# Utilizzo dell'URL metadati fissi di Umbrella per l'autenticazione SWG SAML

## Sommario



## Introduzione

In questo documento viene descritto come utilizzare l'URL di metadati fissi di Umbrella per l'autenticazione SAML Secure Web Gateway (SWG).

## Prerequisiti

### Requisiti

Nessun requisito specifico previsto per questo documento.

### Componenti usati

Le informazioni fornite in questo documento si basano su Umbrella SWG.

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.

## URL metadati fissi

Quando si utilizza l'autenticazione SAML per Umbrella SWG, sono disponibili due opzioni per l'importazione delle informazioni sul certificato nel provider di identità (IdP). Questa operazione è obbligatoria per gli IdP che verificano il certificato di firma della richiesta.

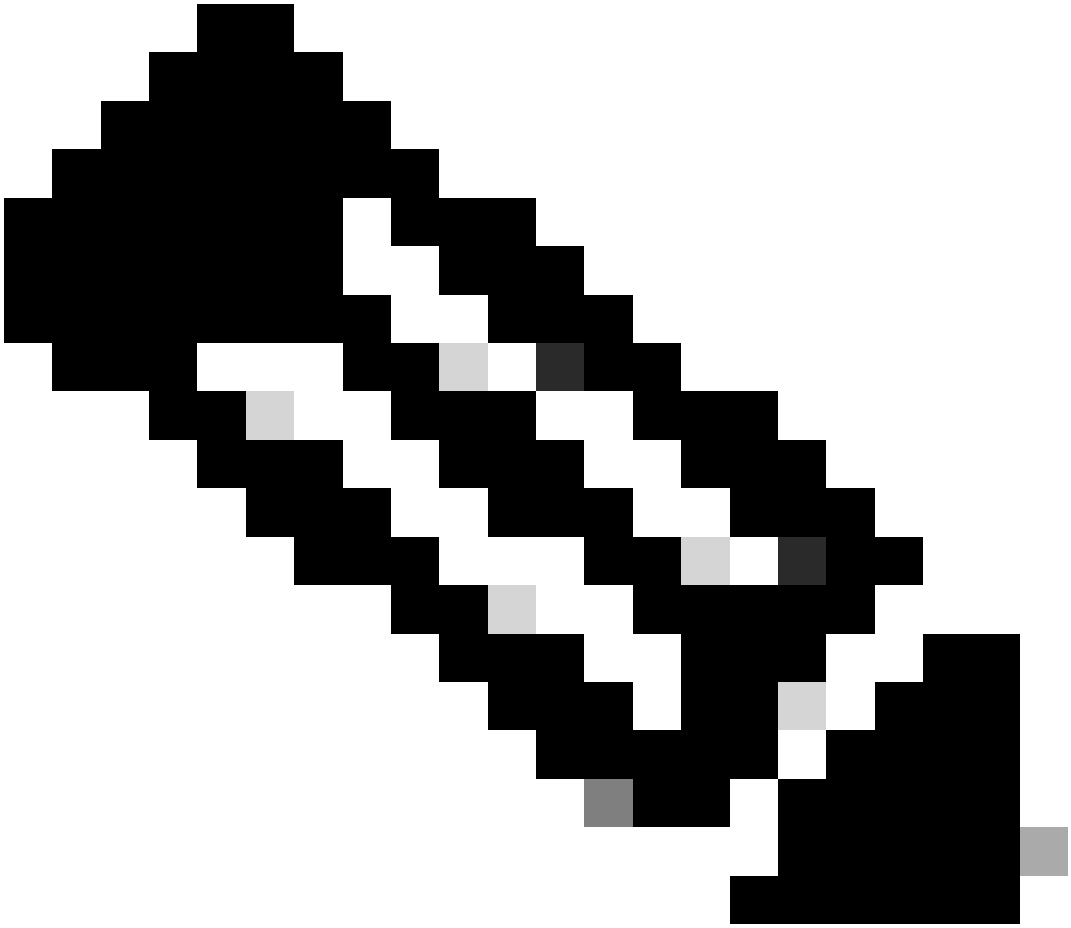
1. Configurazione automatica tramite URL metadati fissi:

https://api.umbrella.com/admin/v2/samlsp/certificates/Cisco_Umbrella_SP_Metadata.xml

2. Importazione manuale del nuovo certificato di firma. Questa operazione deve essere eseguita ogni anno, in quanto il certificato viene sostituito.

La prima opzione è ora il metodo di configurazione preferito per i provider di identità (IdP) che supportano gli aggiornamenti automatici basati su URL dei metadati. Sono inclusi gli IdP più diffusi, ad esempio Microsoft ADFS e Ping Identity.  Il vantaggio è che l'IdP importa automaticamente il nuovo certificato ogni anno senza interventi manuali.

---



Nota: Molti IDP non eseguono la convalida delle firme delle richieste SAML e pertanto questi passaggi non sono necessari.  In caso di dubbi, contattare il fornitore del provider di identità per la conferma.

---

## Requisiti

Requisiti per accedere all'URL dei metadati

- IdP che supporta gli aggiornamenti automatici dei metadati del provider di servizi dall'URL

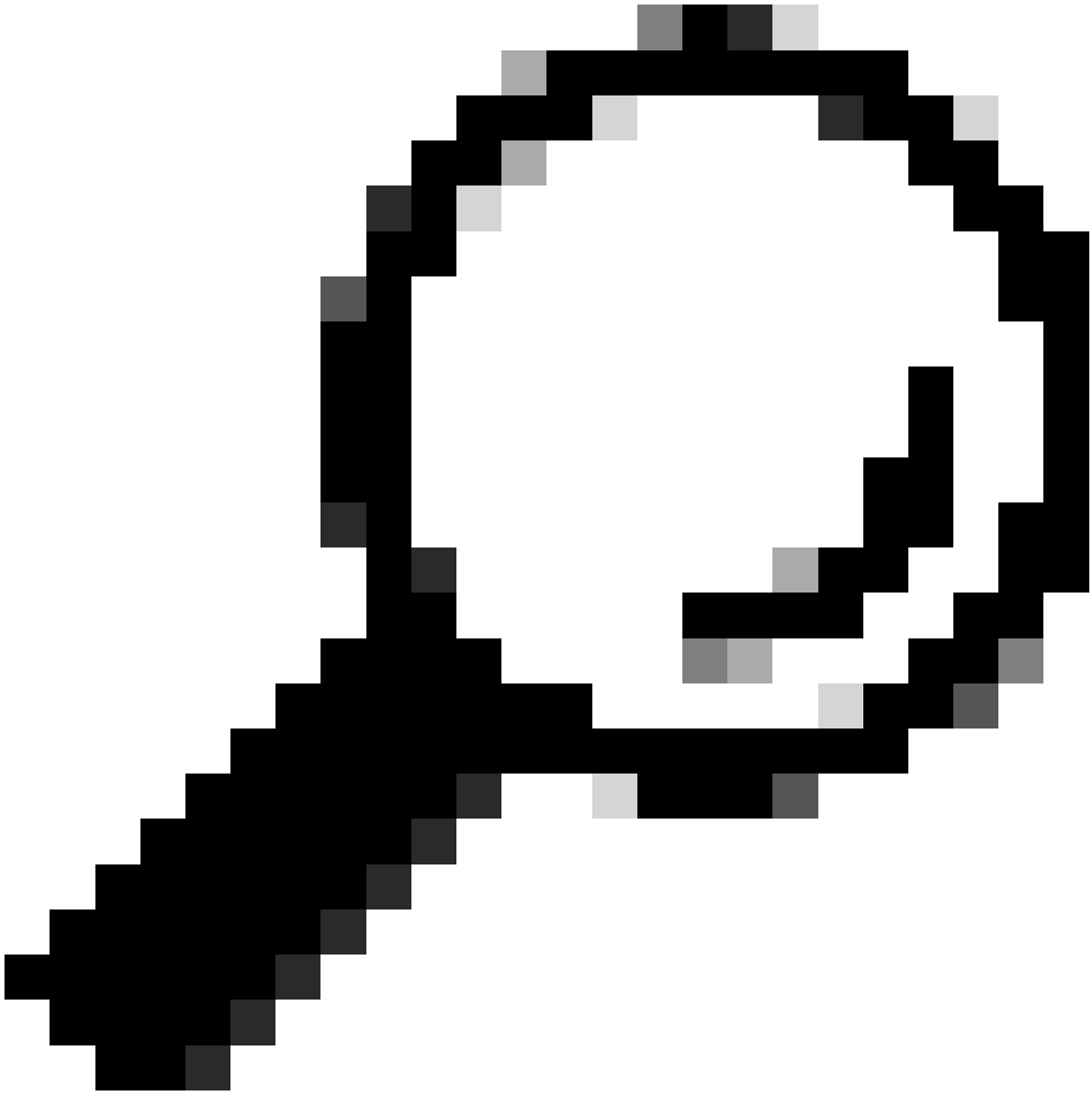
(ad esempio ADFS, Ping)

- La piattaforma IdP deve essere in grado di accedere all'URL dei nostri metadati e agli URL associati dell'autorità di certificazione
- La piattaforma IdP deve inoltre essere in grado di accedere agli URL dell'autorità di certificazione per il certificato stesso
- Per connettersi all'URL dei metadati in modo sicuro, la piattaforma IdP deve supportare TLS 1.2. Se l'applicazione IDP utilizza .NET Framework 4.6.1 o versione precedente, potrebbe essere necessaria un'ulteriore configurazione, come indicato nella documentazione di Microsoft.

## Esempio: Microsoft ADFS

È possibile configurare l'URL dei metadati fissi modificando l'impostazione Attendibilità componente per Umbrella:

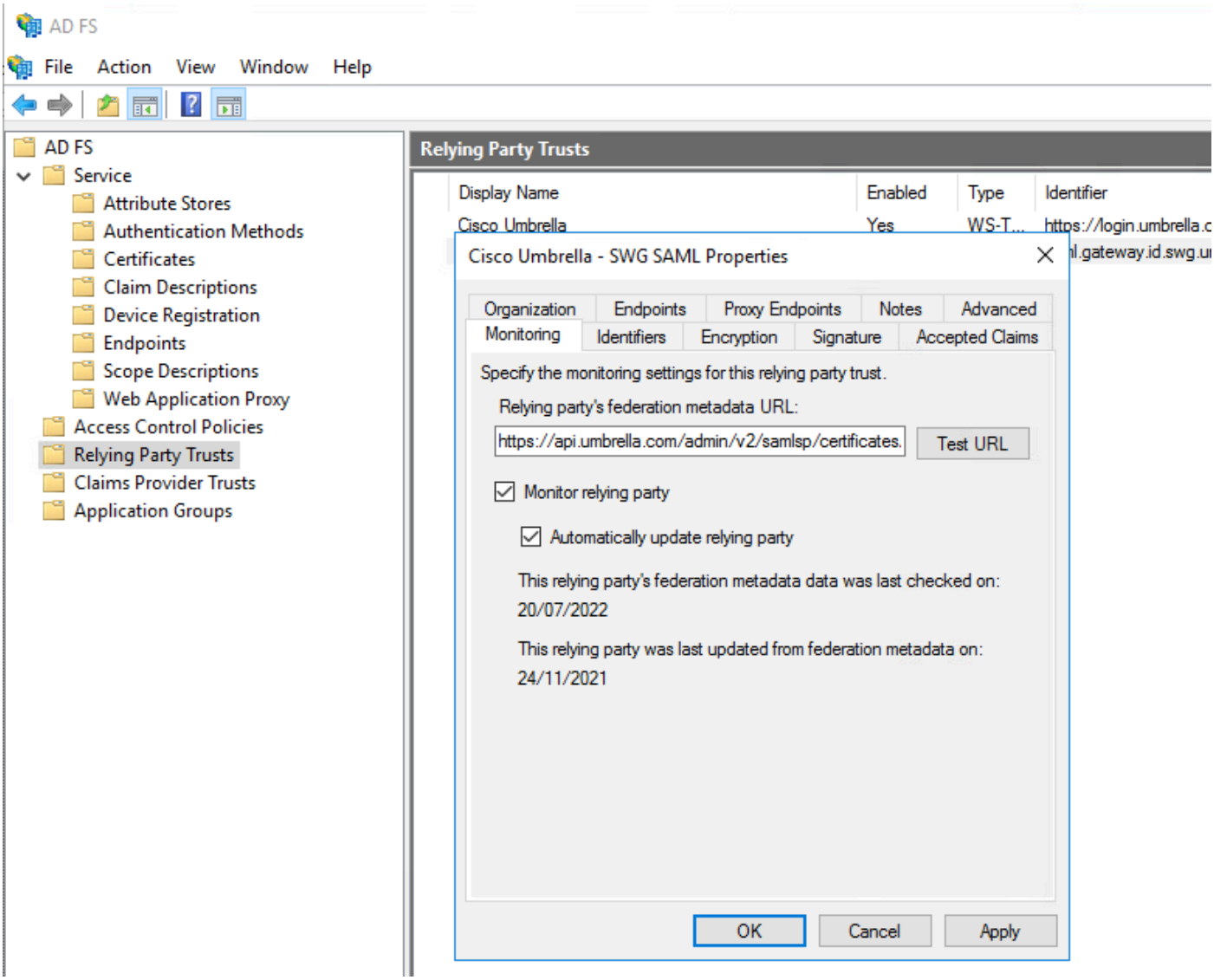
1. Passare alla scheda Monitoraggio e immettere l'URL metadati.
2. Selezionare Controlla relying party e Aggiorna automaticamente relying party.



Suggerimento: Selezionare il pulsante Prova URL per verificare che ADFS contatta l'URL correttamente.

---

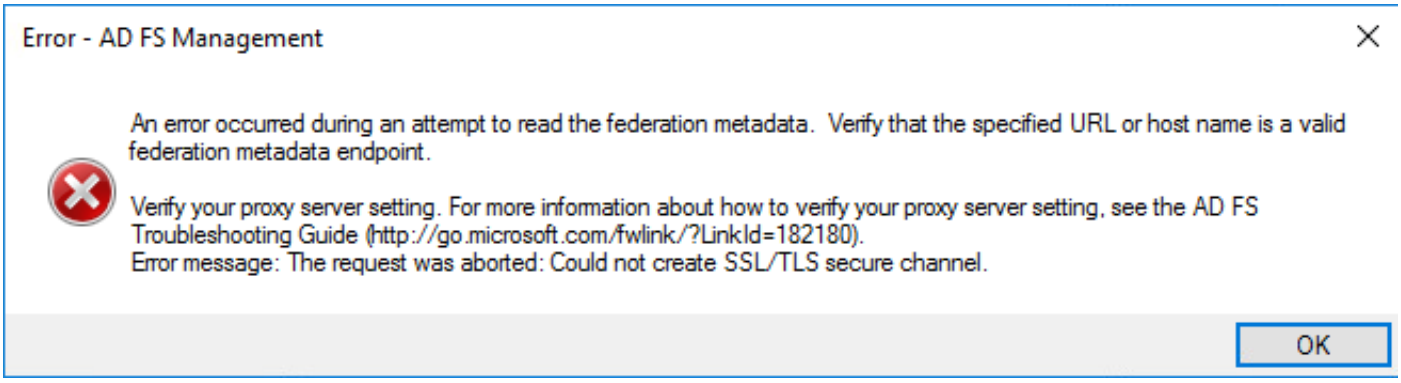
3. Selezionare Applica.




ADFS_RelyingPartyTrust.png

# Risoluzione degli errori

Se viene visualizzato l'errore, "Si è verificato un errore durante un tentativo di lettura dei metadati della federazione. Verificare che l'URL o il nome host specificato sia un "endpoint dei metadati federativi valido" durante il test dell'URL. Ciò indica in genere che è necessaria una modifica del Registro di sistema per impostare la versione di .NET Framework in modo che utilizzi la crittografia avanzata e supporti TLS 1.2.




ADFSmetadata_TLS_error.png

I dettagli completi su queste modifiche sono pubblicati da Microsoft nella sezione .Net Framework della documentazione di Microsoft.

In genere, tuttavia, questa operazione richiede la creazione di questa chiave, quindi la chiusura e la riapertura della console Gestione ADFS:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319]
"SchUseStrongCrypto" = dword:00000001
```

## Limitazione: Caratteristica EntityID specifica dell'organizzazione

Se si utilizza la funzionalità EntityID specifica dell'organizzazione SAML Umbrella, non è necessario utilizzare il meccanismo di aggiornamento dei metadati basato su URL. L'ID entità specifico dell'organizzazione si applica solo se sono presenti più organizzazioni Umbrella collegate allo stesso provider di identità. In questo scenario è necessario aggiungere manualmente il certificato a ogni configurazione IDP.

## Importazione manuale certificati (alternativa)

Se il provider di identità non supporta gli aggiornamenti basati su URL, è necessario importare manualmente ogni anno il nuovo certificato di firma della richiesta Umbrella nel provider di identità.

- Il certificato viene fornito nel portale Annunci di Dell ogni anno poco prima della data di scadenza. Sottoscrivi il portale per le notifiche
- Aggiungere il nuovo certificato all'elenco dei certificati del provider di servizi o della relying party nel provider di identità.
    - NON eliminare i certificati correnti.  Umbrella continua a firmare con il vecchio certificato fino alla scadenza.
- Se l'IdP non contiene la capacità di importare un certificato del provider di servizi o del componente, si tratta di una forte indicazione del fatto che non convalida le richieste SAML e non sono necessarie ulteriori azioni.  Per conferma, contattare il fornitore del provider di identità.

Se si verifica un errore "UPN non configurato" dopo l'importazione del nuovo certificato, significa che è stato generato un errore.  Consultare questo articolo per la risoluzione dei problemi: SWG SAML - Errore UPN non configurato

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).