

# Risoluzione dei problemi di integrazione di UCCE SSO con Azure IdP

## Sommario

---

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Problema: Il Certificato Non Corrisponde](#)

[Soluzione](#)

[Problema: ADSTS900235 - Problema contesto di autenticazione](#)

[Soluzione](#)

[Problema: risposta SAML non firmata](#)

[Soluzione](#)

[Problema: problema con le regole attestazione](#)

[Soluzione](#)

[Problema: ADSTS50011 - L'URL di risposta non corrisponde](#)

[Soluzione](#)

---

## Introduzione

In questo documento viene descritto come risolvere alcuni problemi comuni che si verificano durante l'esecuzione dell'integrazione UCCE SSO con Microsoft Azure IdP.

Contributo di Anurag Atul Agarwal, Cisco TAC Engineer.

## Prerequisiti

### Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- SAML (Security Assertion Markup Language) 2.0
- Cisco Unified/Packaged Contact Center Enterprise UCCE/PCCE
- Single Sign-On (SSO)
- Cisco Identity Service (IdS)
- Provider di identità (IdP)

### Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Azure IdP
- UCCE 12.0.1
- Cisco IdS 12.0.1

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

In questo documento vengono descritti alcuni dei problemi comuni che si verificano durante l'integrazione di Cisco Identity Service (IdS) e Identity Provider (IdP) per l'SSO basato su Azure e le relative potenziali correzioni. Si consiglia sempre di raccogliere questi registri per risolvere i problemi di integrazione SSO:

- Log IdS Cisco: collegamento alla raccolta: [log IDS](#)
- Registri console browser
- Qualsiasi log da IdP

## Problema: Il Certificato Non Corrisponde

Test SSO non riuscito con il messaggio 'IdS non è stato in grado di elaborare la risposta SAML anche se l'autenticazione è riuscita' e nei log IdS viene visualizzato il messaggio di errore: "Elaborazione della risposta SAML non riuscita con eccezione com.sun.identity.saml2.common.SAML2Exception: Il certificato di firma non corrisponde a quanto definito nei metadati dell'entità"

## Soluzione

Verificare il certificato e l'impostazione dell'algoritmo di firma in Azure. Verificare che corrisponda all'algoritmo hash supportato in base alla versione di IdS. Fare riferimento al capitolo 'Single Sign-On' in [Features Guide](#) e verificare l'algoritmo hash sicuro supportato. Scaricare il file di metadati IdP più recente e caricarlo in Cisco IdS tramite l'interfaccia utente di Identity Service Management.

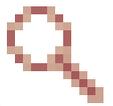
## Problema: ADSTS900235 - Problema contesto di autenticazione

Il test SSO reindirizza alla pagina Microsoft e ha esito negativo con il messaggio: "Si sono verificati problemi durante l'accesso".

ADSTS900235: il valore RequestedAuthenticationContext Comparison della richiesta di autenticazione SAML deve essere Exact. Valore ricevuto: minimo

## Soluzione

Potrebbe essere necessario configurare AuthContext come descritto nel bug [CSCvm69290](#)  
. Contattare Cisco TAC per implementare la soluzione alternativa in IdS.



## Problema: risposta SAML non firmata

Test SSO non riuscito con messaggio. IdS non è stato in grado di elaborare la risposta SAML anche se l'autenticazione è riuscita. I registri IdS visualizzano il messaggio di errore:  
"Elaborazione della risposta SAML non riuscita con eccezione  
com.sun.identity.saml2.common.SAML2Exception: la risposta non è firmata."

## Soluzione

Azure IdP deve inviare l'asserzione firmata a IdS. Modifica l'impostazione di Azure per avere l'opzione di firma: Firma la risposta e l'asserzione SAML

## Problema: problema con le regole attestazione

Test SSO non riuscito con messaggio 'Errore di configurazione IdP: elaborazione SAML non riuscita. Impossibile recuperare l'entità utente dalla risposta SAML.' e i registri IdS visualizzano il messaggio di errore: "Elaborazione della risposta SAML non riuscita con eccezione  
com.sun.identity.saml.common.SAMLException: impossibile recuperare l'entità utente dalla risposta SAML."

## Soluzione

Questo errore fa riferimento a 'Nomi attestazione' errati configurati in Azure. Questo può accadere con altri attributi come UID, NameID, ecc. e errori simili con nomi di attributi diversi è generato. Per risolvere il problema, individuare qualsiasi attributo in Azure nel formato 'schemas.xmlsoap.org/ws/2005/05/identity/claims/<nome\_attributo>'. Rimuovere tutti gli elementi prima del nome effettivo dell'attributo.

In questa sezione viene fornita la configurazione di esempio per ADFS nella guida alle funzionalità e che deve essere replicata in Azure.

[Esempio di configurazione di ADFS](#)

## Problema: ADSTS50011 - L'URL di risposta non corrisponde

Il test SSO reindirizza alla pagina Microsoft e ha esito negativo con il messaggio: "Si sono verificati problemi durante l'accesso.

ADSTS50011: l'URL di risposta specificato nella richiesta non corrisponde all'URL di risposta

configurato per l'applicazione"

## Soluzione

Contattare Cisco TAC. È necessario archiviare il parametro 'Assertion Consumer Service' nella radice del nodo IdS in cui si verifica un errore. Se il parametro è corretto, Microsoft Azure deve risolvere il problema.

## 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).