Risoluzione dei problemi comuni e ADFS/IdS

Sommario

Introduzione

L'interazione SAML (Security Assertion Markup Language) tra Cisco Identity Service (IdS) e Active Directory Federation Services (ADFS) tramite un browser è la base del flusso di accesso Single Sign-On (SSO). Questo documento consente di eseguire il debug dei problemi relativi alle configurazioni in Cisco IdS e ADFS, insieme all'azione consigliata per risolverli.

Modelli di distribuzione Cisco IdS

Prodotto	Implementazione
UCCX	Coresidente
PCCE	Coresidente con CUIC (Cisco Unified Intelligence Center) e LD (Live Data)
UCCE	Coresidenti con CUIC e LD per installazioni 2k. Standalone per installazioni a 4k e 12k.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Cisco Unified Contact Center Express (UCCX) versione 11.5 o Cisco Unified Contact Center Enterprise versione 11.5 o Packaged Contact Center Enterprise (PCCE) versione 11.5, a seconda dei casi.
- Microsoft Active Directory - AD installato in Windows Server
- IdP (provider di identità) - Active Directory Federation Service (ADFS) versione 2.0/3.0

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Dopo aver stabilito la relazione di trust tra Cisco IdS e AD FS (vedere qui per i dettagli, comuni per UCCX e UCCE), l'amministratore deve eseguire il test SSO impostato nella pagina Impostazioni di Identity Service Management per verificare che la configurazione tra Cisco IdS e AD FS funzioni correttamente. Se il test non riesce, utilizzare le applicazioni e i suggerimenti appropriati forniti in questa guida per risolvere il problema.

Applicazioni e log utili per il debug

Applicazione/Registro	Dettagli	Dove trovare lo strumento
Registro Cisco IdS	Il logger di Cisco IdS registrerà tutti gli errori che si sono verificati in Cisco IdS.	Utilizzare RTMT per ottenere i registri IdS Cis Per informazioni sull'utilizzo di RTMT, vedere Guida all'utilizzo di RTMT Il nome RTMT è **Cisco Identity Service**. Per trovare i log, selezionare **Cisco Identity Servi > log**
Registri dei fogli	I log dei fogli informativi forniscono ulteriori dettagli su qualsiasi errore SAML che si verifica in Cisco IdS	Utilizzare RTMT per ottenere i registri dei foglietti. Il percorso del registro Fedlet è uguale a que dei registri IdS Cisco. I registri dei volantini iniziano con il prefisso

Metriche API Cisco IdS	Le metriche API possono essere utilizzate per analizzare e convalidare eventuali errori restituiti dalle API Cisco IdS e il numero di richieste elaborate da tali API	**fedlet-** Utilizzare RTMT per ottenere le metriche API Il nome RTMT è **Cisco Identity Service** Questo verrà visualizzato in una **metrica di** cartella separata. Notare che **saml_metrics.cs** e **authorization_metrics.csv** sono le metriche rilevanti per questo documento.
Visualizzatore eventi in ADFS	Consente agli utenti di visualizzare i registri eventi nel sistema. Qualsiasi errore in ADFS durante l'elaborazione della richiesta SAML o l'invio della risposta SAML verrà registrato qui.	Nel computer ADFS passare a **Visualizzatore eventi > Registri applicazioni** e **servizi >AdDF 2.0 > Amministrazione** In Windows 2008, avviare il Visualizzatore eventi dal **Pannello di controllo > Prestazioni manutenzione > Strumenti di amministrazion** In Windows 2012, avviarlo da Pannello di controllo\Sistema e protezione\Strumenti di amministrazione. Consultare la documentazione di Windows p sapere dove trovare il Visualizzatore eventi.
Visualizzatore SAML	Un visualizzatore SAML consente di esaminare la richiesta e la risposta SAML inviate da/a Cisco IdS. Questa applicazione browser è molto utile per l'analisi di SAML Request/Response.	Questi sono alcuni visualizzatori SAML consigliati che è possibile utilizzare per esaminare la richiesta e la risposta SAML 1. Fiddler Come utilizzare il violino con ADFSPlugin Fiddler Chrome 2. SAML Tracer - Firefox 3. Pannello SAML Chrome

Diagramma di flusso con opzioni di debug

I vari passaggi per l'autenticazione SSO sono mostrati nell'immagine insieme agli elementi e al debug in ogni passaggio in caso di errore in quel passaggio.

Questa tabella fornisce i dettagli su come identificare gli errori in ogni passaggio di SSO nel browser. Vengono inoltre specificati i diversi strumenti e il relativo supporto per il debug.

Passaggio	Come identificare il guasto nel browser	Strumenti/Registro	Configurazioni da esaminare
Elaborazione richiesta AuthCode da parte di Cisco IdS	In caso di errore, il browser non viene reindirizzato all'endpoint SAML o ad AD FS e viene visualizzato un errore JSON da Cisco IdS, che indica che l'ID client o l'URL di reindirizzamento non è valido.	Log IdS Cisco: indica gli errori che si verificano durante la convalida ed elaborazione della richiesta authcode. Metriche API Cisco IdS: indica il numero di richieste elaborate e non riuscite.	Registrazione client
Richiesta SAML avviata da Cisco IdS	In caso di errore, il browser non viene reindirizzato ad AD FS e gli ID Cisco visualizzeranno una pagina o un messaggio di errore.	Log IdS Cisco: indica se esiste un'eccezione durante l'avvio della richiesta. Metriche API Cisco IdS: indica il numero di richieste elaborate e non riuscite.	ID Cisco in stato NOT_CONFIGURED.
Elaborazione richiesta SAML da AD	In caso di errore durante l'elaborazione della richiesta, il server AD FS visualizzerà una	Visualizzatore eventi in ADFS: indica gli errori che si verificano durante	Configurazione attendibilità componente in IdP

FS	pagina di errore anziché la pagina di accesso.	l'elaborazione della richiesta. Plugin browser SAML: consente di visualizzare la richiesta SAML inviata ad ADFS.	
Invio risposta SAML da AD FS	Se l'invio della risposta non riesce, dopo l'invio delle credenziali valide verrà visualizzata una pagina di errore nel server AD FS.	Visualizzatore eventi in ADFS: indica gli errori che si verificano durante l'elaborazione della richiesta.	• Configurazione attendibilità componente in IdP • Impostazione Autenticazione modulo in AD FS.
Elaborazione risposta SAML da parte di Cisco IdS	Cisco IdS visualizzerà un errore 500 con il motivo dell'errore e una pagina di controllo rapido.	Visualizzatore eventi in AD FS: indica l'errore se AD FS invia una risposta SAML senza un codice di stato valido. Plugin browser SAML: consente di visualizzare la risposta SAML inviata da ADFS per identificare gli errori. Log IdS Cisco: indica l'errore/eccezione verificatasi durante l'elaborazione. Metriche API Cisco IdS: indica il numero di richieste elaborate e non riuscite.	• Configurazione regole attestazioni • Firma messaggio e asserzione

Elaborazione delle richieste Authcode da parte di Cisco IdS

Il punto di partenza dell'accesso SSO, per quanto riguarda gli ID Cisco, è la richiesta di un codice di autorizzazione da un'applicazione abilitata all'SSO. La convalida della richiesta API viene eseguita per verificare se si tratta di una richiesta di un client registrato. Se la convalida riesce, il browser viene reindirizzato all'endpoint SAML di Cisco IdS. In caso di errore nella convalida della richiesta, viene restituita una pagina di errore/JSON (JavaScript Object Notation) da Cisco IdS.

Errori comuni rilevati durante il processo

1. Registrazione del cliente non eseguita

Riepilogo del problema

Richiesta di accesso non riuscita con errore 401 nel browser.

Messaggio di errore

Browser:

Errore 401 con questo messaggio: {"error":"invalid_client","error_description":"ClientId non val

Registro Cisco IdS:

```
2016-09-02 00:16:58.604 IST(+0530) [IdSEndPoints-51] WARN com.cisco.ccbu.ids IdSConfigImpl.j
client: fb308a80050b2021f974f48a72ef9518a5e7ca69 inesistente 2016-09-02 00:16:58.604 IST(+05
[IdSEndPoints-51] ERROR com.cisco.ccbu.ids IdSOAuthEndPoint.java:45 - Eccezione durante l'el
richiesta di autorizzazione. org.apache.oltu.oauth2.common.exception.OAuthProblemException:
ClientId non valido. all'indirizzo
```

	`org.apache.oltu.oauth2.common.exception.OAuthProblemException.error(OAuthProblemException.ja`
	`all'indirizzo`
	`com.cisco.ccbu.ids.auth.validator.IdSAuthorizeValidator.validateRequestParams(IdSAuthorizeVa`
	`all'indirizzo`
	`com.cisco.ccbu.ids.auth.validator.IdSAuthorizeValidator.validateRequiredParameters(IdSAuthor`
	`ava:70) all'indirizzo org.apache.oltu.oauth2.as.request.OAuthRequest.validate(OAuthRequest.j`

Possibile causa	La registrazione del client con Cisco IdS non è stata completata.
Azione consigliata	Accedere alla console di gestione Cisco IdS e verificare che la registrazione del client sia stat correttamente. In caso contrario, registrare i client prima di procedere con SSO.

2. L'utente accede all'applicazione utilizzando l'indirizzo IP o il nome host alternativo

Riepilogo del problema	Richiesta di accesso non riuscita con errore 401 nel browser.
Messaggio di errore	**Browser:** Errore 401 con questo messaggio: {"error":"invalid_redirectUri","error_description":"Uri di reindirizzamento non valido"}
Possibile causa	L'utente accede all'applicazione utilizzando Indirizzo IP/Nome host alternativo. In modalità SSO, se si accede all'applicazione utilizzando IP, l'operazione non funziona. È necessario accedere alle applicazioni dal nome host con cui sono registrate in Cisco IdS. Questo problema può verificarsi se l'utente accede a un nome host alternativo non registrato con Cisco IdS.
Azione consigliata	Accedere alla console di gestione Cisco IdS e verificare che il client sia registrato con l'URL di reindirizzamento corretto e che venga utilizzato per accedere all'applicazione.

Richiesta SAML avviata da Cisco IdS

L'endpoint SAML di Cisco IdS è il punto di partenza del flusso SAML nell'accesso basato su SSO. In questo passaggio viene attivato l'avvio dell'interazione tra Cisco IdS e AD FS. Il prerequisito è che gli ID Cisco siano a conoscenza dell'ADFS a cui connettersi, in quanto i metadati IdP corrispondenti devono essere caricati negli ID Cisco affinché questo passaggio abbia esito positivo.

Errori comuni rilevati durante il processo

1. Metadati ADFS non aggiunti a Cisco IdS

Riepilogo del problema	Richiesta di accesso non riuscita con errore 503 nel browser.
Messaggio di errore	**Browser:** 503 errore con questo messaggio: {"error":"service_unavailable","error_description":"Metadati SAML non inizializzati"}
Possibile causa	Metadati Idp non disponibili in Cisco IdS. La definizione del trust tra Cisco IdS e AD FS è completa.
Azione consigliata	Passare alla console di gestione IdS Cisco e verificare se l'ID è in stato **Non configurat** Verificare se i metadati IdP sono stati caricati o meno. In caso contrario, caricare i metadati IdP scaricati da AD FS. Per ulteriori dettagli, vedere qui.

Elaborazione richiesta SAML da AD FS

Elaborazione richieste SAML è il primo passaggio di ADFS nel flusso SSO. La richiesta SAML

inviata dagli Id Cisco viene letta, convalidata e decifrata da ADFS in questo passaggio. L'elaborazione di questa richiesta ha come risultato due scenari:

1. Se si tratta di un nuovo accesso in un browser, ADFS visualizza il modulo di accesso.Se si tratta del reaccesso di un utente già autenticato da una sessione del browser esistente, ADFS tenta di inviare la risposta SAML direttamente.

   Nota: Il prerequisito principale per questo passaggio è la configurazione dell'attendibilità del destinatario della risposta da parte di ADFS.

Errori comuni rilevati durante il processo

1. AD FS non dispone del certificato SAML Cisco IdS più recente.

Riepilogo del problema	ADFS non visualizza la pagina di accesso, ma visualizza una pagina di errore.

Messaggio di errore	**Browser**
	In ADFS viene visualizzata una pagina di errore simile alla seguente:
	Si è verificato un problema durante l'accesso al sito. Riprovare a passare al sito.
	Se il problema persiste, contattare l'amministratore del sito e fornire il numero di riferimento pe problema.
	Numero di riferimento: 1ee602be-382c-4c49-af7a-5b70f3a7bd8e
	Visualizzatore eventi AD FS
	Errore del servizio federativo durante l'elaborazione della richiesta di autenticazione SAML.
	Dati aggiuntivi
	`Dettagli eccezione: Microsoft.IdentityModel.Protocols.XmlSignature.SignatureVerificationFail`
	`MSIS0038: Firma del messaggio SAML errata. Emittente: 'myuccx.cisco.com'. all'indirizzo`
	`Microsoft.IdentityServer.Protocols.Saml.Contract.SamlContractUtility.CreateSamlMessage(messa`
	`MSISSamlBindingMessage) all'indirizzo`
	`Microsoft.IdentityServer.Service.SamlProtocol.SamlProtocolService.CreateErrorMessage(CreateE`
	`createErrorMessageRequest) all'indirizzo`
	`Microsoft.IdentityServer.Service.SamlProtocol.SamlProtocolService.ProcessRequest(Message req`

Possibile causa	L'attendibilità del componente non è stata stabilita o il certificato Cisco IdS è stato modificato, è stato caricato in AD FS. Stabilire la relazione di trust tra ADFS e ID Cisco con il certificato ID Cisco più recente.
Azione consigliata	Verificare che il certificato Cisco IdS non sia scaduto. È possibile visualizzare il dashboard di s Identity Service Management. In tal caso, rigenerare il certificato nella pagina Impostazioni. Per ulteriori dettagli su come stabilire un trust metadati tra ADFS e Cisco IdS, vedere qui

Risposta SAML inviata da AD FS

Una volta completata l'autenticazione dell'utente, ADFS invia la risposta SAML agli ID Cisco tramite il browser. ADFS è in grado di inviare una risposta SAML con un codice di stato indicante Operazione riuscita o Operazione non riuscita. Se l'autenticazione basata su form non è abilitata in ADFS, ciò indica una risposta di errore.

Errori comuni rilevati durante il processo

1. Autenticazione modulo non abilitata in AD FS

Riepilogo del problema	Il browser mostra l'accesso NTLM e quindi non riesce senza reindirizzare correttamente Cisco IdS.
Fase di errore	Invio risposta SAML
Messaggio di errore	**Browser:** Il browser mostra l'accesso NTLM, ma dopo aver eseguito correttamente l'accesso non riesce con molti reindirizzamenti.
Possibile causa	Cisco IdS supporta solo l'autenticazione basata su modulo, l'autenticazione basata su modulo non è abilitata in ADFS.
Azione consigliata	Per ulteriori informazioni su come abilitare l'autenticazione basata su form, vedere: Impostazione autenticazione modulo ADFS 2.0 Impostazione autenticazione modulo ADFS 3.0

Elaborazione delle risposte SAML da parte di Cisco IdS

In questa fase, Cisco IdS riceve una risposta SAML da ADFS. La risposta potrebbe contenere un codice di stato che indica Operazione riuscita o Operazione non riuscita. Una risposta di errore da ADFS genera una pagina di errore che deve essere sottoposta a debug.

Durante la risposta SAML, l'elaborazione della richiesta può non riuscire per i seguenti motivi:

- Metadati IdP (AD FS) non corretti.
- Impossibile recuperare le attestazioni in uscita previste da AD FS.
- Gli orologi Cisco IdS e ADFS non sono sincronizzati.

Errori comuni rilevati durante il processo

1. Il certificato ADFS in Cisco IdS non è l'ultimo.

Riepilogo del problema	Richiesta di accesso non riuscita con errore 500 nel browser. Il codice di errore è invalidSigna
Fase di errore	Elaborazione risposta SAML
Messaggio di errore	**Browser:** Errore 500 con questo messaggio nel browser: Codice errore: firmaNonValida Messaggio: Il certificato di firma non corrisponde a quanto definito nei metadati dell'entità. **Visualizzatore eventi AD FS:** Nessun errore **Registro Cisco IdS:** `2016-04-13 12:42:15.896 IST(+0530) errore predefinito [IdSEndPoints-0] com.cisco.ccbu.ids IdSEndPoint.java:102 - Richiesta di elaborazione eccezione com.sun.identity.saml2.common.SAML2Eccezione: Il certificato di firma non corrisponde a quan definito nei metadati dell'entità. at com.sun.identity.saml2.xmlsig.FMSigProvider.verify(FMSigProvider.java:331) at com.sun.identity.saml2.protocol.impl.StatusResponseImpl.isSignatureValid(StatusResponseImpl. at com.sun.identity.saml2.profile.SPACSUtils.getResponseFromPost(SPACSUtils.java:985) at com.sun.identity.saml2.profile.SPACSUtils.sm Risposta(SPACSUtils.java:196)`
Possibile causa	Elaborazione della risposta SAML non riuscita perché il certificato IdP è diverso da quello disp in Cisco IdS.
Azione consigliata	Scaricare i metadati ADFS più recenti da: **https://<ADFServer>/federationmetadata/2007-06/federationmetadata.xml** E caricarlo su Cisco IdS tramite l'interfaccia utente di Identity Service Management.

Per informazioni dettagliate, vedere Configurare Cisco IdS e AD FS

2. Gli orologi Cisco IdS e AD FS non sono sincronizzati.

Riepilogo del problema	La richiesta di accesso non riesce con un errore 500 sul browser con il codice di stato: urn:oasis:names:tc:SAML:2.0:status:Success
Fase di errore	Elaborazione risposta SAML
Messaggio di errore	**Browser:** Errore 500 con questo messaggio: Errore di configurazione IdP: Elaborazione SAML non riuscita Asserzione SAML non riuscita da IdP con codice di stato: urn:oasis:names:tc:SAML:2.0:status Verificare la configurazione del provider di identità e riprovare. **Registro Cisco IdS** `2016-08-24 18:46:56.780 IST(+0530) [IdSEndPoints-SAML-22] ERROR com.cisco.ccbu.ids IdSSAMLAsyncServlet.java:298 - Elaborazione della risposta SAML non riuscita con eccezione com.sun.identity.saml2.common.SAML2Eccezione: Ora in SubjectConfirmationData non valida. at com.sun.identity.saml2.common.SAML2Utils.isBearerSubjectConfirmation(SAML2Utils.java:766) at 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.processResponseFor edlet(SPACSUtils.java:2038) all com.cisco.ccbu.ids.auth.api.IdSSAMLAsyncServlet.getAttributesMapFromSAMLResponse(IdSSAMLAsyn all'indirizzo com.cisco.ccbu.ids.auth.api.IdSSAMLAsyncServlet.processSamlPostResponse(IdSSAMLAsyncServlet. all'indirizzo com.cisco.cisco u.ids.auth.api.IdSSAMLAsyncServlet.processIdSEndPointRequest(IdSSAMLAsyncServlet.java:176) a com.cisco.ccbu.ids.auth.api.IdSEndPoint$1.run(IdSEndPoint.java:269) all'indirizzo java.util.concurrent.ThreadPoolExecutor.runWorker(ThreadPoolExecutor.java:1145) all'indirizz concurrent.ThreadPoolExecutor$Worker.run(ThreadPoolExecutor.java:615) in java.lang.Thread.run(Thread.java:745)2016-08-24 18:24:20.510 IST(+0530) [pool-4-thread-1]` **Visualizzatore SAML:** Cercare i campi NotBefore e NotOnOrAfter <Conditions NotBefore="2016-08-28T14:45:03.325Z" NotOnOrAfter="2016-08-28T15:45:03.3
Possibile causa	L'ora nel sistema Cisco IdS e IdP non è sincronizzata.
Azione consigliata	Sincronizzare l'ora nel sistema Cisco IdS e AD FS. È consigliabile sincronizzare l'ora del siste ID Cisco tramite il server NTP.

3. Algoritmo di firma errato (da SHA256 a SHA1) in ADFS

Riepilogo del problema	La richiesta di accesso non riesce con un errore 500 nel browser con codice di stato:urn:oasis:names:tc:SAML:2.0:status:Responder Messaggio di errore nel registro di visualizzazione eventi di AD FS - Algoritmo di firma errato (SHA256 rispetto a SHA1) in AD FS
Fase di errore	Elaborazione risposta SAML
Messaggio di errore	**Browser** Errore 500 con questo messaggio: Errore di configurazione IdP: Elaborazione SAML non riuscita Asserzione SAML non riuscita da IdP con codice di stato: urn:oasis:names:tc:SAML:2.0:status:Responder. Verificare la configurazione del provider di id riprovare. **Visualizzatore eventi AD FS:** La richiesta SAML non è firmata con l'algoritmo di firma previsto. La richiesta SAML è firmata l'algoritmo di firma http://www.w3.org/2001/04/xmldsig-more#rsa-sha256 .

L'algoritmo di firma previsto è http://www.w3.org/2000/09/xmldsig#rsa-sha1

Registro Cisco IdS:

```
ERRORE com.cisco.ccbu.ids IdSSAMLAsyncServlet.java:298 - Elaborazione della risposta SAML no
riuscita con eccezione com.sun.identity.saml2.common.SAML2Eccezione: Codice di stato non val
nella risposta. at com.sun.identity.saml2.common.SAML2Utils.verifyResponse(SAML2Utils.java:4
com.sun.identity.saml2.profile.SPACSUtils.processResponse(SPACSUtils.java:1050) at
com.sun.identity.saml2.profile.SPACSUtils.processResponseForFedlet(SPACSUtils.java:2038) at
com.cisco.ccbu.ids.auth.api.IdSSAMLAsync
Servlet.getAttributesMapFromSAMLResponse(IdSSAMLAsyncServlet.java:472)
```

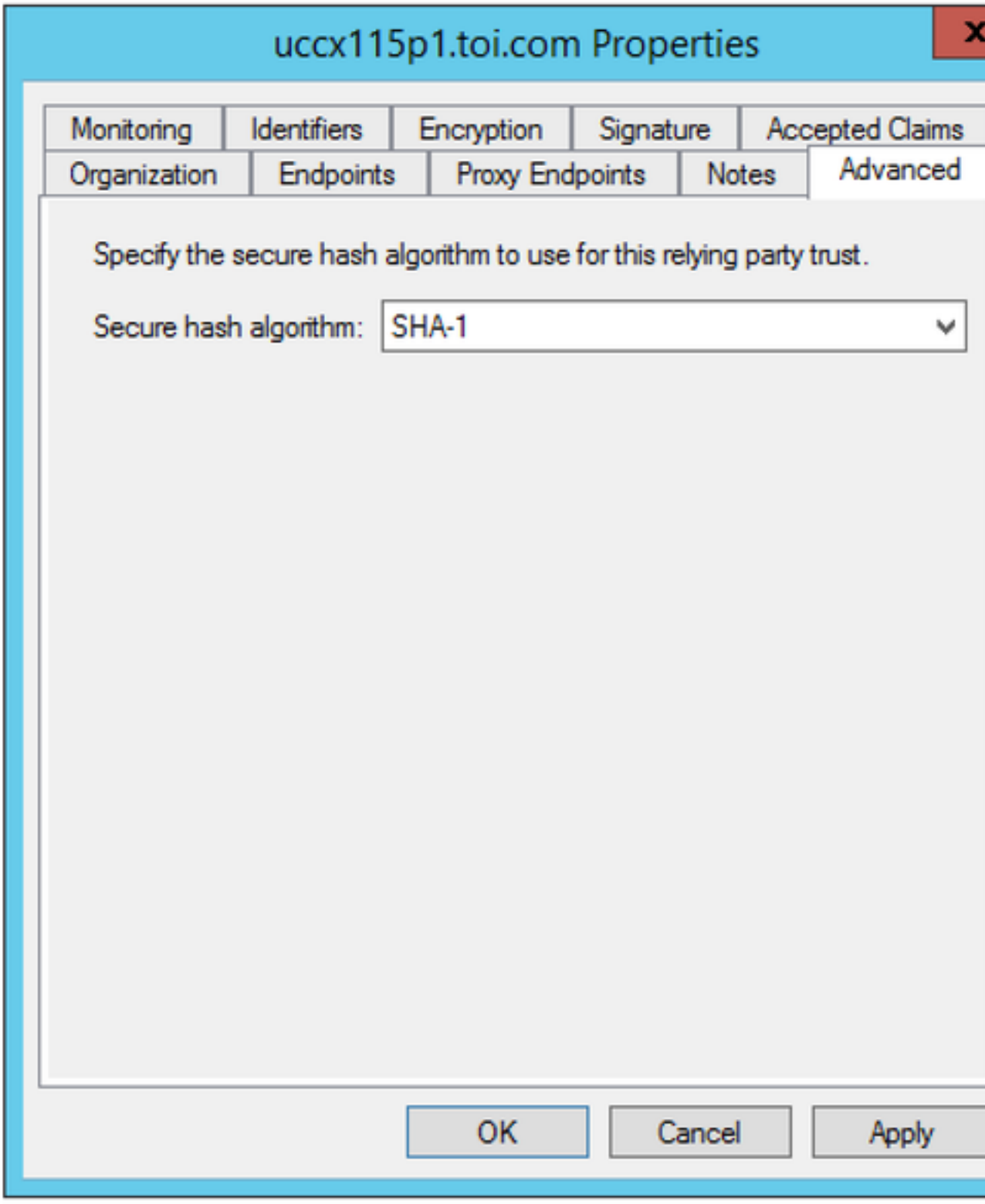
Possibile causa

ADFS è configurato per l'utilizzo di SHA-256.

Azione consigliata

Aggiornare AD FS per utilizzare SHA-1 per la firma e la crittografia.

1. RDP al sistema AD FS.
2. Aprire la console ADFS.
3. Selezionare l'**attendibilità componente** e fare clic su **Proprietà**
4. Selezionare la scheda **Avanzate**.
5. Selezionare SHA-1 dall'elenco a discesa.



4. Regola attestazione in uscita non configurata correttamente

Riepilogo del problema	La richiesta di accesso non riesce con un errore 500 nel browser con il messaggio "Impossibil l'identificatore utente dalla risposta SAML./Impossibile recuperare l'entità utente dalla risposta uid e/o user_principal non impostato nelle attestazioni in uscita.
Fase di errore	Elaborazione risposta SAML
Messaggio di errore	**Browser:** Errore 500 con questo messaggio: Errore di configurazione IdP: Elaborazione SAML non riuscita. Impossibile recuperare l'identificatore utente dalla risposta SAML./Impossibile recuperare l'ent

risposta SAML.

Visualizzatore eventi AD FS:

Nessun errore

Registro Cisco IdS:

```
ERRORE com.cisco.ccbu.ids IdSSAMLAsyncServlet.java:294 - Elaborazione della risposta SAML no
eccezione com.sun.identity.saml.common.SAMLException: Impossibile recuperare l'identificator
risposta SAML. at
com.cisco.ccbu.ids.auth.api.IdSSAMLAsyncServlet.validateSAMLAttributes(IdSSAMLAsyncServlet.j
com.cisco.ccbu.ids.auth.api.IdSSAMLAsyncServlet.processSamlPostResponse(IdSSAMLAsyncServlet.
com.cisco.ccbu.ids.auth.api.IdSSAMLAsyncServlet.processId RichiestaPuntoFine(IdSSAMLAsyncSer
```

Possibile causa

Le attestazioni in uscita obbligatorie (uid e user_principal) non sono configurate correttamente attestazione.

Se la regola di attestazione NameID non è stata configurata oppure uid o user_principal non è correttamente.

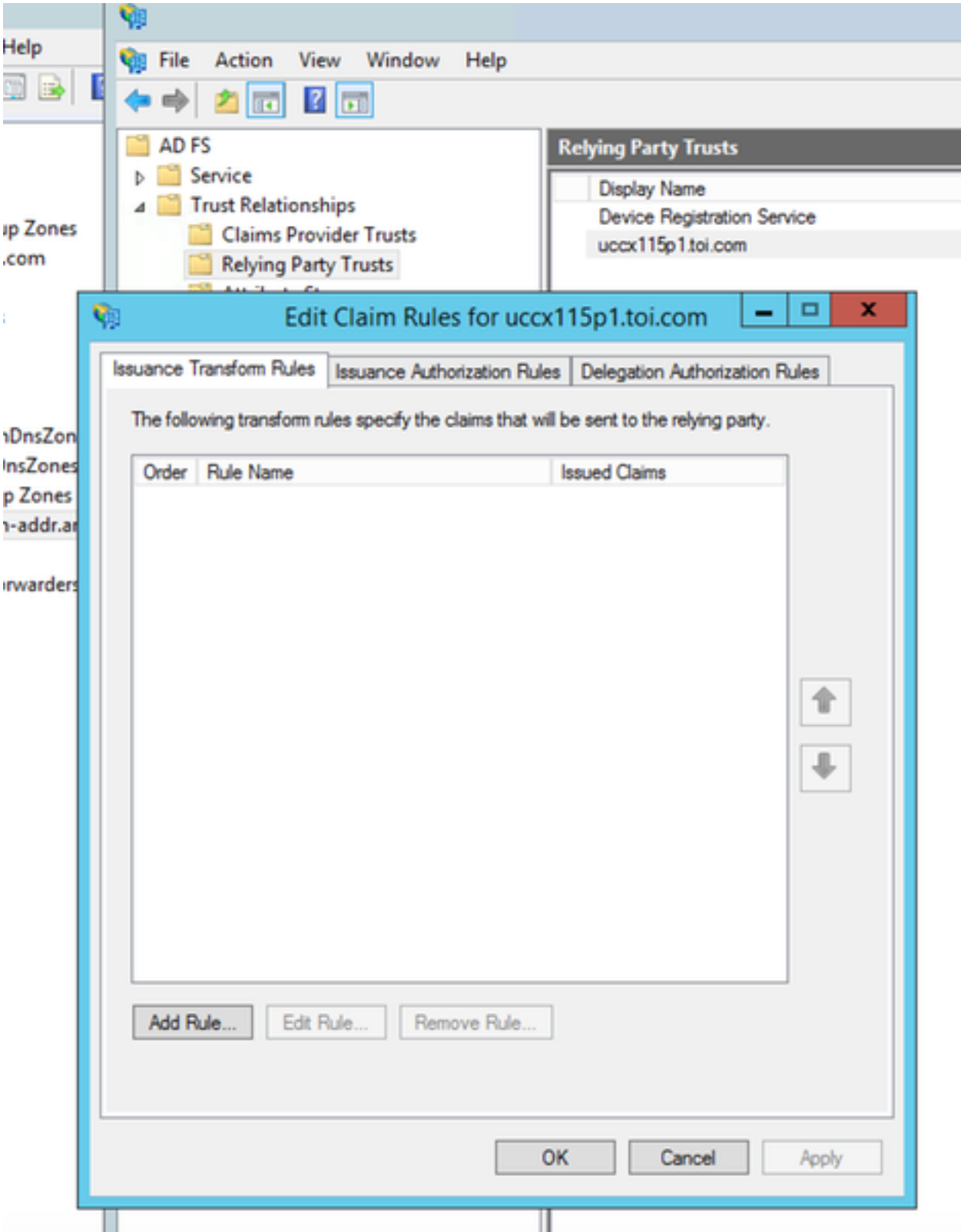
Se la regola NameID non è configurata o l'elemento user_principal non è mappato correttame indica che l'elemento user_principal non viene recuperato poiché questa è la proprietà che Cis

Se l'uid non è mappato correttamente, l'ID utente Cisco non viene recuperato.

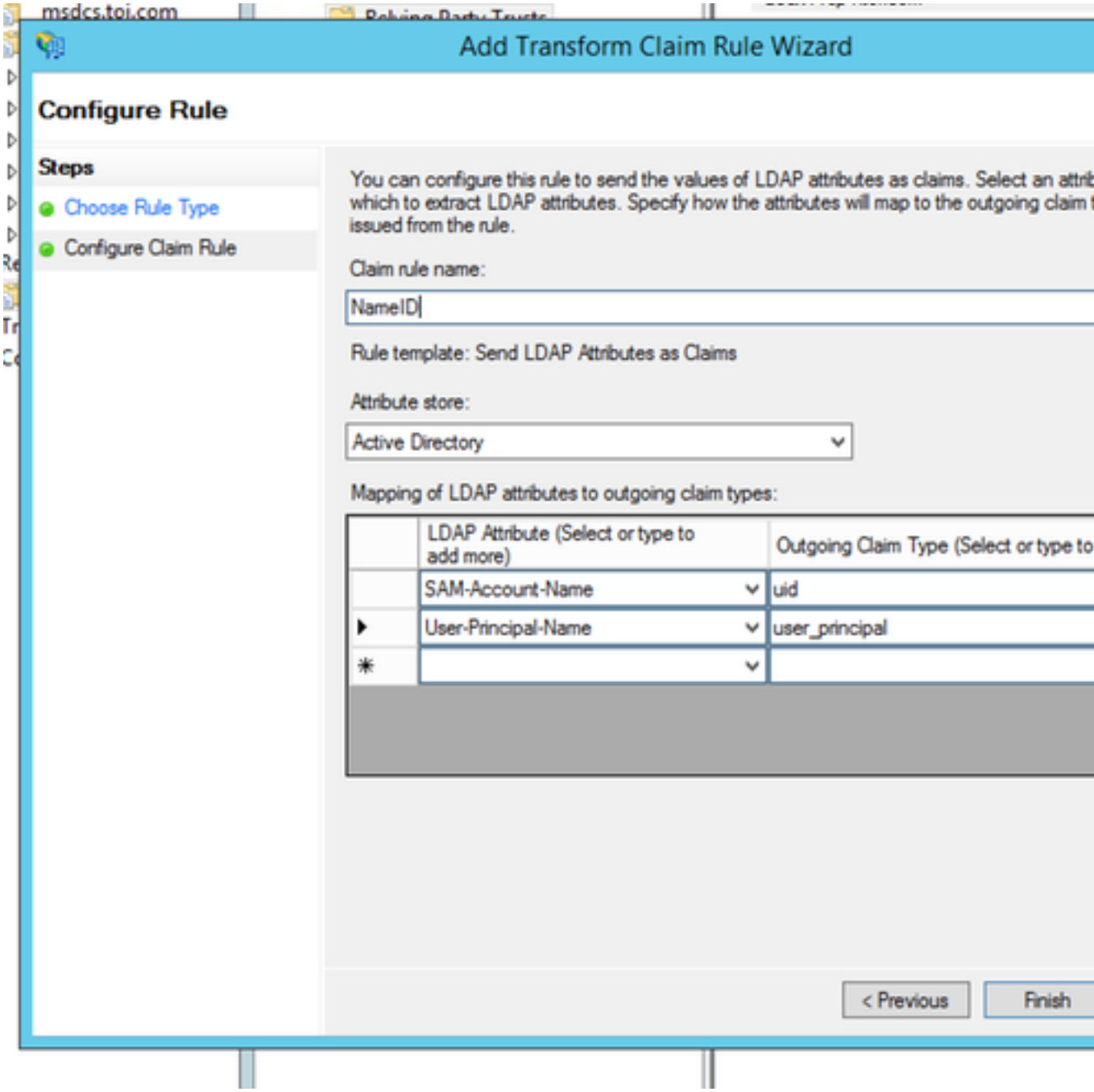
In Regole attestazioni ADFS verificare che il mapping degli attributi per "user_principal" e "uid" indicato nella guida alla configurazione del provider di identità (quale guida?).

Azione consigliata

1. RDP nel sistema AD FS.
2. Modificare le regole attestazione per l'attendibilità del componente.



3. Verificare che user_principal e uid siano mappati correttamente



5. La regola attestazione in uscita non è configurata correttamente in un ADFS federato

Riepilogo del problema	Richiesta di accesso non riuscita con errore 500 nel browser con il messaggio "Unable not ret user identifier from SAML response" (Impossibile recuperare l'identificatore utente dalla rispos SAML). o Impossibile recuperare l'entità utente dalla risposta SAML." quando ADFS è un ADF federato.
Fase di errore	Elaborazione risposta SAML
Messaggio di errore	**Browser** Errore 500 con questo messaggio: Errore di configurazione IdP: Elaborazione SAML non riuscita Impossibile recuperare l'identificatore utente dalla risposta SAML./ Impossibile recuperare l'en utente dalla risposta SAML. **Visualizzatore eventi AD FS:** Nessun errore **Registro Cisco IdS:** `ERRORE com.cisco.ccbu.ids IdSSAMLAsyncServlet.java:294 - Elaborazione della risposta SAML no riuscita con eccezione com.sun.identity.saml.common.SAMLException: Impossibile recuperare l'identificatore utente dalla risposta SAML. at`

```
com.cisco.ccbu.ids.auth.api.IdSSAMLAsyncServlet.validateSAMLAttributes(IdSSAMLAsyncServlet.j
at
com.cisco.ccbu.ids.auth.api.IdSSAMLAsyncServlet.processSamlPostResponse(IdSSAMLAsyncServlet.
at com.cisco.ccbu.ids.auth.api.IdSSAMLAsyncServlet.processId
RichiestaPuntoFine(IdSSAMLAsyncServlet.java:176)
```

Possibile causa In un ADFS federato sono necessarie più configurazioni che potrebbero mancare.

Azione consigliata Verificare se la configurazione di AD FS in AD federato viene eseguita come indicato nella se **una configurazione multidominio per AD FS federato** in Configurare ID Cisco e AD FS

6. Regole attestazione personalizzate non configurate correttamente

Riepilogo del problema La richiesta di accesso non riesce con un errore 500 nel browser con il messaggio "Impossibil l'identificatore utente dalla risposta SAML./Impossibile recuperare l'entità utente dalla risposta uid e/o user_principal non impostato nelle attestazioni in uscita.

Fase di errore Elaborazione risposta SAML

Messaggio di errore

Browser
Errore 500 con questo messaggio:
Asserzione SAML non riuscita da IdP con codice di stato:
urn:oasis:names:tc:**SAML:2.0:status:Requester/urn:oasis:names:tc:SAML:2.0:status:InvalidNa**
Verificare la configurazione del provider di identità e riprovare.

Visualizzatore eventi AD FS:
Impossibile soddisfare il criterio NameID della richiesta di autenticazione SAML.
Richiedente: myids.cisco.com
Formato identificatore nome: urn:oasis:names:tc:SAML:2.0:nameid-format:transient
Qualificatore nome SPN: myids.cisco.com
Dettagli eccezione:
MSIS1000: La richiesta SAML contiene un NameIDPolicy non soddisfatto dal token rilasciato. richiesto: ConsentiCreazione: Formato True: urn:oasis:names:tc:SAML:2.0:nameid-format:SP transitorio: su myids.cisco.com. Proprietà NameID effettive: null.
Richiesta non riuscita.
Azione utente
Utilizzare lo snap-in Gestione AD FS 2.0 per configurare la configurazione che genera l'identif richiesto.

Registro Cisco IdS:

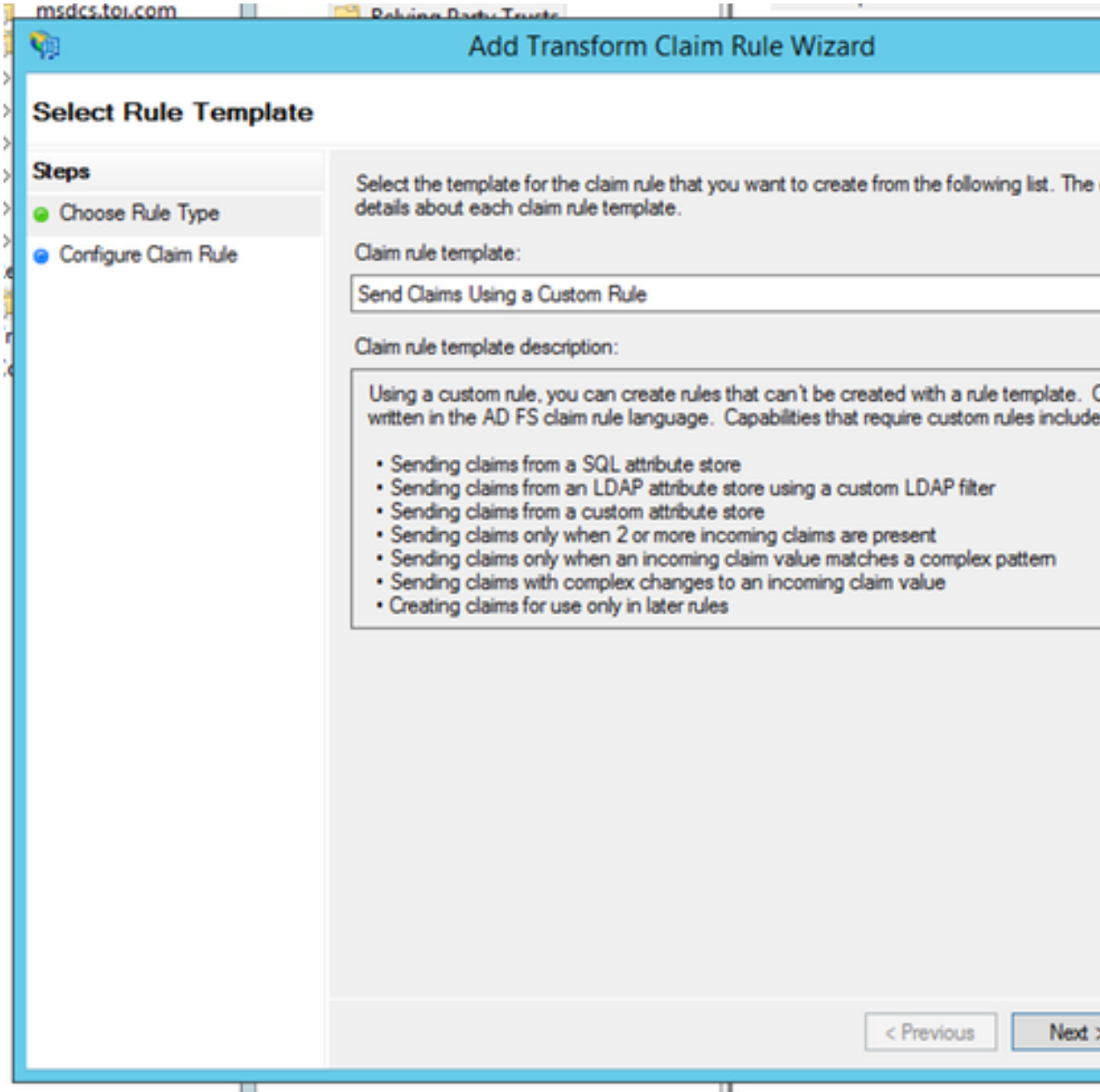
```
2016-08-30 09:45:30.471 IST(+0530) [IdSEndPoints-SAML-82] INFO com.cisco.ccbu.ids SAML2SPAda
Errore SSO con codice: 1. Stato risposta: <samlp:Status> <samlp:StatusCode
Value="urn:oasis:names:tc:SAML:2.0:status:Requester"> <samlp:StatusCode
Value="urn:oasis:names:tc:SAML:2.0:status:InvalidNameIDPolicy"> </samlp:StatusCode> </samlp:
</samlp:Status> per AuthnRequest: n/d 2016-08-30 09:45:30.471 IST(+0530) [IdSEndPoints-SAML-
com.cisco.ccbu.ids IdSSAMLAsyncServlet.java:299 - Elaborazione della risposta SAML non riusc
com.sun.identity.saml2.common.SAML2Eccezione: Codice di stato non valido nella risposta. 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:2038)
```

Possibile causa Regola attestazione personalizzata non configurata correttamente.

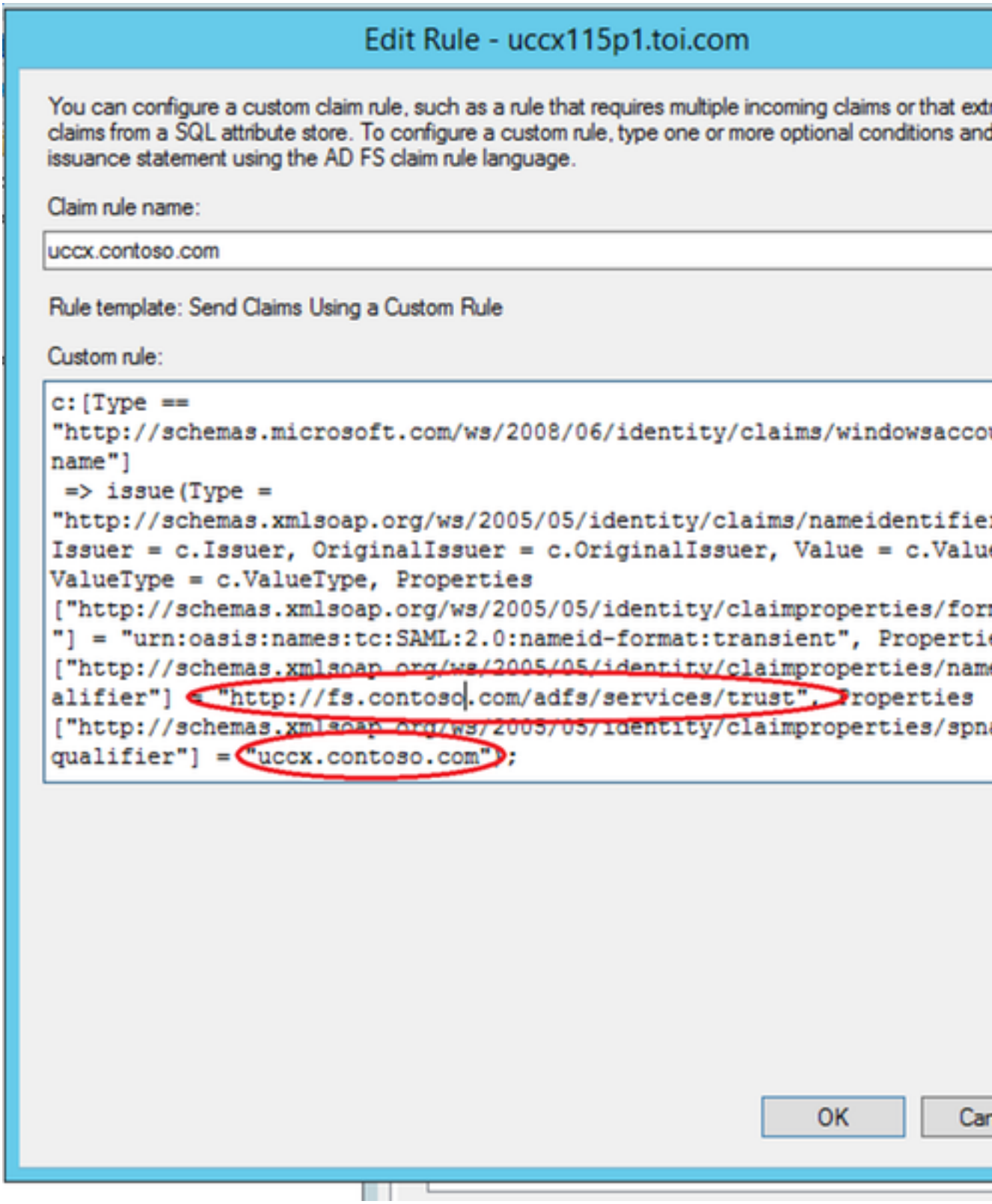
Azione consigliata

In Regole attestazioni ADFS verificare che il mapping degli attributi per "user_principal" e "uid" indicato nella guida alla configurazione (quale guida?).

1. RDP nel sistema AD FS.
2. Modificare le regole attestazione per le regole attestazione personalizzate.



3. Verificare che siano stati specificati i nomi di dominio completi di AD FS e Cisco IdS.



7. Troppe richieste ad ADFS.

Riepilogo del problema	La richiesta di accesso non riesce con un errore 500 nel browser con codice di stato:urn:oasis:names:tc:SAML:2.0:status:Responder Il messaggio di errore nel registro di visualizzazione eventi di AD FS indica che sono presenti troppe richieste ad AD FS.
Fase di errore	Elaborazione risposta SAML
Messaggio di errore	**Browser** Errore 500 con questo messaggio: Errore di configurazione IdP: Elaborazione SAML non riuscita

Asserzione SAML non riuscita da IdP con codice di stato: urn:oasis:names:tc:SAML:2.0:status:Responder. Verificare la configurazione del provider di identità e riprovare.

Visualizzatore eventi AD FS:

Eccezione Microsoft.IdentityServer.Web.InvalidRequestException: MSIS7042: **La stessa sessione del browser client ha effettuato 6 richieste nell'ultimo '16' secondi. Per ulteriori informazioni, contattare l'amministratore.** all'indirizzo Microsoft.IdentityServer.Web.FederationPassiveAuthentication.UpdateLoopDetectionCookie() in Microsoft.IdentityServer.Web.FederationPassiveAuthentication.SendSignInResponse(risp MSISSignInResponse)

```
Codice XML evento: <Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event">
<System> <Provider Name="AD FS 2.0" Guid="{20E25DDB-09E5-404B-8A56-EDAE2F12E81}" />
<EventID>364</EventID> <Version>0</Version> <Level>2</Level> <Task>0</Task> <Opcode>0</Opcod
<Keywords>0x8000 0000000001</Keywords> <TimeCreated SystemTime="2016-04-19T12:14:58.47462600
/> <EventRecordID>29385</EventRecordID> <Correlation ActivityID="{98778DB0-869A-4DD5-B3B6-05
65AC17BFFE}"/> <Execution ProcessID="2264" ThreadID="392" /> <Channel>AD FS 2.0/Admin</Chann
<Computer>myadfs.cisco.com</Computer> <Security UserID="S-1-5-21-1680627477-1295527365-15022
46-1105"/> </System> <UserData> <Event xmlns:auto-
ns2="http://schemas.microsoft.com/win/2004/08/events"
xmlns="http://schemas.microsoft.com/ActiveDirectoryFederationServices/2.0/Events"> <EventDat
<Data>Microsoft.IdentityServer.Web.InvalidRequestException: MSIS7042: La stessa sessione del
browser client ha effettuato 6 richieste negli ultimi 16 secondi. Per ulteriori informazioni
contattare l'amministratore. all'indirizzo
Microsoft.IdentityServer.Web.FederationPassiveAuthentication.UpdateLoopDetectionCookie()
all'indirizzo
Microsoft.IdentityServer.Web.FederationPassiveAuthentication.SendSignInResponse(risposta
MSISSignInResponse) </Data> </EventData> </Event> </UserData> </Event>
```

Registro Cisco IdS

```
2016-04-15 16:19:01.220 EDT(-0400) errore predefinito [IdSEndPoints-1] com.cisco.ccbu.ids
IdSEndPoint.java:102 - Richiesta di elaborazione eccezione
com.sun.identity.saml2.common.SAML2Eccezione: Codice di stato non valido nella risposta. 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:2038) at
com.cisco.ccbu.ids.auth.api.IdSSAMLAsync
Servlet.getAttributesMapFromSAMLResponse(IdSSAMLAsyncServlet.java:451)
```

Possibile causa

Troppe richieste provenienti da ADFS dalla stessa sessione del browser.

Azione consigliata

Ciò non dovrebbe di norma avvenire nella produzione. In questo caso, tuttavia, è possibile:

1. Controllare il Visualizzatore eventi di Windows AD FS.
2. Ricontrolla impostazioni attendibilità componente. Per ulteriori informazioni, *vedere* Configurare Cisco IdS e AD FS
3. Riaccedere.

8. ADFS non è configurato per firmare sia l'asserzione che il messaggio.

Riepilogo del problema

Richiesta di accesso non riuscita con errore 500 nel browser. Codice errore: invalidSignature

Fase di errore

Elaborazione risposta SAML

Messaggio di errore

Browser

Errore 500 con questo messaggio:
Codice errore:invalidSignature
Messaggio: firma non valida in ArtifactResponse.

Registro Cisco IdS:

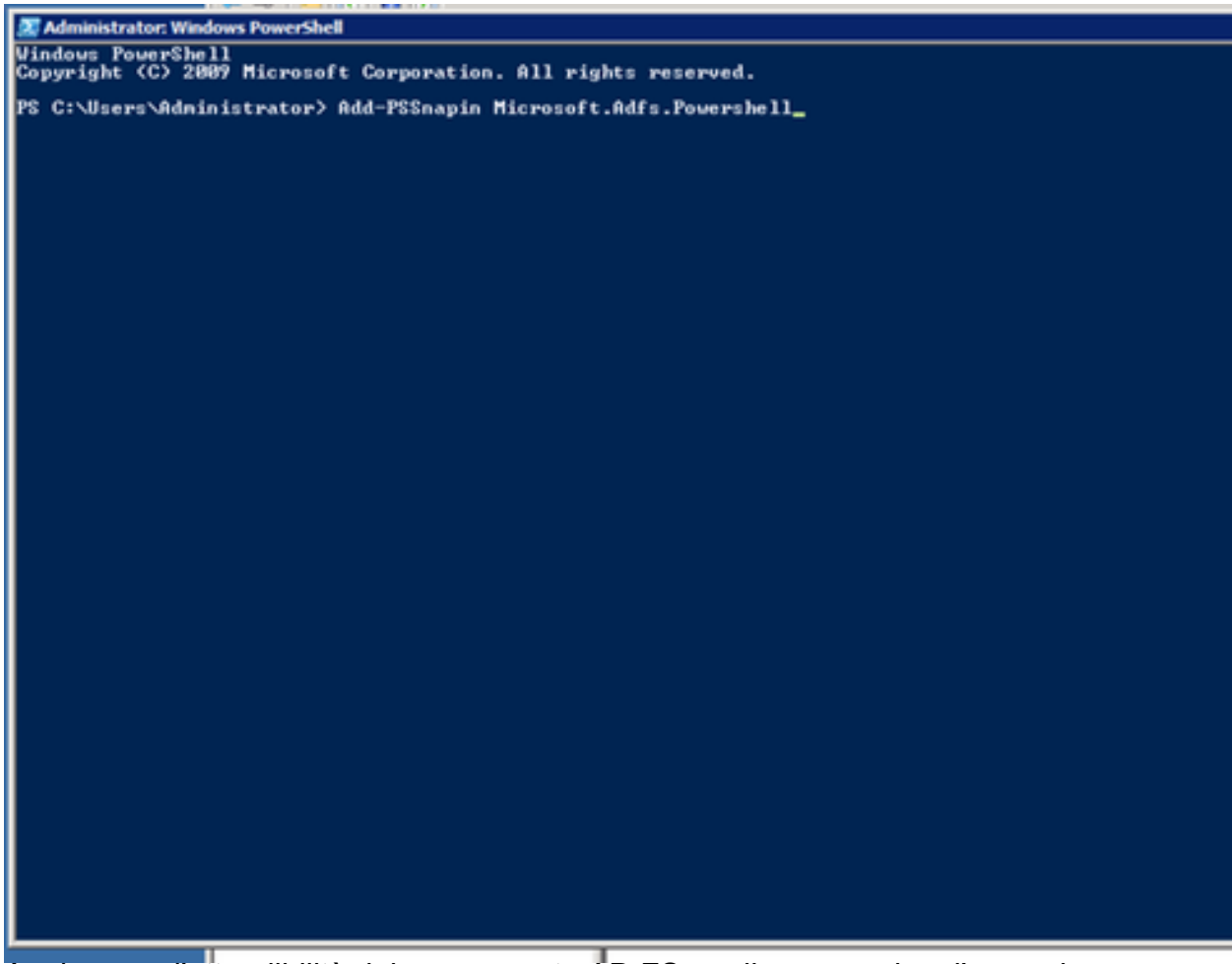
```
2016-08-24 10:53:10.494 IST(+0530) [IdSEndPoints-SAML-241] INFO saml2error.jsp saml2error_js
Elaborazione della risposta SAML non riuscita con codice: firma non valida; messaggio: Firma
ArtifactResponse. 2016-08-24 10:53:10.494 IST(+0530) [IdSEndPoints-SAML-241] ERRORE com.cisc
IdSSAMLAsyncServlet.java:298 - Elaborazione della risposta SAML non riuscita con eccezione
com.sun.identity.saml2.common.SAML2Eccezione: Firma non valida in Response. at
com.sun.identity.saml2.profile.SPACSUtils.getResponseFromPost(SPACSUtils.java:994) at
com.sun.identity.saml2.profile.SPACSUtils.getResponse(SPACSUtils.java:196) at
com.sun.identity.saml2.profile.SPACSUtils.processResponseForFedlet(SPACSUtils.java:2028) at
com.cisco.ccbu.ids.auth.api.IdSSAMsyncServlet.getAttributesMapFromSAMLResponse(IdSSAMLAsyncS
```

Possibile causa

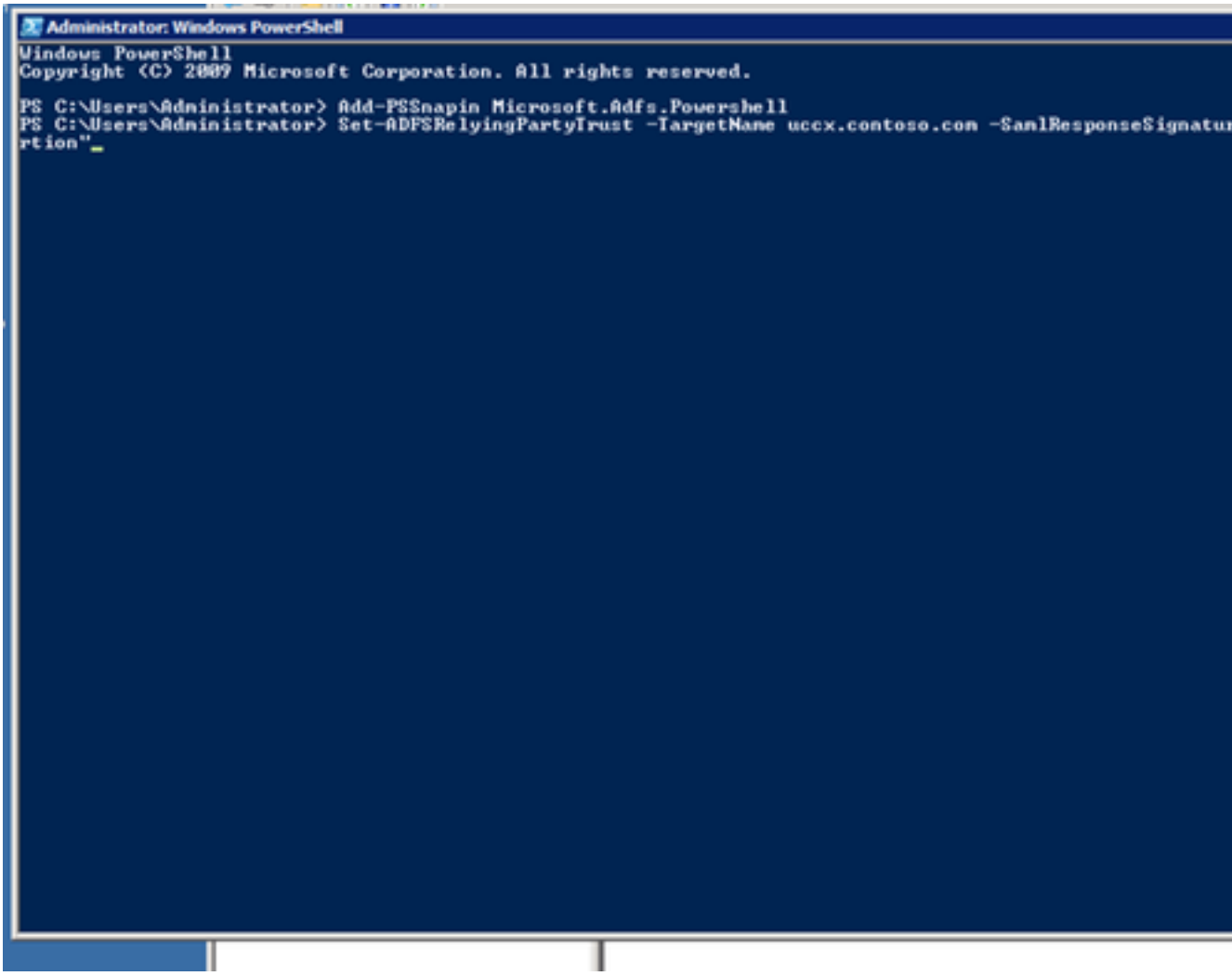
ADFS non è configurato per firmare sia l'asserzione che il messaggio.

Azione consigliata

1. Eseguire il comando PowerShell di AD FS: **Set-ADFSRelyingPartyTrust -TargetName <I attendibilità componente> -SamlResponseSignature "MessageAndAssertion"**
2. RDP al sistema AD.
3. Aprire **Powershell**.
4. Aggiungere gli snap-in di Windows PowerShell alla sessione corrente. Questo passaggio essere necessario in se si utilizza ADFS 3.0 poiché il cmdlet è già installato come parte e funzionalità.



5. Aggiungere l'attendibilità del componente AD FS per il messaggio e l'asserzione.



Informazioni correlate

Ciò è correlato alla configurazione del provider di identità descritta nell'articolo:

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