

# Aggiungere manualmente l'UID dell'attributo richiesto nel server ADFS

## Sommario

---

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Configurazione](#)

[Scenario 1](#)

[Scenario 2](#)

[Configurazioni](#)

[Aggiungere una regola attestazione personalizzata nel server ADFS in Attendibilità componente Webex](#)

[Passi per la creazione della regola](#)

---

## Introduzione

In questo documento viene descritto come aggiungere manualmente un UID attributo nell'attendibilità del componente ADFS utilizzando una sintassi.

## Prerequisiti

### Requisiti

- server ADFS
- Hub di controllo

### Componenti usati

- server ADFS
- Cisco Webex Control Hub
- Active Directory locale

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.

## Configurazione

Si tratta di un'opzione utile nel caso si verifichi un problema durante l'aggiunta di un'attestazione basata su attributi in ADFS a causa di un attributo esistente.

## Scenario 1

È presente un'attendibilità del componente esistente con una regola di attestazione creata con un attributo denominato UID o Uid.

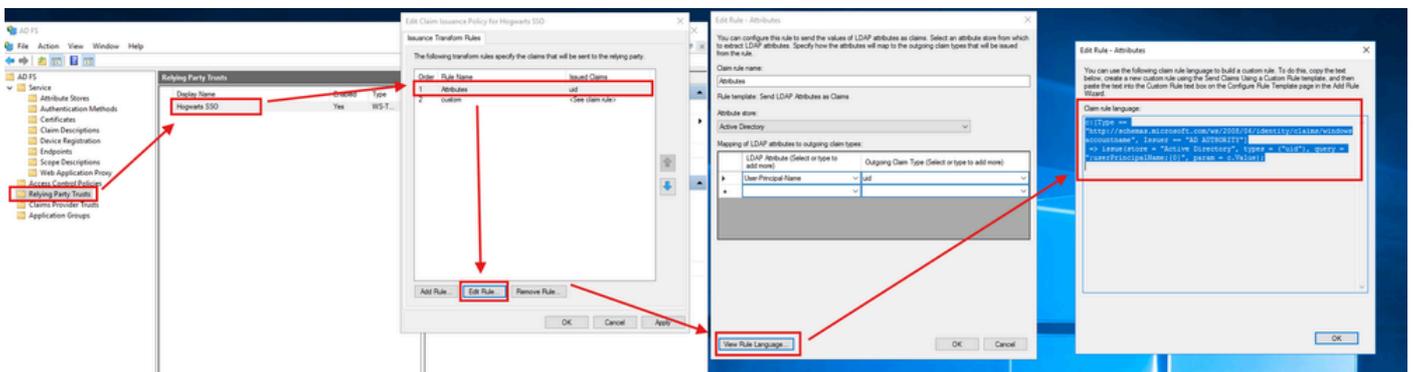
L'autenticazione ha esito negativo perché per l'attributo obbligatorio Webex (SP) viene fatta distinzione tra maiuscole e minuscole e deve essere uid e deve passare l'indirizzo e-mail dell'utente nella risposta SAML.

## Scenario 2

Si dispone di un'attendibilità parte con una regola Attestazione che passa un attributo denominato uid ma associato a un attributo diverso da quello necessario in Active Directory (emailAddress/UserPrincipleName). Ciò crea problemi.

## Configurazioni

In una configurazione ideale come quella della Cisco Webex Guide, la configurazione ADFS deve avere questo aspetto:



Gli amministratori ADFS possono visitare questa pagina dai trust della relying party-> Trust che hanno creato per Webex -> Edit Claim Issuance Policy -> Edit Rule -> Attributes -> View Rule Language.

La lingua della regola in testo normale è:

```
c:[Tipo == "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname",  
Emittente == "AUTORITÀ AD"]  
=> problema(archivio = "Active Directory", tipi = ("uid"), query = ";userPrincipalName;{0}",  
parametro = c.Value);
```

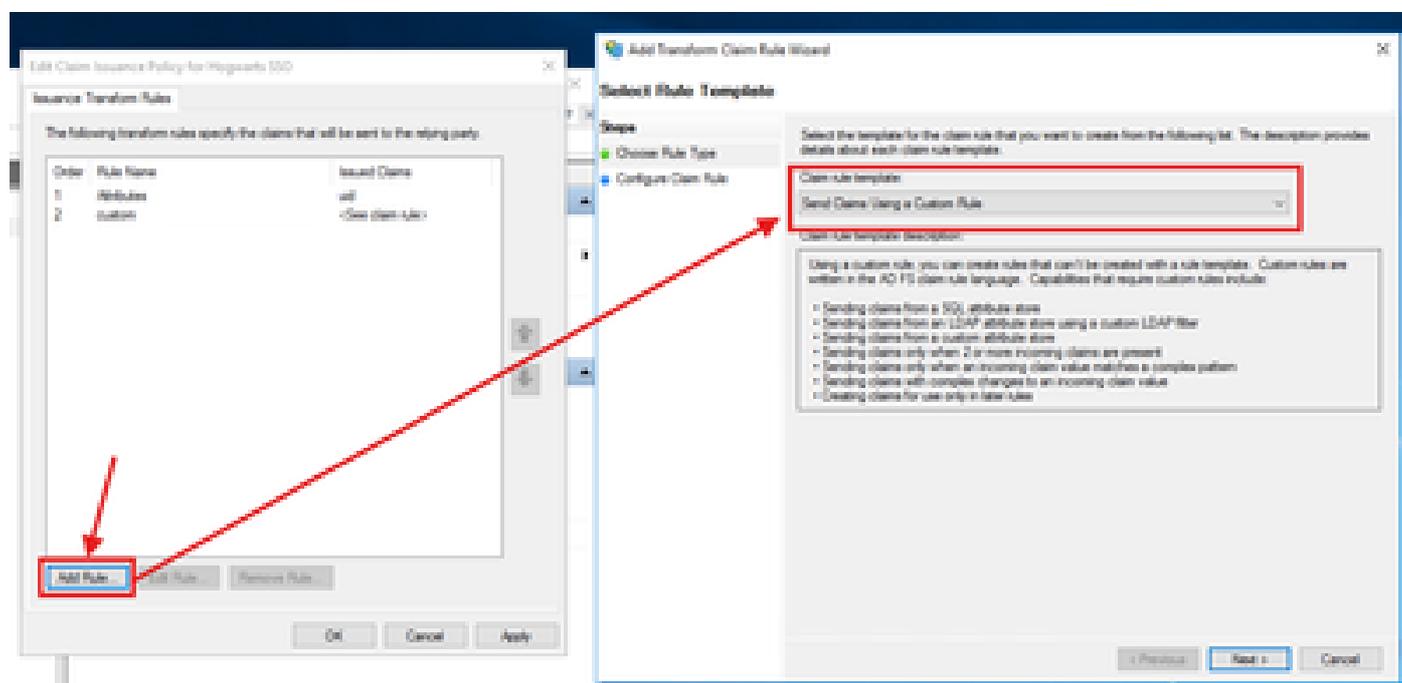
Poiché la configurazione non viene visualizzata correttamente, creare manualmente la regola utilizzando il testo normale della lingua della regola.

# Aggiungere una regola attestazione personalizzata nel server ADFS in Attendibilità componente Webex

## Passi per la creazione della regola

1. Nel riquadro principale ADFS selezionare la relazione di trust creata e quindi selezionare Modifica regole attestazione. Nella scheda Regole trasformazione rilascio, selezionare Aggiungi regola.
2. Selezionare Invia attestazioni utilizzando una regola personalizzata, quindi scegliere Avanti.
3. Copiare la regola dall'editor di testo (partendo da c:) e incollarla nella casella della regola personalizzata sul server ADFS.

Il formato deve essere simile al seguente:



Una volta eseguita questa operazione, è possibile eseguire il test dell'SSO dall'hub di controllo e che deve funzionare come previsto.

## Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).