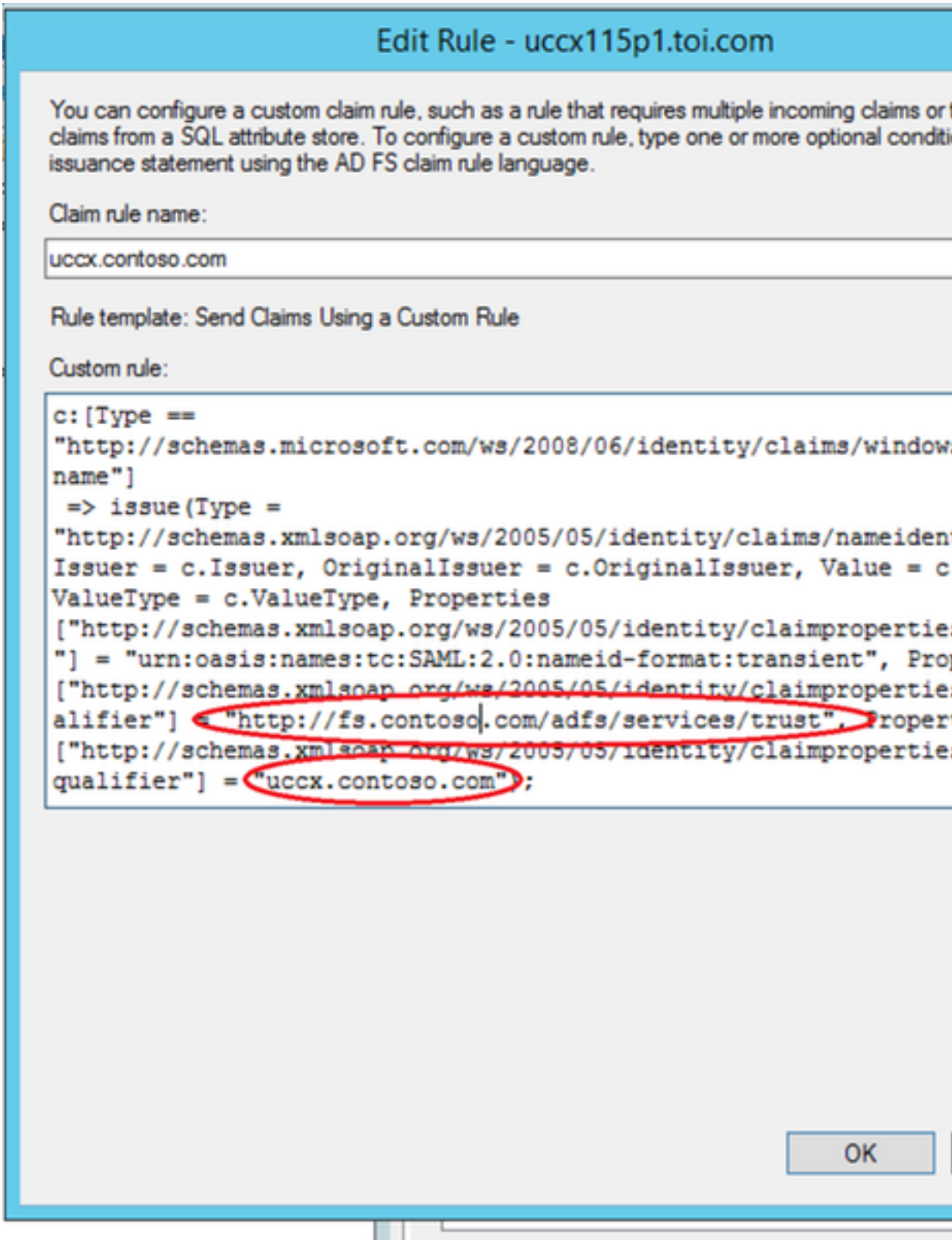
Problemübersicht	Die Anmeldeanforderung schlägt im Browser mit dem Fehler 500 fehl, und es wird die M Benutzerkennung konnte nicht aus der SAML-Antwort abgerufen werden./Der Benutzer aus der SAML-Antwort abgerufen werden." uid und/oder user_capital nicht in den ausgehenden Ansprüchen festgelegt.
Fehlerschritt	SAML-Antwortverarbeitung **Browser** 500 Fehler mit dieser Meldung: SAML Assertion fehlgeschlagen von IdP mit Statuscode: urn:oasis:names:tc:**SAML:2.0:status:Requester/urn:oasis:names:tc:SAML:2.0:status:Inv** Überprüfen Sie die IDP-Konfiguration, und versuchen Sie es erneut. **AD FS Event Viewer:** **Die SAML-Authentifizierungsanfrage verfügte über eine NameID-Richtlinie, die nicht erf** Antragsteller: myids.cisco.com Format der Namenskennung: urn:oasis:names:tc:SAML:2.0:nameid format:transient SPNameQualifier: myids.cisco.com Ausnahmedetails: MSIS1000: Die SAML-Anforderung enthielt eine NameIDP-Richtlinie, die vom ausgege wurde. Angeforderter NameIDP-Richtlinie: AllowCreate: Echtformat: urn:oasis:names:tc format:transient SPNameQualifier: myids.cisco.com. Tatsächliche NameID-Eigenschaft Diese Anfrage ist fehlgeschlagen. Benutzeraktion Konfigurieren Sie mithilfe des AD FS 2.0 Management-Snap-Ins die Konfiguration, die Namenskennung ausgibt.

Fehlermeldung	**Cisco IDs-Protokoll**:
	`2016-08-30 09:45:30.471 IST(+0530) [IdSEndPoints-SAML-82] INFO com.cisco.ccbu.ids SAM`
	`SSO ist mit folgendem Code fehlgeschlagen: 1. Antwortstatus: <samlp:Status> <samlp:Sta`
	`Value="urn:oasis:names:tc:SAML:2.0:status:Requester"> <samlp:StatusCode`
	`Value="urn:oasis:names:tc:SAML:2.0:status:InvalidNameIDPopolicy"> </samlp:StatusCode>`
	`</samlp:Status> für AuthnRequest: n/a 2016-08-30 09:45:30.471 IST(+0530) [IdSEndPoints`
	`com.cisco.ccbu.ids IdSSAMLAsyncServlet.java:299 - SAML-Antwort Verarbeitung fehlgesch`
	`com.sun.identity.saml2.common.SAML2Ausnahme: Ungültiger Statuscode als Antwort. unter`
	`com.sun.identity.saml2.common.SAML2Utils.verifyResponse(SAML2Utils.java:425) unter`
	`com.sun.identity.saml2.profile.SPACSUtils.processResponse(SPACSUtils.java:1050) unter`
	`com.sun.identity.saml2.profile.SPACSZ Utils.processResponseForFedlet(SPACSUtils.java:`

Mögliche Ursache	Benutzerdefinierte Anspruchsregel ist nicht richtig konfiguriert.
Empfohlene Aktion	Stellen Sie unter AD FS-Anspruchsregeln sicher, dass die Attributzuordnung für "user_ Konfigurationsleitfaden (welcher Leitfaden?) definiert ist. 1. RDP an AD FS-System. 2. Bearbeiten Sie die Anspruchsregeln für benutzerdefinierte Anspruchsregeln.



3. Überprüfen Sie, ob die vollständig qualifizierten AD FS- und Cisco IDS-Domänenn
werden.



7. Zu viele Anfragen an AD FS.

Problemübersicht	Die Anmeldeanforderung schlägt im Browser mit dem Statuscode 500 fehl:urn:oasis:names:tc:SAML:2.0:status:Responder Fehlermeldung im AD FS Event View Log (Ereignisanzeigeprotokoll) weist darauf hin, FS vorliegen.
Fehlerschritt	SAML-Antwortverarbeitung
Fehlermeldung	**Browser** 500 Fehler mit dieser Meldung: IDP-Konfigurationsfehler: SAML-Verarbeitung fehlgeschlagen SAML Assertion fehlgeschlagen von IdP mit Statuscode: urn:oasis:names:tc:SAML:2.0

Überprüfen Sie die IDP-Konfiguration, und versuchen Sie es erneut.
AD FS Event Viewer:
Microsoft.IdentityServer.Web.InvalidRequestException:
MSIS7042: **In derselben Client-Browser-Sitzung wurden in der letzten '16' Sekunden. Weitere Informationen erhalten Sie von Ihrem Administrator.**
unter Microsoft.IdentityServer.Web.FederationPassiveAuthentication.UpdateLoopDet
at Microsoft.IdentityServer.Web.FederationPassiveAuthentication.SendSignInRespon
Antwort)

```
Ereignis XML: <Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event"> <
2.0" Guid="{20E25DDB-09E5-404B-8A56-EDAE2F12EE81}" /> <EventID>364</EventID> Version>
<Task>0</Task> <Opcode>0</Opcode> <Schlüsselwörter>0x80000000000001</Schlüsselwörter>
SystemTime="2016-04-1 9T12:14:58.474662600Z" /> <EventRecordID>29385</EventRecordID>
ActivityID="{9878DB0-869A-4DD5-B3B6-05 <AusführungsprozessID="2264" ThreadID="392" />
2.0/Admin</Channel> <Computer>myadfs.cisco.com</Computer> <Security UserID="S-1-5-21-
1502263146-1105"/> </System> <UserData> <Event xmlns:auto-ns2="http://schemas.microso
xmlns="http://schemas.microsoft.com/ActiveDirectoryFederationServices/2.0/Events "> <
<Data>Microsoft.IdentityServer.Web.InvalidRequestException: MSIS7042: Dieselbe Client
Anfragen in den letzten '16' Sekunden gestellt. Weitere Informationen erhalten Sie vo
Microsoft.IdentityServer.Web.FederationPassiveAuthentication.UpdateLoopDetectionCooki
Microsoft.IdentityServer.Web.FederationPassiveAuthentication.SendSignInResponse(MSISS
</EventData> </Event> </UserData> </Event> </Event>
```

Cisco IDs-Protokoll

```
2016-04-15 16:19:01.220 EDT(-0400) Standard-FEHLER [IdSEndPoints-1] com.cisco.ccbu.ids
Ausnahmeverarbeitungsanfrage com.sun.saml2.common.SAML2Ausnahme: Ungültiger Statuscode
com.sun.identity.saml2.common.SAML2Utils.verifyResponse(SAML2Utils.java:425) unter
com.sun.identity.saml2.profile.SPACSUtils.processResponse(SPACSUtils.java:1050) unter
com.sun.identity.saml2.profile.SPACSZ Utils.processResponseForFedlet(SPACSUtils.java:
com.cisco.ccbu.ids.auth.api.IdSSAMLAsyncServlet.getAttributesMapFromSAMLResponse(IdSS
```

Mögliche Ursache

Es gibt zu viele Anfragen, die von derselben Browsersitzung an AD FS gesendet werde

Empfohlene Aktion

Dies sollte in der Regel nicht in der Produktion geschehen. Aber wenn Sie auf diese Sit

1. Aktivieren Sie die Option AD FS Windows Event Viewer.
2. Überprüfen Sie erneut die Einstellungen für die Vertrauenswürdigkeit der zugrund Informationen *finden Sie unter* Konfigurieren von Cisco IDs und AD FS.
3. Melden Sie sich erneut an.

8. AD FS ist nicht konfiguriert, um Assertion und Nachricht zu signieren.

Problemübersicht

Die Anmeldeanforderung schlägt im Browser mit dem Fehlercode:invalidSignature fehl, angezeigt.

Fehlerschritt

SAML-Antwortverarbeitung

Fehlermeldung

Browser
500 Fehler mit dieser Meldung:
Fehlercode:invalidSignature
Nachricht: Ungültige Signatur in ArtifactResponse.
Cisco IDs-Protokoll:

```
2016-08-24 10:53:10.494 IST(+0530) [IdSEndPoints-SAML-241] INFO saml2error.jsp saml2e
Antwortverarbeitung fehlgeschlagen mit Code: invalidSignature; Nachricht: Ungültige S
2016-08-24 10:53:10.494 IST(+0530) [IdSEndPoints-SAML-241] ERROR com.cisco.ccbu.ids I
SAML-Antwort Fehler mit Ausnahme com.sun.identity.saml2.common.SAML2Ausnahme: Ungültig
com.sun.identity.saml2.profile.SPACSUtils.getResponseFromPost(SPACSUtils.java:994) un
com.sun.identity.saml2.profile.SPACSUtils.getResponse(SPACSUtils.java:196) unter
com.sun.identity.saml2.profile.SPACSUtils.processResponseForFedlet(SPACSUtils.java:20
com.cisco.ccbu.ids.auth.api.IdSSAMLAsyncServlet.getAttributesMapFromSAMLResponse(IdSS
a:472)
```

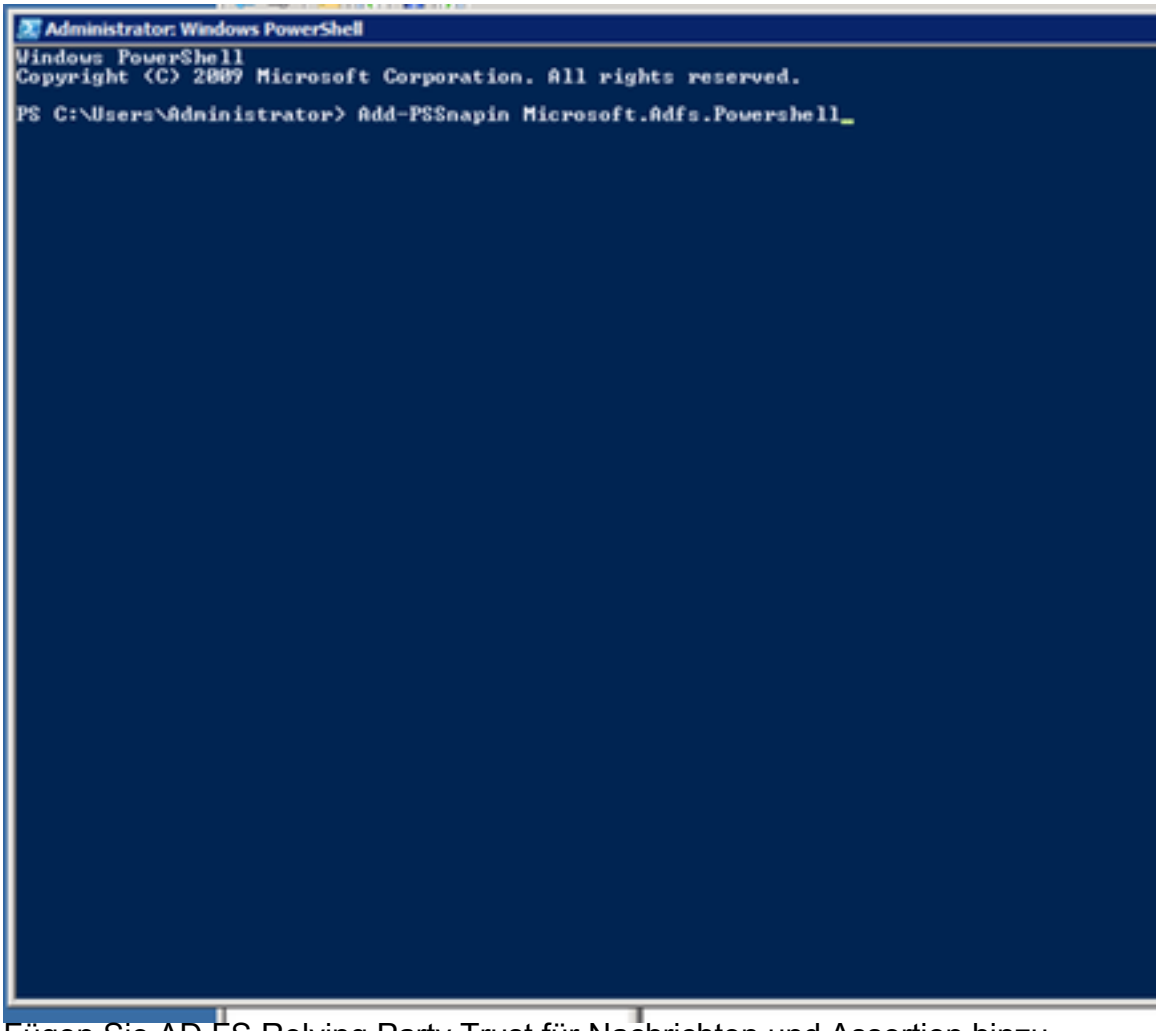
Mögliche

AD FS ist nicht für die Signierung von Assertion und Message konfiguriert.

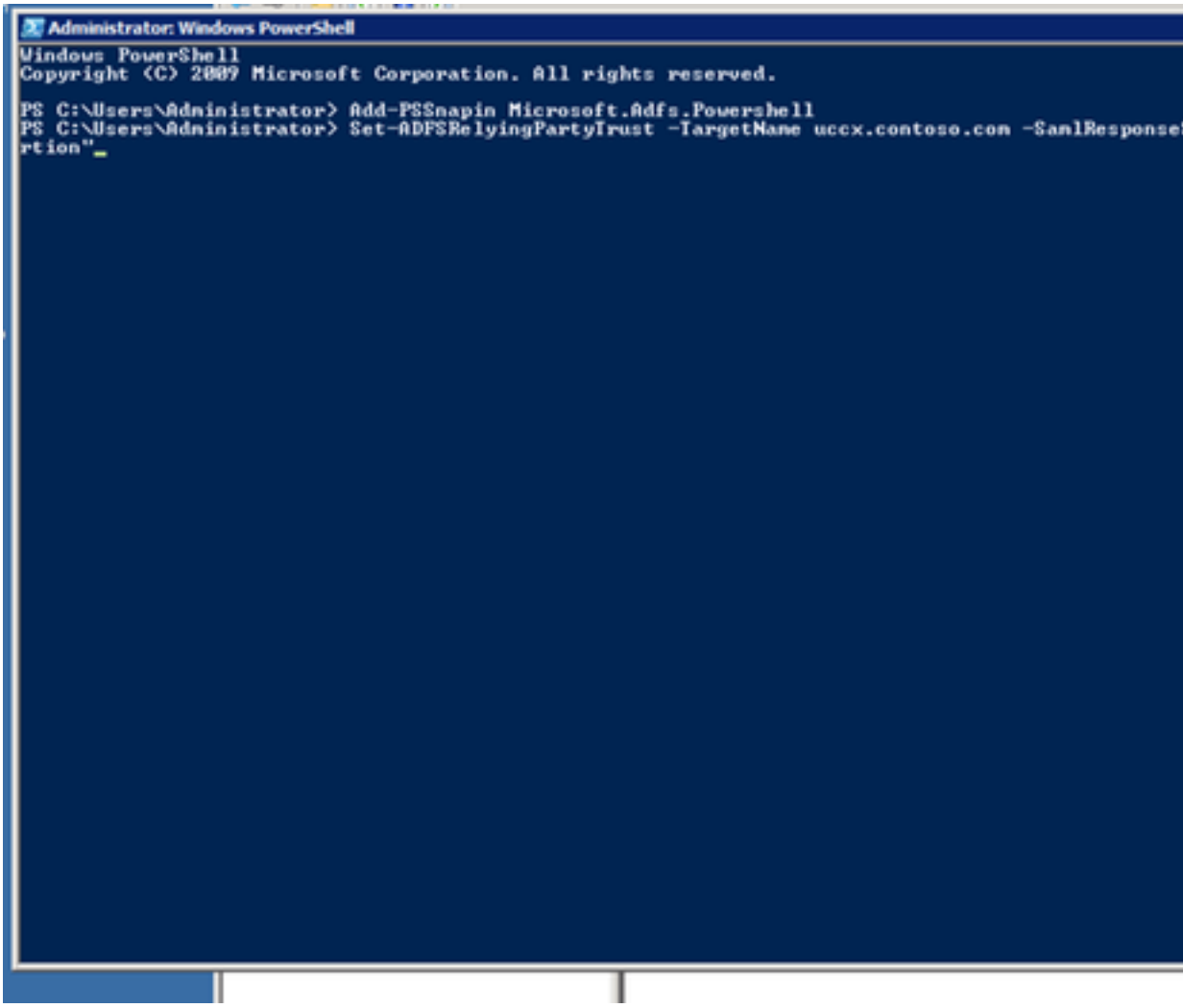
Ursache

Empfohlene Aktion

1. Führen Sie den Befehl AD FS powershell aus: **Set-ADFSRelyingPartyTrust -Targe Identifier> -SamlResponseSignature "MessageAndAssertion"**
2. RDP an AD-System.
3. Öffnen Sie **Powershell**.
4. Fügen Sie der aktuellen Sitzung Windows PowerShell-Snap-Ins hinzu. Dieser Sch erforderlich, wenn Sie ADFS 3.0 verwenden, da der CmdLet bereits installiert ist, hinzuzufügen.



5. Fügen Sie AD FS Relying Party Trust für Nachrichten und Assertion hinzu.



Zugehörige Informationen

Dies bezieht sich auf die Konfiguration des Identitätsanbieters, die im folgenden Artikel beschrieben wird:

- https://www.cisco.com/c/en/us/support/docs/customer-collaboration/unified-contact-center-express/200612-Configure-the-Identity-Provider-for-UCCX.html
- Technischer Support und Dokumentation - Cisco Systems