Risoluzione dei problemi relativi all'errore UPN non configurato dopo il rinnovo del certificato Umbrella in SWG SAML

Sommario

Introduzione

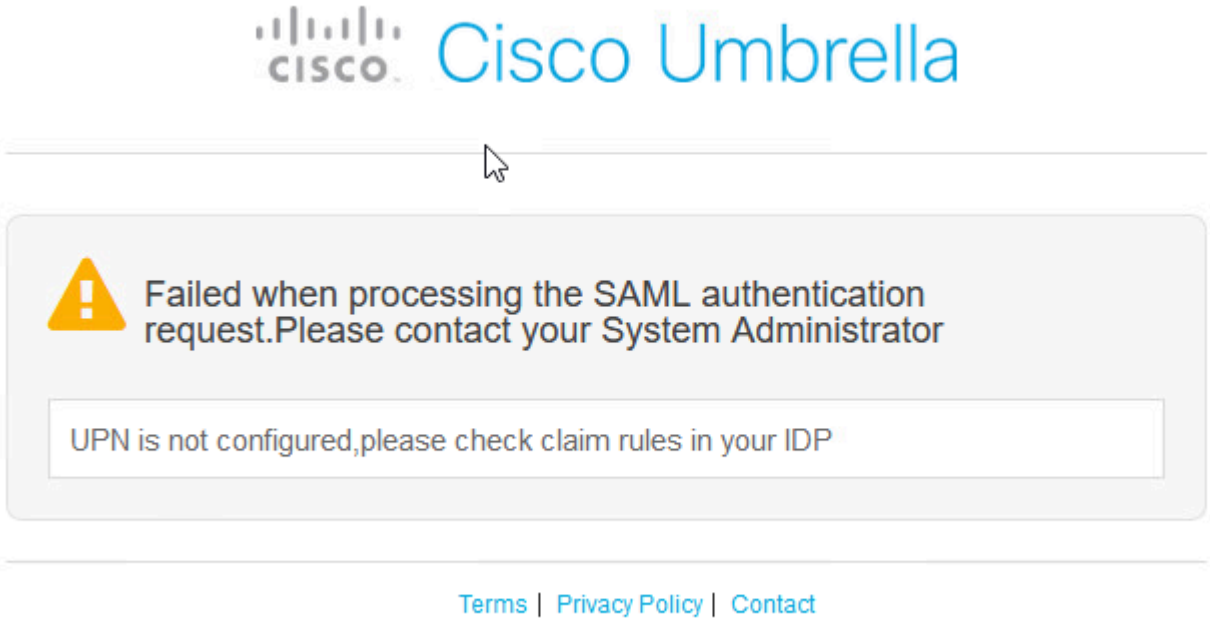
In questo documento viene descritto come risolvere un errore "UPN non configurato" dopo il rinnovo del certificato di firma SAML Umbrella.

Panoramica

L'errore "UPN non configurato" è un errore generico che può verificarsi per diversi motivi. Una possibile causa è la scadenza del certificato di firma SAML Umbrella che viene rinnovato annualmente. Per informazioni aggiornate sulla scadenza del certificato, consultare il portale Annunci.

Se il certificato Umbrella scade e non è stata intrapresa alcuna azione, gli utenti vengono bloccati dall'accesso a Internet con questi potenziali errori:

- Errore "UPN non configurato" di marchio Umbrella durante l'esplorazione del Web tramite SWG
- Altri errori presentati dal provider di identità



In questo articolo vengono illustrati due diversi scenari che causano l'errore:

- Scenario 1 - Errore dopo l'importazione di un nuovo certificato Umbrella
- Scenario 2 - Errore dopo la scadenza del certificato Umbrella

Conseguenze

I nuovi accessi utente per SWG non riescono, bloccando l'accesso a Internet. Ciò non si applica necessariamente a tutti gli utenti, ma viene attivato quando:

- La sessione di un utente scade a causa dell'impostazione di riautenticazione (ad esempio, giornaliera)
- Un nuovo utente accede
- Un utente cancella la cache del browser o utilizza un nuovo browser.

Scenario 1 - Errore dopo l'importazione di un nuovo certificato Umbrella

Se l'errore si verifica direttamente dopo aver apportato una modifica (ad esempio, in preparazione del rinnovo del certificato di Umbrella), è probabile che sia stato commesso un errore con l'importazione del certificato.

Assicurarsi che vengano importati sia i certificati Umbrella correnti che quelli nuovi

In preparazione al rinnovo del certificato, Umbrella rende disponibile un nuovo certificato, ma il nuovo certificato non viene utilizzato per la firma fino alla scadenza. Pertanto, la configurazione

IdP deve avere due certificati elencati nella configurazione del provider di servizi o della relying party. Riconfigurare dai metadati per risolvere il problema.

- Certificato corrente - Con una prossima data di scadenza
- Certificato futuro - Valido per l'anno successivo.

Verificare che il mapping Attributo Attestazioni sia corretto

Se il provider di servizi/componente è stato riconfigurato, è necessario apportare ulteriori modifiche alla configurazione per assicurarsi che l'IdP invii gli attributi necessari per convalidare la risposta SAML. Questa operazione è comune con Microsoft ADFS, in cui è necessario ricreare la mappa delle richieste di rimborso.

Scenario 2 - Errore dopo la scadenza del certificato Umbrella

Se l'errore si verifica dopo la scadenza del certificato Umbrella e non sono state apportate modifiche all'IdP.

Verificare che il nuovo certificato sia stato importato nel provider di identità

Per risolvere il problema Importare manualmente il nuovo certificato nel provider di identità. Quando il certificato sta per essere rinnovato, il nuovo certificato viene reso disponibile nel portale Annunci.

(CONSIGLIATO) Configurare gli aggiornamenti automatici dei metadati

Umbrella ora fornisce un URL di metadati fisso che può essere utilizzato per aggiornamenti di metadati senza problemi. È consigliabile configurare questo metodo per impedire azioni manuali durante il successivo rollover del certificato.

Verificare che gli indirizzi del server CRL siano accessibili al provider di identità

Umbrella ora utilizza un'autorità di certificazione diversa, quindi assicurati che questi indirizzi CRL/OCSP siano disponibili per il server IdP:

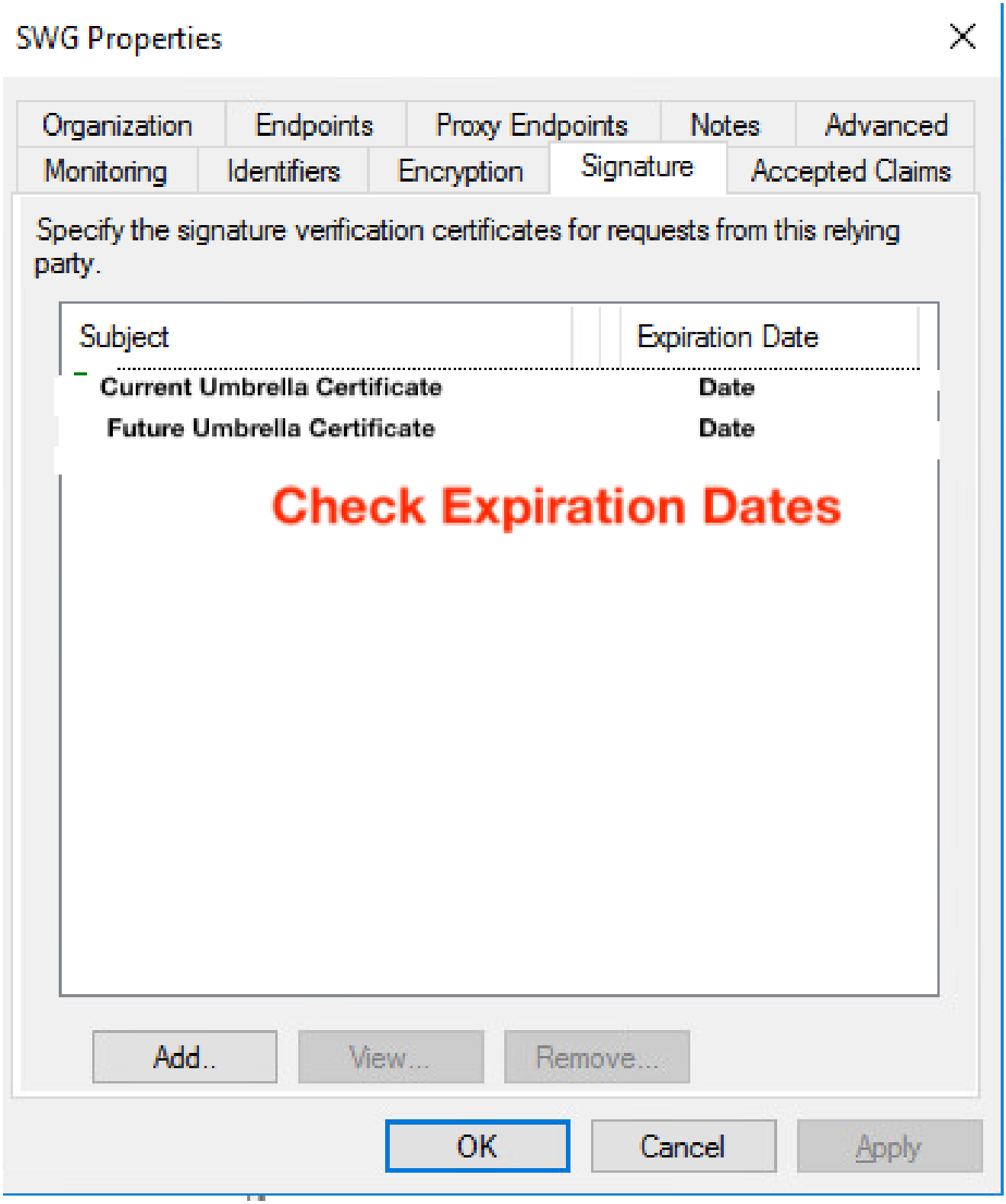
- http://validation.identrust.com
- http://commercial.ocsp.identrust.com

Microsoft ADFS - Esempio di importazione manuale dei certificati

Microsoft ADFS è un IdP comune noto per convalidare le firme delle richieste. Il certificato può essere aggiornato come segue:

- Apri gestione ADFS
- Espandere i trust tra relying party e individuare l'RP per Umbrella SWG
- Fare clic con il pulsante destro del mouse sul componente in ADFS e selezionare Proprietà

- Caricare il nuovo certificato nella scheda Firma



Quando si avvicina la data di scadenza del certificato, i metadati forniti da Cisco includono più certificati per preparare il rollover senza problemi. Non eliminare il certificato corrente mentre è ancora valido. Cisco continua a firmare con il certificato corrente fino alla data/ora di scadenza.

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).