Risoluzione Dei Problemi Di CCE Single Sign-On Con Gestione Certificati Identity Service (IdS)

Sommario

Introduzione

In questo documento viene descritto in dettaglio come rigenerare e scambiare i certificati SAML in UCCE/PCCE, garantendo processi sicuri e trasparenti.

Contributo di Nagarajan Paramasivam, Cisco TAC Engineer.

Prerequisiti

Requisiti

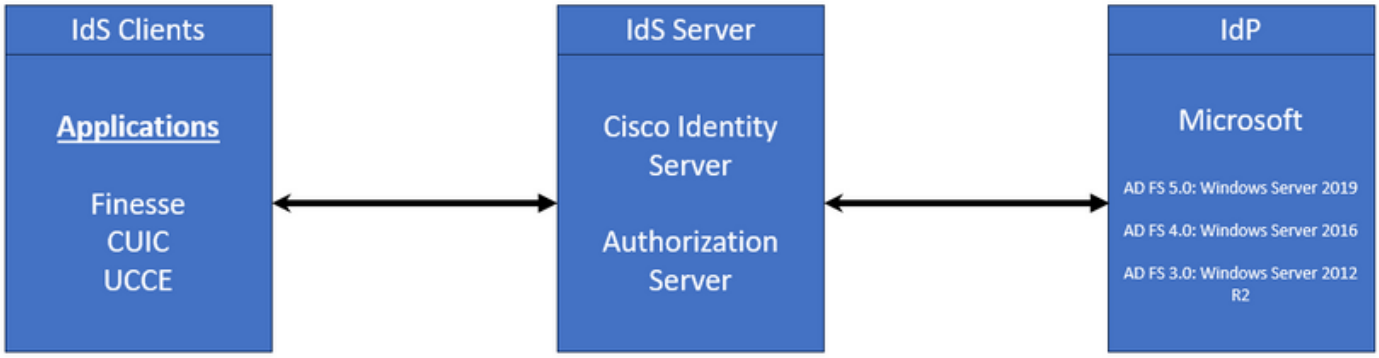
Cisco raccomanda la conoscenza dei seguenti argomenti:

- Packaged/Unified Contact Center Enterprise (PCCE/UCCE)
- Piattaforma VOS (Voice Operating System)
- Gestione certificati
- SAML (Security Assertion Markup Language)
- SSL (Secure Sockets Layer)
- Active Directory Federation Services (ADFS)
- Single Sign-On (SSO)

Componenti usati

Le informazioni fornite in questo documento si basano sui seguenti componenti:

- Cisco Identity Service (Cisco IdS)
- Provider di identità (IdP) - Microsoft Windows ADFS



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 UCCE/PCCE Cisco Identity Service (Cisco IdS) fornisce l'autorizzazione tra il provider di identità (IdP) e le applicazioni.

Quando si configura l'IdS Cisco, viene impostato uno scambio di metadati tra l'IdS Cisco e l'IdP. Questo scambio stabilisce una relazione di trust che consente quindi alle applicazioni di utilizzare gli ID Cisco per l'SSO. Per stabilire la relazione di trust, è necessario scaricare un file di metadati dagli IdS Cisco e caricarlo nell'IdP.

Il certificato SAML è simile a un certificato SSL e, analogamente, deve essere aggiornato o modificato quando si verificano determinate situazioni. La rigenerazione o lo swapping del certificato SAML sul server Cisco Identity Services (IdS) può causare un'interruzione nella connessione trusted con il provider di identità (IdP). Questa interruzione può causare problemi in cui i client o gli utenti che si basano su Single Sign-On non possono ottenere l'autorizzazione necessaria per accedere al sistema.

Questo documento ha lo scopo di coprire una vasta gamma di situazioni comuni in cui è necessario creare un nuovo certificato SAML sul server Cisco IdS. Viene inoltre illustrato come assegnare il nuovo certificato al provider di identità (IdP) in modo che sia possibile ricreare il trust. In questo modo, i client e gli utenti possono continuare a utilizzare il servizio Single Sign-on senza alcun problema. L'obiettivo è assicurarsi di disporre di tutte le informazioni necessarie per gestire il processo di aggiornamento dei certificati in modo semplice e senza confusione.

Punti chiave da ricordare:

1. Il certificato SAML viene generato per impostazione predefinita durante l'installazione del server Cisco IdS con validità di 3 anni

2. Il certificato SAML è autofirmato

3. Il certificato SAML è un certificato SSL che risiede nel server di pubblicazione e nel sottoscrittore Cisco IDS

4. La rigenerazione del certificato SAML può essere eseguita solo nel nodo Cisco IDS Publisher

5. I tipi disponibili di algoritmo hash sicuro per il certificato SAML sono SHA-1 e SHA-256

6. L'algoritmo SHA-1 viene utilizzato con IdS 11.6 e nelle versioni precedenti viene utilizzato con IdS 12.0 e nelle versioni successive

7. Sia il provider di identità (IdP) che il servizio di identità (IdS) devono utilizzare lo stesso tipo di algoritmo.

8. Il certificato SAML Cisco IdS può essere scaricato solo dal nodo Cisco IdS Publisher (sp-<Cisco IdS_FQDN>.xml)

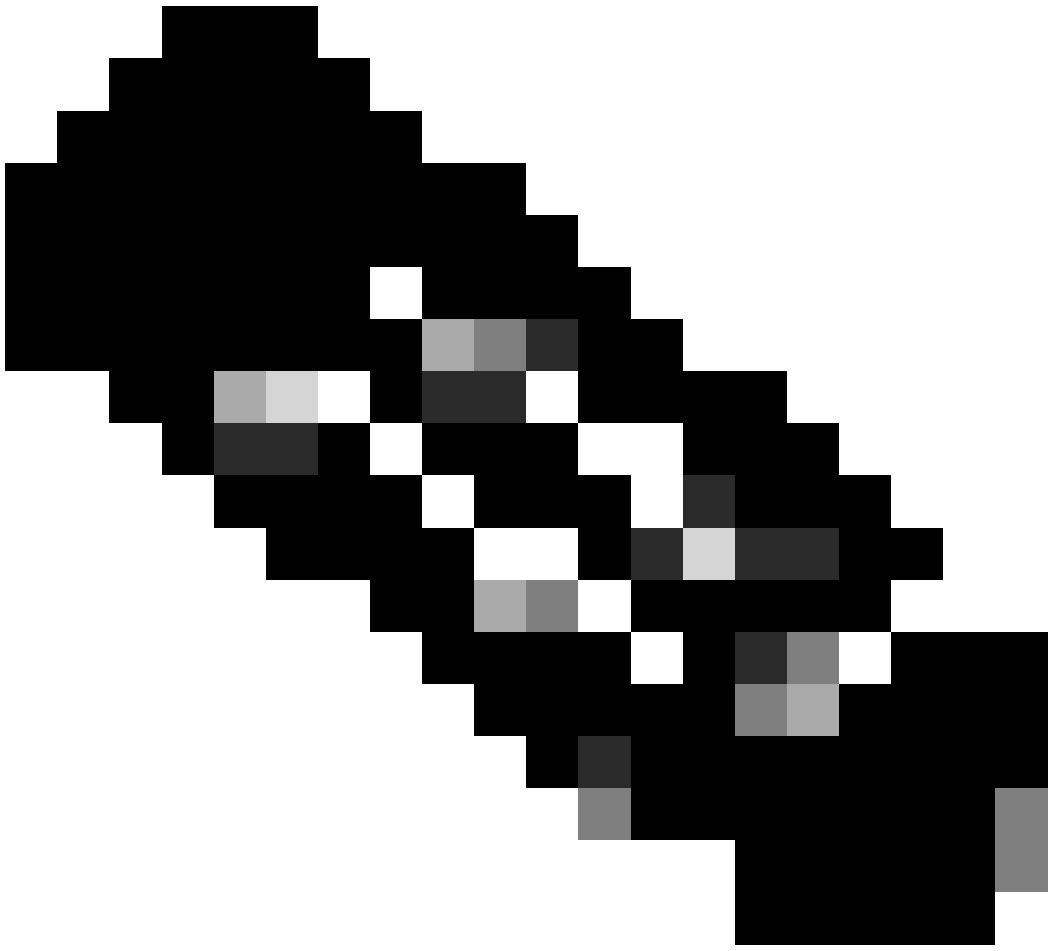
9. Vedere questo collegamento per informazioni sulla configurazione Single Sign-On UCCE/PCCE. Guida alle funzionalità di UCCE 12.6.1

Certificato SAML scaduto

Il certificato SAML è generato con validità di 3 anni (1095 giorni) ed è necessario rinnovarlo prima della scadenza. Il certificato SSL scaduto è considerato non valido e interrompe la catena di certificati tra Cisco Identity Service (IdS) e Identity Provider (IdP).

Soluzione

1. Controllare la data di scadenza del certificato SAML
2. Rigenerare il certificato SAML
3. Scaricare il file sp.xml
4. Recuperare il certificato SAML dal file sp.xml
5. Sostituire il vecchio certificato SAML con il nuovo certificato SAML nell'IdP
6. Per i passaggi dettagliati, vedere la sezione Riferimento



(Nota: {Poiché è stato modificato solo il certificato SAML, lo scambio di metadati IdS in IdP non è necessario})

Modifica dell'algoritmo hash sicuro nel provider di identità (IdP)

Si supponga che in un ambiente PCCE/UCCE esistente con Single Sign-On. Sia il server IdP che il server IdS Cisco sono stati configurati con l'algoritmo hash sicuro SHA-1. Considerata la debolezza di SHA-1 necessaria per modificare l'algoritmo hash sicuro in SHA-256.

Soluzione

1. Modificare l'algoritmo hash sicuro nel componente attendibile di AD FS (da SHA-1 a SHA-256)
2. Modificare l'algoritmo hash sicuro nell'editore IdS in Chiavi e certificato (da SHA-1 a SHA-256)
3. Rigenerare il certificato SAML nel server di pubblicazione IdS
4. Scaricare il file sp.xml
5. Recuperare il certificato SAML dal file sp.xml
6. Sostituire il vecchio certificato SAML con il nuovo certificato SAML nell'IdP
7. Per i passaggi dettagliati, vedere la sezione Riferimento

Modifica nome host o indirizzo IP server Cisco IdS - Coresidente CUIC/LiveData/IdS Publisher o Autore IdS autonomo ricostruito - Coresidente CUIC/LiveData/IdS sottoscrittore o sottoscrittore IdS autonomo ricostruito

Queste situazioni si verificano raramente ed è consigliabile ricominciare con la configurazione Single Sign-On (SSO) per garantire che la funzionalità SSO nell'ambiente di produzione venga ripristinata in modo rapido ed efficiente. È essenziale assegnare priorità a questa riconfigurazione per ridurre al minimo le interruzioni dei servizi SSO da cui dipendono gli utenti.

Soluzione

1. Eliminare il componente attendibile esistente da ADFS
2. Caricare il certificato SSL di AD FS nel server IdS Cisco per creare un trust
3. Scaricare il file sp.xml
4. Per i passaggi dettagliati, vedere la sezione di riferimento e la guida alle caratteristiche
5. Configurare la relying trust party in ADFS

6. Aggiungere le regole attestazione

7. Abilita asserzione SAML firmata

8. Scarica metadati federazione ADFS

9. Caricare i metadati federativi nel server Cisco IdS

10. Esegui test SSO

Riferimento

Come aggiungere una relying trust party in ADFS o

Come abilitare l'asserzione SAML firmata

Per i passaggi dettagliati, vedere questo documento: Guida alle caratteristiche di UCCE 12.6.1

Come caricare il certificato SSL di AD FS nell'attendibilità Cisco IdS tomcat

1. Scaricare o recuperare il certificato SSL di ADFS

2. Accedere alla pagina Cisco IdS Publisher OS Administration

3. Accedere con le credenziali dell'amministratore del sistema operativo

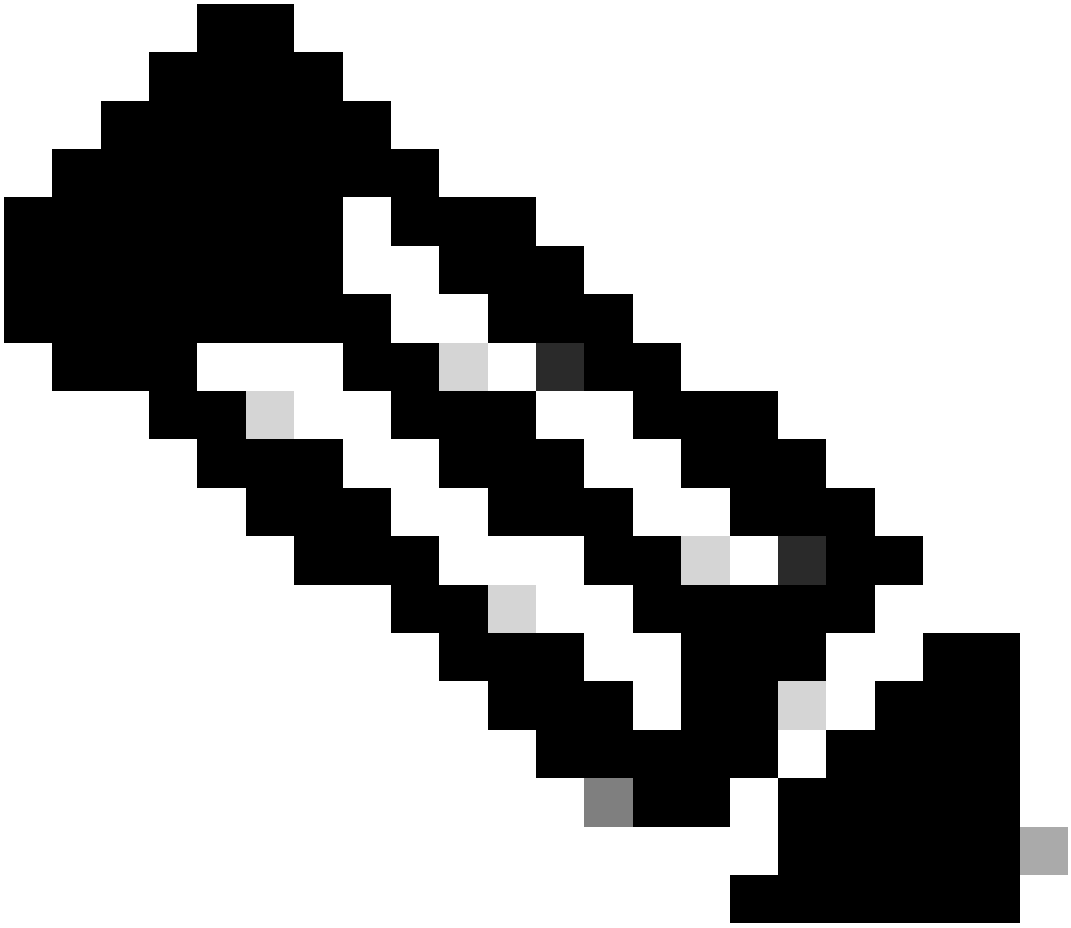
4. Passare a Sicurezza > Gestione certificati

5. Fare clic su Carica certificato/catena di certificati per aprire una finestra popup

6. Fare clic sul menu a discesa e selezionare tomcat-trust su scopo certificato

7. Fare clic su Sfoglia e selezionare il certificato SSL di ADFS

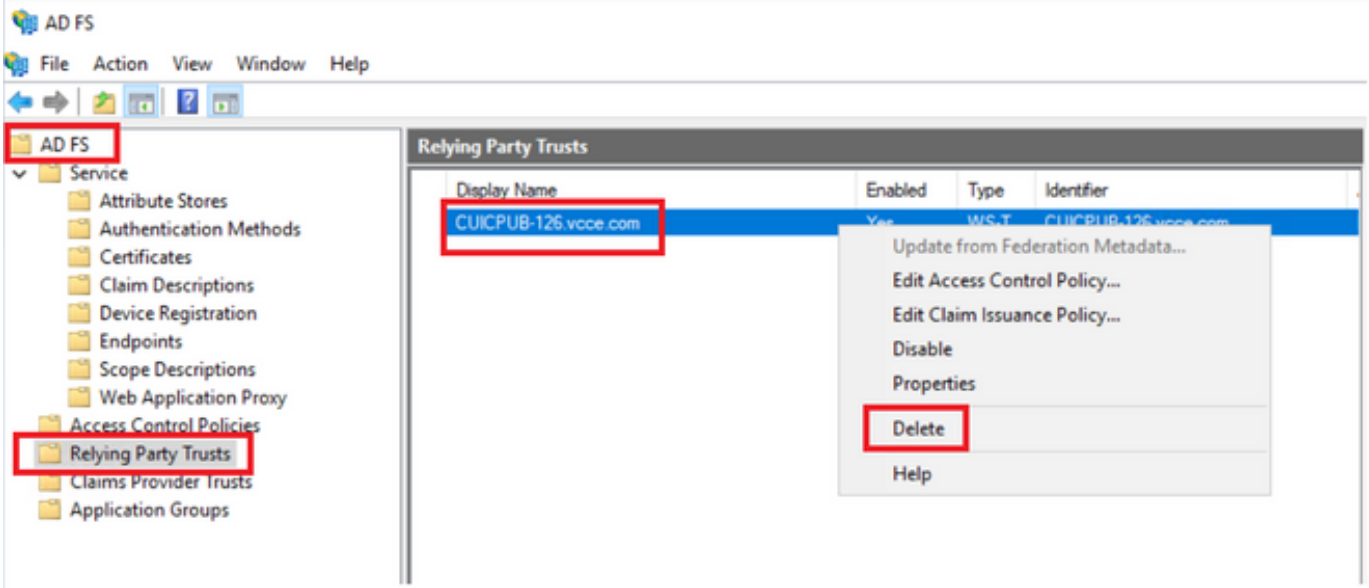
8. Fare clic su Upload



(Nota: {I certificati di attendibilità vengono replicati nei nodi del Sottoscrittore. Non è necessario eseguire il caricamento nel nodo del Sottoscrittore.})

Come eliminare il trust in ADFS

1. Accedere al server del provider di identità (IdP) con le credenziali con privilegi di amministratore
2. Aprire Server Manager e scegliere AD FS > Strumenti > Gestione AD FS
3. Nell'albero a sinistra selezionare i trust della relying party in ADFS
4. Fare clic con il pulsante destro del mouse sul server Cisco IdS e selezionare Elimina



Come controllare o modificare l'algoritmo hash sicuro configurato nel provider di identità (IdP)

1. Accedere al server del provider di identità (IdP) con le credenziali con privilegi di amministratore

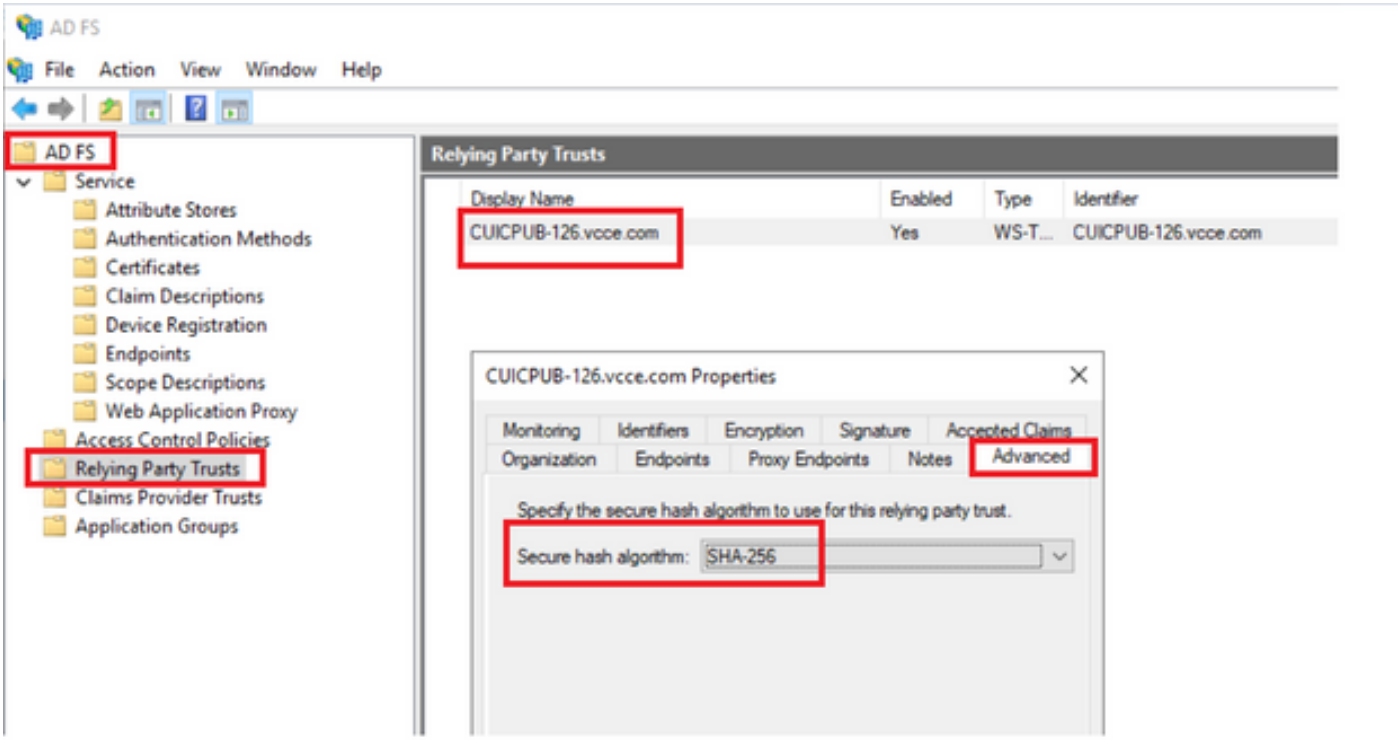
2. Aprire Server Manager e scegliere AD FS > Strumenti > Gestione AD FS

3. Nell'albero a sinistra selezionare i trust della relying party in ADFS

4. Fare clic con il pulsante destro del mouse sul server Cisco IdS e selezionare proprietà

5. Passare alla scheda Avanzate

6. L'opzione Secure Hash Algorithm consente di visualizzare l'algoritmo hash sicuro configurato nel server AD FS.



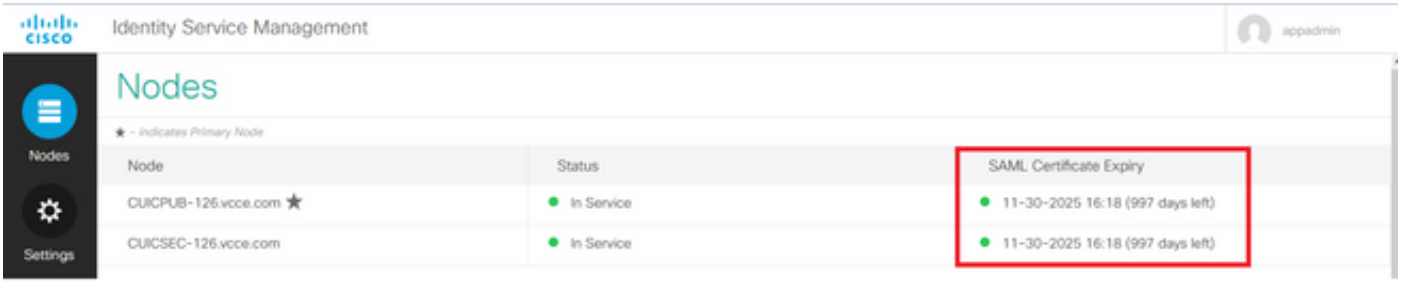
7. Fare clic sul menu a discesa e selezionare l'algoritmo hash sicuro desiderato.

Come verificare la data di scadenza del certificato SAML del server Cisco IdS

1. Accedere al server di pubblicazione o al nodo del Sottoscrittore Cisco IdS con le credenziali utente dell'applicazione

2. Dopo aver eseguito correttamente l'accesso alla pagina, accedere a Identity Service Management > Nodi

3. Visualizza il nodo Autore e Sottoscrittore di Cisco IdS, lo stato e la scadenza del certificato SAML



—

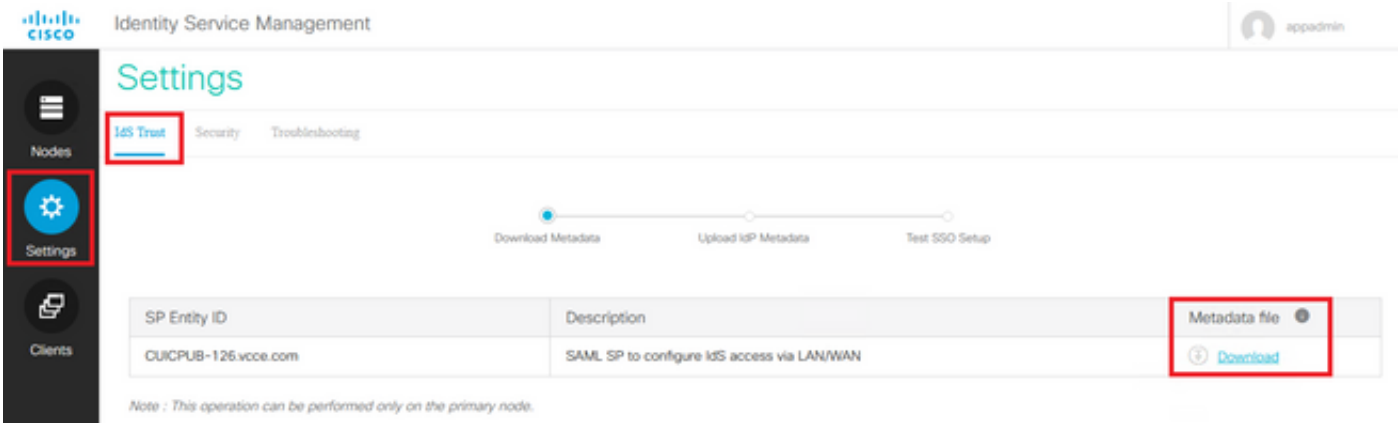
Come scaricare i metadati del server Cisco IdS

1. Accedere al nodo Cisco IdS Publisher con le credenziali utente dell'applicazione

2. Fare clic sull'icona Impostazioni

3. Passare alla scheda Trust IDS

4. Fare clic sul collegamento Download per scaricare i metadati del cluster Cisco IdS



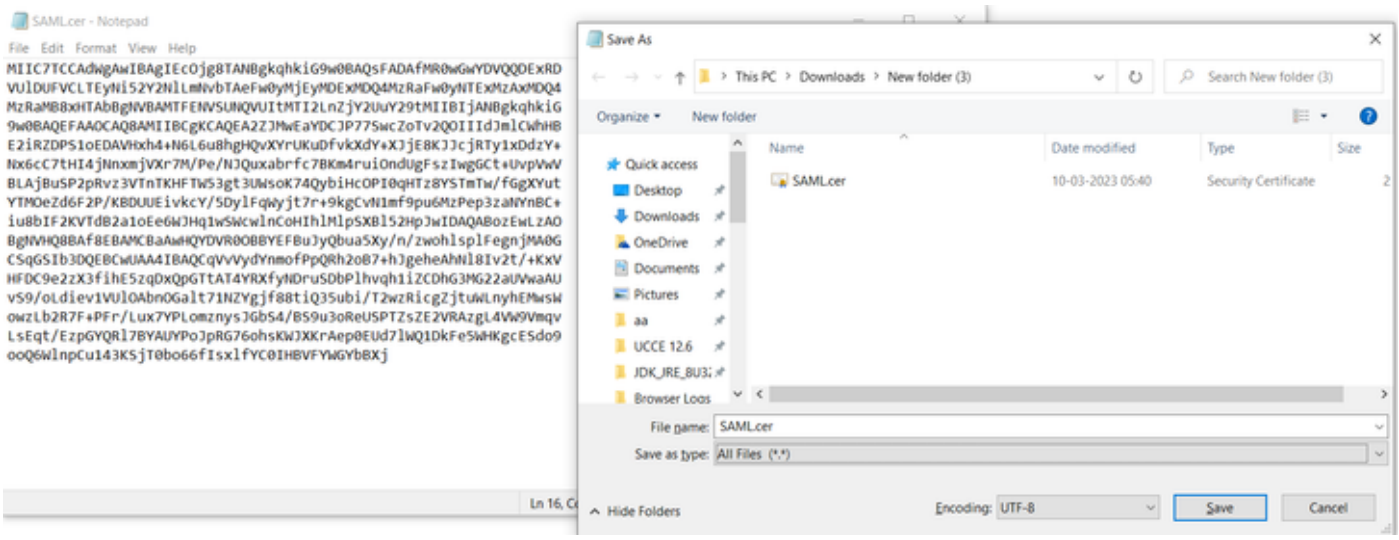
Come recuperare il certificato SAML dal file sp.xml

1. Aprire il file sp.xml con un editor di testo

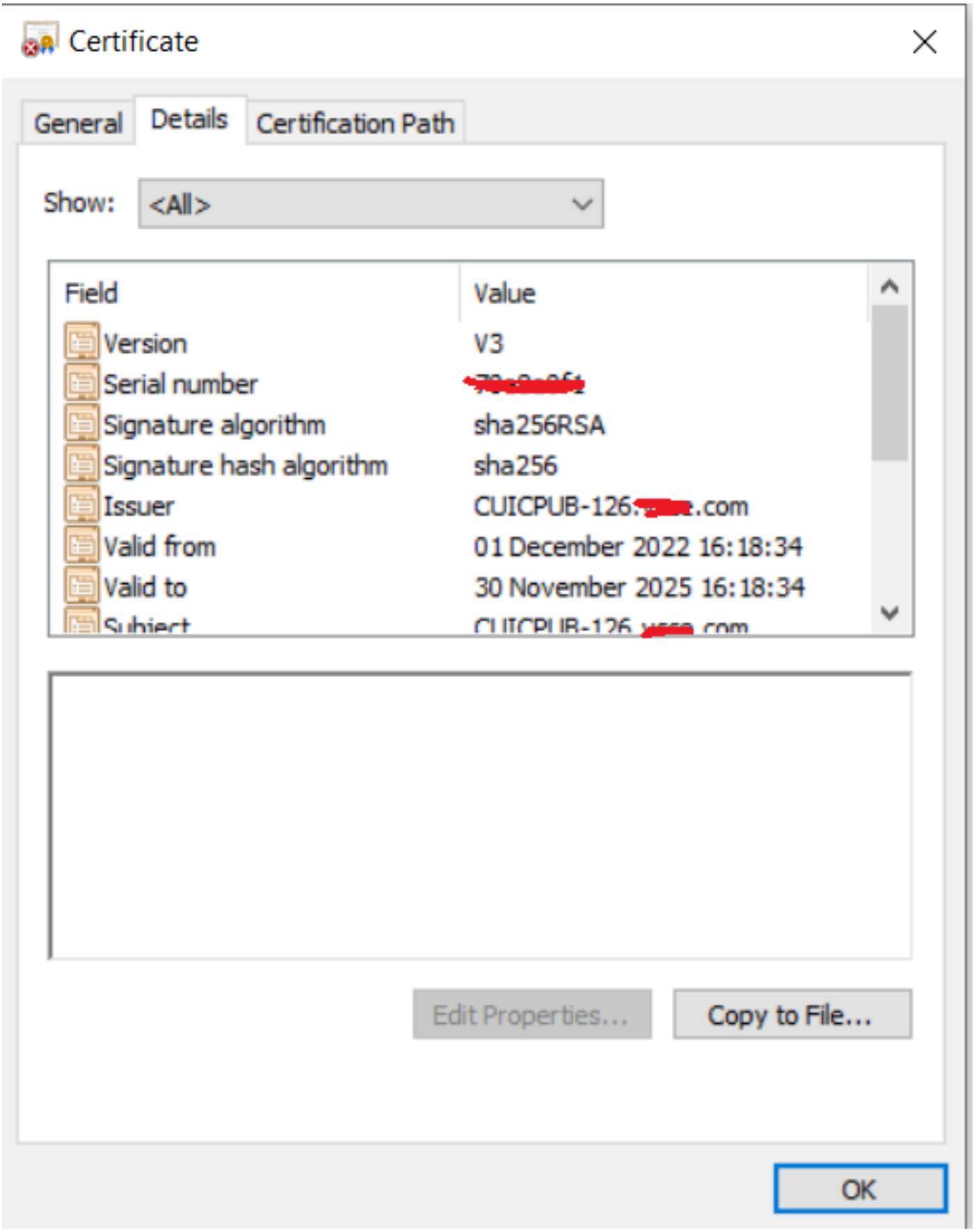
2. Copiare i dati raw tra l'intestazione <ds:X509Certificate></ds:X509Certificate>

3. Aprire un altro editor di testo e incollare i dati copiati

4. salvare il file in formato CER



5. Aprire il certificato per esaminarne le informazioni



Come sostituire il certificato SAML in ADFS

1. Copiare il file del certificato SAML nel server AD FS recuperato dal file sp.xml

2. Aprire Server Manager e scegliere AD FS > Strumenti > Gestione AD FS

3. Nell'albero a sinistra selezionare i trust della relying party in ADFS

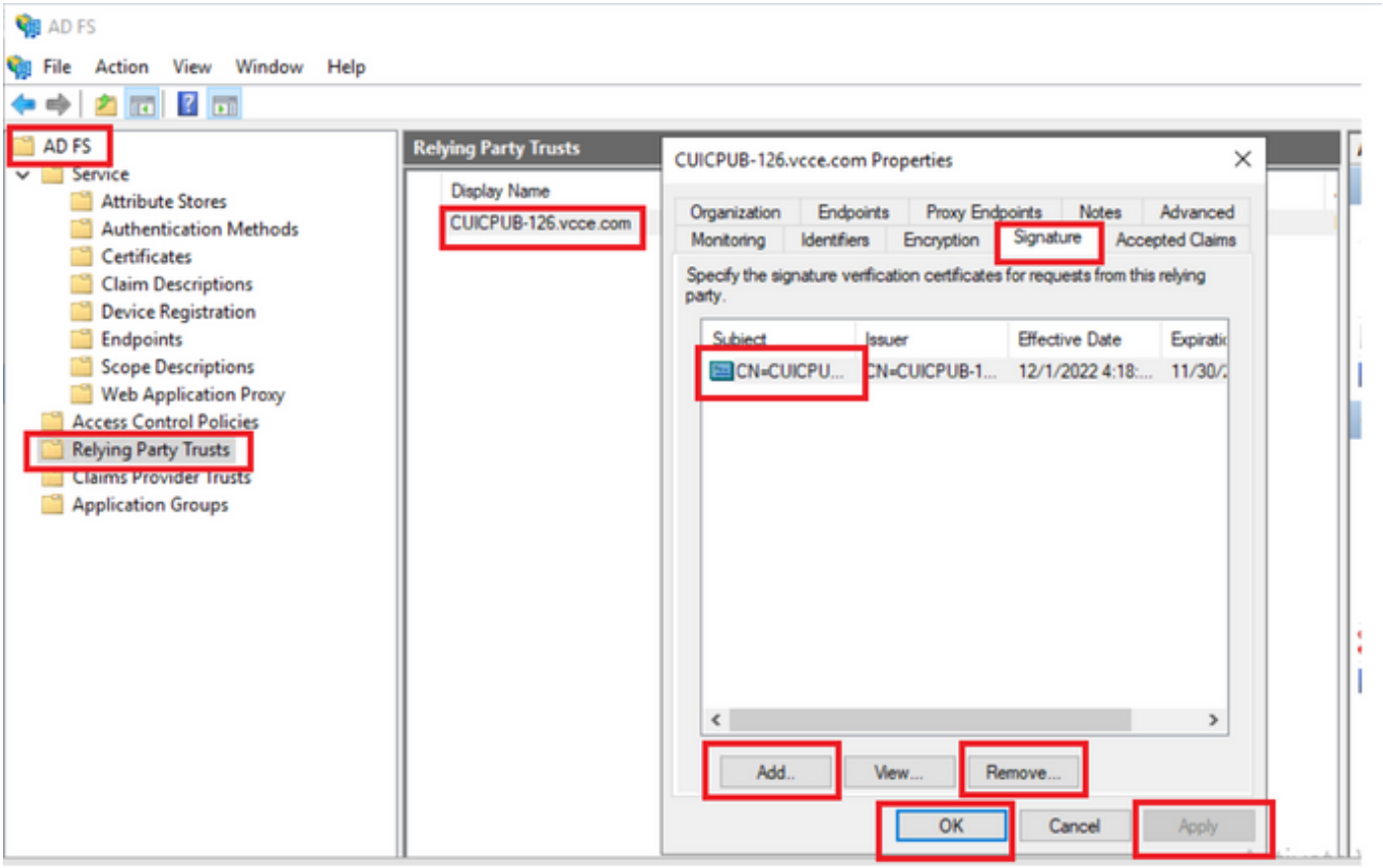
4. Fare clic con il pulsante destro del mouse sul server Cisco IdS e selezionare proprietà

5. Passare alla scheda Firma

6. Fare clic su Aggiungi e scegliere il certificato SAML appena generato

7. Selezionare il vecchio certificato SAML e fare clic su Rimuovi

8. Applicazione e salvataggio



Come rigenerare il certificato SAML nel server Cisco IdS

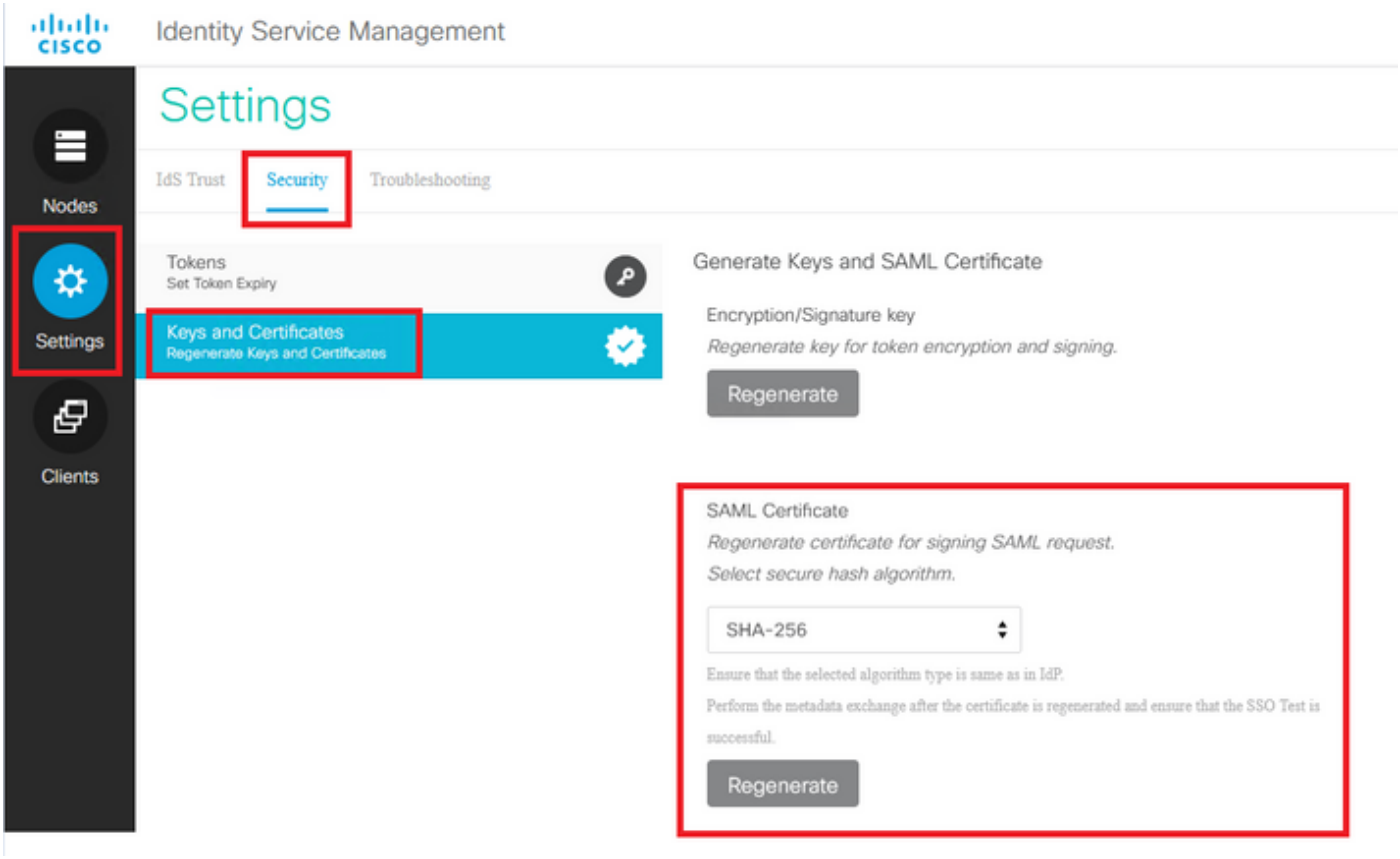
1. Accedere al nodo Cisco IdS Publisher con le credenziali utente dell'applicazione

2. Fare clic sull'icona Impostazioni

3. Passare alla scheda Protezione

4. Selezionare l'opzione Chiavi e certificati

5. fare clic sul pulsante Rigenera nella sezione del certificato SAML (evidenziato)



Test SSO

In caso di modifica del certificato SAML, accertarsi che il TEST SSO abbia esito positivo nel server Cisco IdS e registrare nuovamente tutte le applicazioni dalla pagina CEAdmin.

1. Accedere alla pagina CEAdmin dal server AW principale

2. Accedere al portale CEAdmin con i privilegi di livello admin

3. Passare a Panoramica > Funzionalità > Single Sign-On

4. Fare clic sul pulsante Registra in Registra con Cisco Identity Service

5. Esegui test SSO

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).