Configurare ADFS nel dashboard ombrello

Sommario

Introduzione

In questo documento viene descritto come configurare ADFS in Cisco Umbrella Dashboard per consentire gli accessi con un indirizzo di posta elettronica.

Panoramica

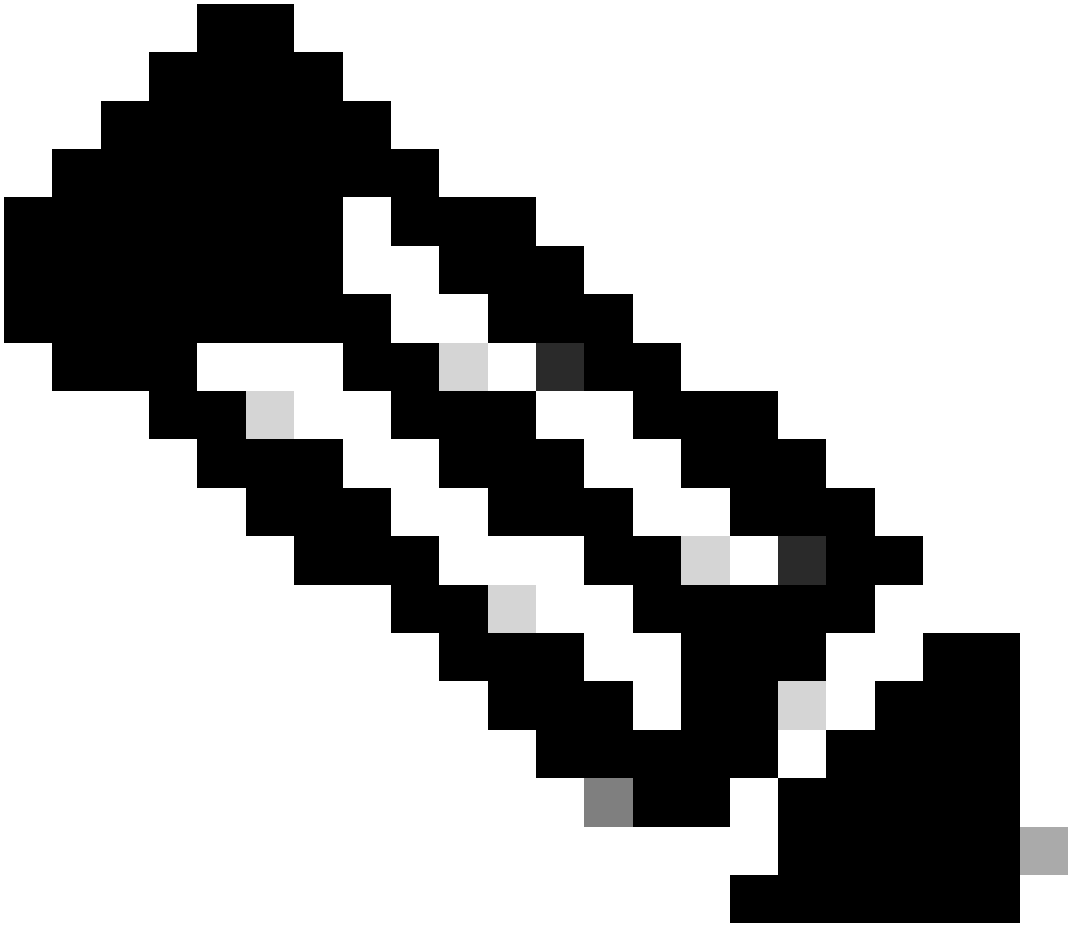
Questo documento è relativo agli utenti che desiderano configurare l'autenticazione Single Sign-On tra Cisco Umbrella Dashboard e Active Directory Federated Services (ADFS). Questo documento è un'appendice alle istruzioni principali di ADFS riportate nella Guida alla configurazione di Cisco Umbrella con Active Directory Federation Services (ADFS) versione 3.0 tramite SAML.

In questo articolo viene inoltre fornito un esempio di configurazione di ADFS per consentire l'accesso con un indirizzo di posta elettronica.

Configurazione

Per impostazione predefinita, ADFS esegue l'autenticazione degli utenti in base al relativo nome dell'entità utente (UPN). Spesso questo UPN corrisponde sia all'indirizzo di posta elettronica che all'indirizzo di posta elettronica dell'account Umbrella dell'utente, pertanto non è richiesta alcuna azione.

Tuttavia, in alcuni casi, l'indirizzo di posta elettronica dell'utente è diverso dal relativo UPN e sono necessari questi passaggi aggiuntivi.



Nota: Questo esempio viene fornito "così com'è" in base a un ambiente ADFS funzionante. Il supporto Umbrella non è in grado di supportare la configurazione dei singoli ambienti ADFS.

Passaggio 1. Consenti accesso indirizzo di posta elettronica (facoltativo)

Il comando PowerShell configura AD FS in modo da consentire l'utilizzo dell'attributo mail come ID di accesso. Sostituire <Domain> con il nome del dominio Active Directory:

```
Set-AdfsClaimsProviderTrust -TargetIdentifier "AD AUTHORITY" -AlternateLoginID mail -LookupForests <Dom
```

In questo modo si evita di creare confusione negli utenti finali, poiché possono utilizzare lo stesso nome utente per entrambi i sistemi. Dopo questa modifica, l'utente può accedere come:

- Immettere il nome utente Umbrella (ad esempio, email@domain.tld)
- Immettere email@domain.tld o upn@domain.tld come nome utente ADFS

Se questo passaggio non viene seguito, l'utente finale può dover utilizzare un nome utente diverso per entrambi i sistemi:

- Immettere il nome utente Umbrella (ad esempio, email@domain.tld)
- Immettere upn@domain.tld come nome utente ADFS

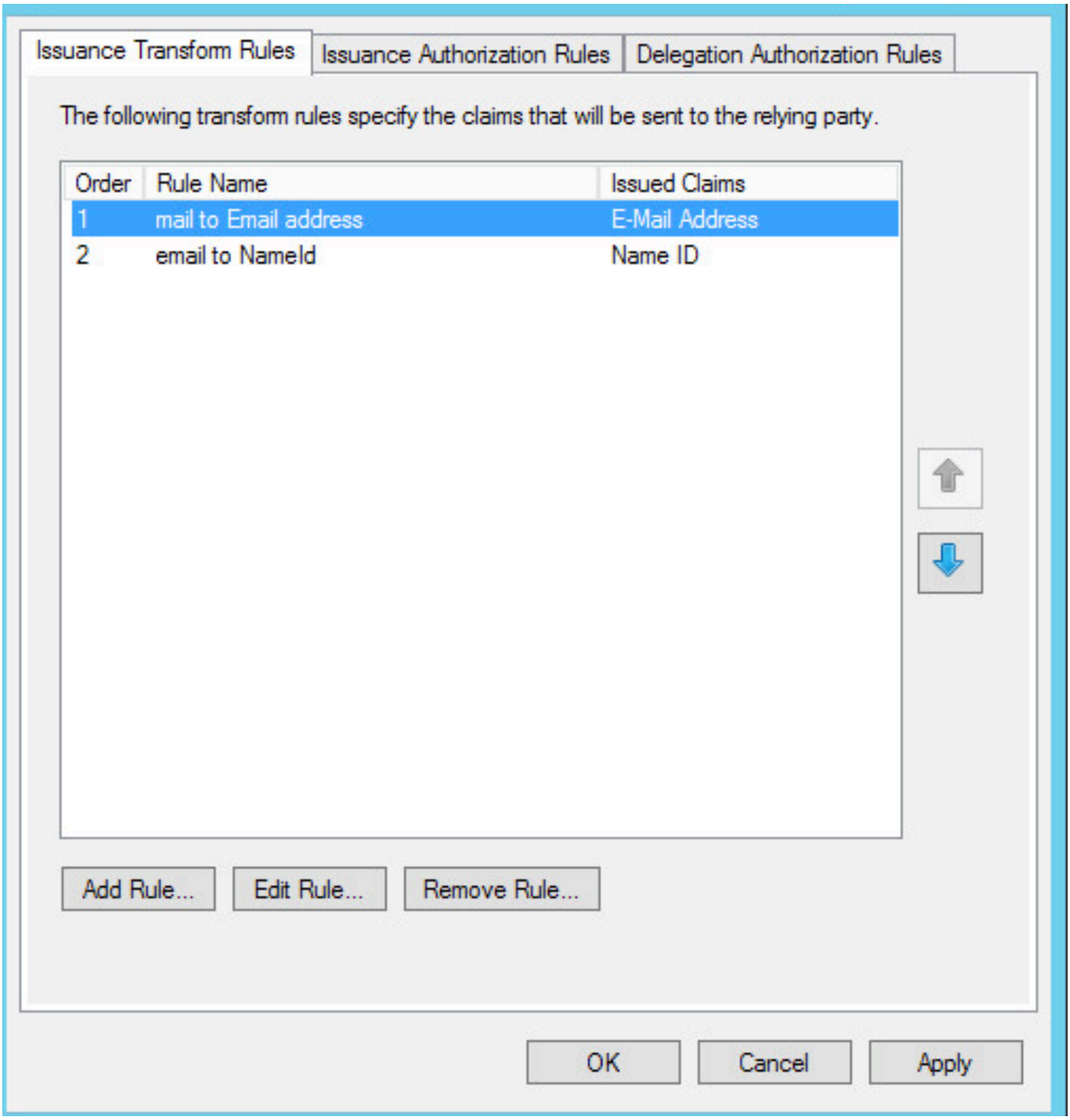
Passaggio 2. Modifica regole attestazioni (obbligatorio)

Esaminare le informazioni nelle istruzioni di ADFS contenute nella Guida alla configurazione di Cisco Umbrella con Active Directory Federation Services (ADFS) versione 3.0 tramite SAML. La regola attestazioni userPrincipalName in Email address deve essere eliminata e sostituita con la regola denominata mail to Email address.

In questo modo viene indicato ad ADFS di includere l'attributo mail nella risposta SAML:

```
c:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname", Issuer == "AD
=> issue(store = "Active Directory", types = ("http://schemas.xmlsoap.org/ws/2005/05/identity/claims/em
```

Le regole attestazioni devono essere configurate nell'ordine corretto con l'indirizzo di posta elettronica come prima regola:



360024534972

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).