アイデンティティサービス(IdS)を使用したCCEシングルサインオンのトラブルシューティング：証明書管理

内容

はじめに

このドキュメントでは、UCCE/PCCEでSAML証明書を再生成および交換し、安全で明確なプロセスを実現するための詳細な手順について説明します。

著者：Cisco TACエンジニア、Nagarajan Paramasivam

前提条件

要 件

次の項目に関する知識があることが推奨されます。

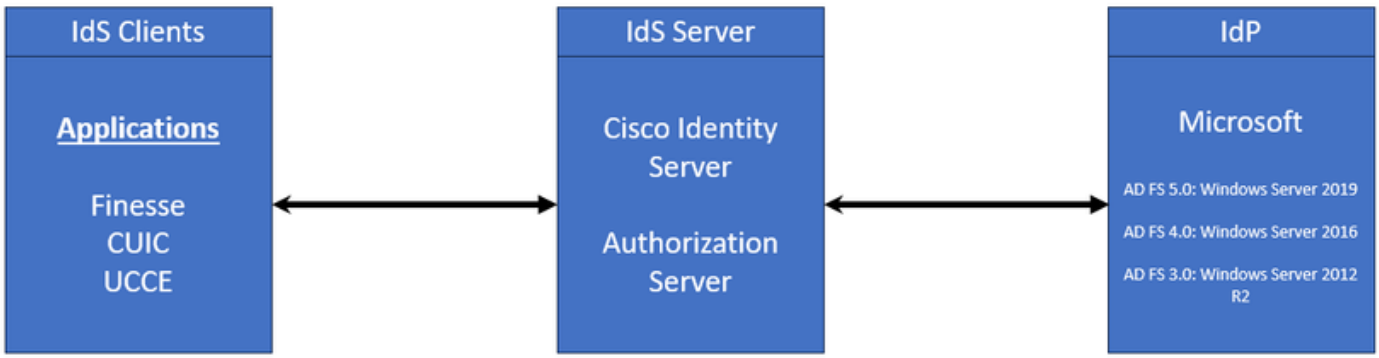
- Packaged/Unified Contact Center Enterprise(PCCE/UCCE)

- 音声オペレーティングシステム(VOS)プラットフォーム
- 証明書の管理
- Security Assertion Markup Language(SAML)
- Secure Socket Layer (SSL)
- Active Directoryフェデレーションサービス(AD FS)
- シングルサインオン(SSO)

使用するコンポーネント

このドキュメントの情報は、次のコンポーネントに基づくものです。

- シスコアイデンティティサービス(Cisco Id)
- アイデンティティプロバイダー(IdP):Microsoft Windows ADFS



このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

バックグラウンド情報

UCCE/PCCEでは、Cisco Identity Service(Cisco IdS)によって、アイデンティティプロバイダー(IdP)とアプリケーションの間の認証が提供されます。

Cisco IdSを設定するときは、Cisco IdSとIdPの間のメタデータ交換を設定します。この交換によって信頼関係が確立され、アプリケーションはSSOにCisco IdSを使用できるようになります。信頼関係を確立するには、Cisco IdSからメタデータファイルをダウンロードし、IdPにアップロードします。

SAML証明書はSSL証明書に似ており、同様に、特定の状況が発生したときに更新または変更する必要があります。Cisco Identity Services(IdS)サーバでSAML証明書を再生成またはスワップアウトすると、アイデンティティプロバイダー(IdP)との信頼できる接続が切断される可能性があります。 この中断により、シングルサインオンに依存するクライアントまたはユーザがシステムにアクセスするために必要な許可を取得できないという問題が発生する可能性があります。

このドキュメントの目的は、Cisco IdSサーバで新しいSAML証明書を作成する必要がある一般的

な状況について幅広く説明することです。また、信頼を再構築できるように、この新しい証明書をアイデンティティプロバイダー(IdP)に渡す方法についても説明します。これにより、クライアントとユーザは問題なくシングルサインオンを使用し続けることができます。目標は、証明書の更新プロセスを円滑かつ混乱なく処理するために必要なすべての情報を確実に入手することです。

覚えておくべき重要なポイント：

1. SAML証明書は、Cisco IdSサーバのインストール時にデフォルトで生成され、3年間有効です

2. SAML証明書は自己署名証明書です

3. SAML証明書は、Cisco IDSパブリッシャおよびサブスクライバ上に存在するSSL証明書です

4. SAML証明書の再生成は、Cisco IDSパブリッシャノードでのみ実行できました

5. SAML証明書に使用できるセキュアハッシュアルゴリズムの種類は、SHA-1およびSHA-256です

6. SHA-1アルゴリズムはIdS 11.6で使用され、以前のバージョンではSHA-256アルゴリズムはIdS 12.0以降のバージョンで使用されていました

7. アイデンティティプロバイダー(IdP)とアイデンティティサービス(IdS)の両方が同じアルゴリズムタイプを使用する必要があります。

8. Cisco IdS SAML証明書は、Cisco IdSパブリッシャノード(sp-<Cisco IdS_FQDN>.xml)からのみダウンロードできました

9. UCCE/PCCEシングルサインオン設定については、このリンクを参照してください。 UCCE 12.6.1機能ガイド

SAML証明書の有効期限が切れました

SAML証明書は3年（1095日）の有効期間で生成され、有効期限の前にSAML証明書を更新する必要があります。期限切れのSSL証明書は無効な証明書と見なされ、Cisco Identity Service(IdS)とIdentity Provider(IdP)間の証明書チェーンが壊れます。

ソリューション

1. SAML証明書の有効期限を確認する

2. SAML証明書の再生成

3. sp.xmlファイルをダウンロードします

4. sp.xmlファイルからSAML証明書を取得します

5. IdPで古いSAML証明書を新しいSAML証明書に置き換える

6. 詳細な手順については、「参考資料」のセクションを参照してください

(注:{SAML証明書のみが変更されたため、IdPへのIdSメタデータ交換は必要ありません})

アイデンティティプロバイダー(IdP)でのセキュアハッシュアルゴリズムの変更

シングルサインオンを使用する既存のPCCE/UCCE環境で想定します。IdPサーバとCisco IdSサーバの両方にSHA-1セキュアハッシュアルゴリズムが設定されています。セキュアハッシュアルゴリズムをSHA-256に変更するために必要なSHA-1の弱点を考慮します。

ソリューション

1. AD FS証明書利用者信頼パーティのセキュアハッシュアルゴリズムを変更する（SHA-1からSHA-256）

2. [キーと証明書]のIdS発行元のセキュアハッシュアルゴリズムを変更します（SHA-1からSHA-256）

3. IdSパブリッシャでSAML証明書を再生成する

4. sp.xmlファイルをダウンロードします

5. sp.xmlファイルからSAML証明書を取得します

6. IdPで古いSAML証明書を新しいSAML証明書に置き換える

7. 詳細な手順については、「参考資料」のセクションを参照してください

Cisco IdSサーバのIPアドレスまたはホスト名の変更 – 共存CUIC/LiveData/IdSパブリッシャまたはスタンドアロンIdSパブリッシャの再構築 – 共存CUIC/LiveData/IdSサブスクライバまたはスタンドアロンIdSサブスクライバの再構築

このような状況はめったに発生しません。実稼働環境でSSO機能が迅速かつ効率的に復元されるように、シングルサインオン(SSO)セットアップを新たに開始することを強くお勧めします。ユーザが依存するSSOサービスの中断を最小限に抑えるには、この再設定を優先させることが重要です。

ソリューション

1. AD FSから既存の証明書利用者を削除します

2. AD FS SSL証明書をCisco IdSサーバのtomcat信頼にアップロードする

3. sp.xmlファイルをダウンロードします

4. 詳細な手順については、「リファレンス」セクションと「機能ガイド」を参照してください

5. AD FSで証明書利用者を構成する

6. クレームルールの追加

7. 署名付きSAMLアサーションの有効化

8. AD FSフェデレーションメタデータのダウンロード

9. Cisco IdSサーバへのフェデレーションメタデータのアップロード

10. テストSSOの実行

参考

ADFSに証明書利用者を追加する方法

署名付きSAMLアサーションを有効にする方法

詳細な手順については、次のドキュメントを参照してください。UCCE 12.6.1機能ガイド

AD FS SSL証明書をCisco IdS tomcat信頼にアップロードする方法

1. AD FS SSL証明書をダウンロードまたは取得する

2. Cisco IdS Publisher OS Administrationページにアクセスします

3. OS管理者クレデンシャルでログインします。

4. [セキュリティ] > [証明書管理]に移動します

5. [証明書/証明書チェーンのアップロード]をクリックすると、ポップアップウィンドウが開きます

6. ドロップダウンメニューをクリックして、証明書の目的でtomcat-trustを選択します。

7. [参照]をクリックし、AD FS SSL証明書を選択します

8. 「アップロード」をクリックします

(注:{信頼証明書はサブスクライバノードに複製されます。サブスクライバノードにアップロードする必要はありません。})

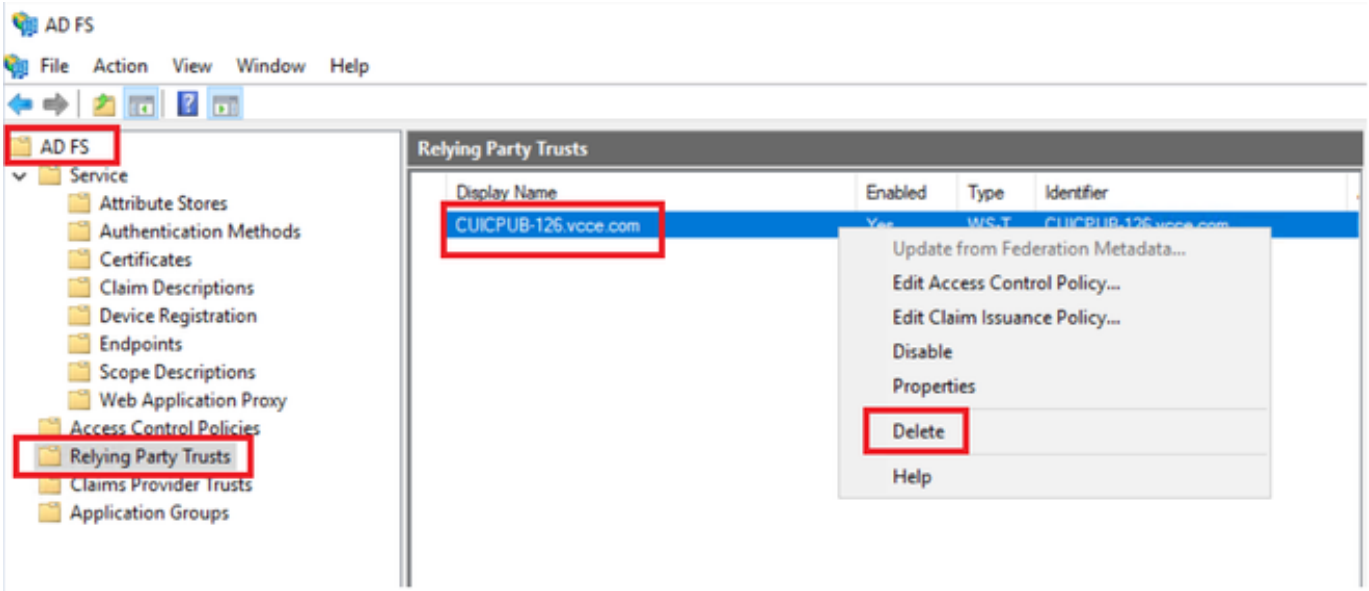
AD FSで証明書利用者信頼を削除する方法

1. 管理者の特権を持つ資格情報を使用して、アイデンティティプロバイダー(IdP)サーバーにログインします

2. サーバーマネージャーを開き、[AD FS] > [ツール] > [AD FS管理]を選択します

3. 左側のツリーで、AD FSの下にある証明書利用者信頼を選択します

4. Cisco IdSサーバを右クリックし、Deleteを選択します



アイデンティティプロバイダー(IdP)で設定されているセキュアハッシュアルゴリズムを確認または変更する方法

1. 管理者の特権を持つ資格情報を使用して、アイデンティティプロバイダー(IdP)サーバーにログインします

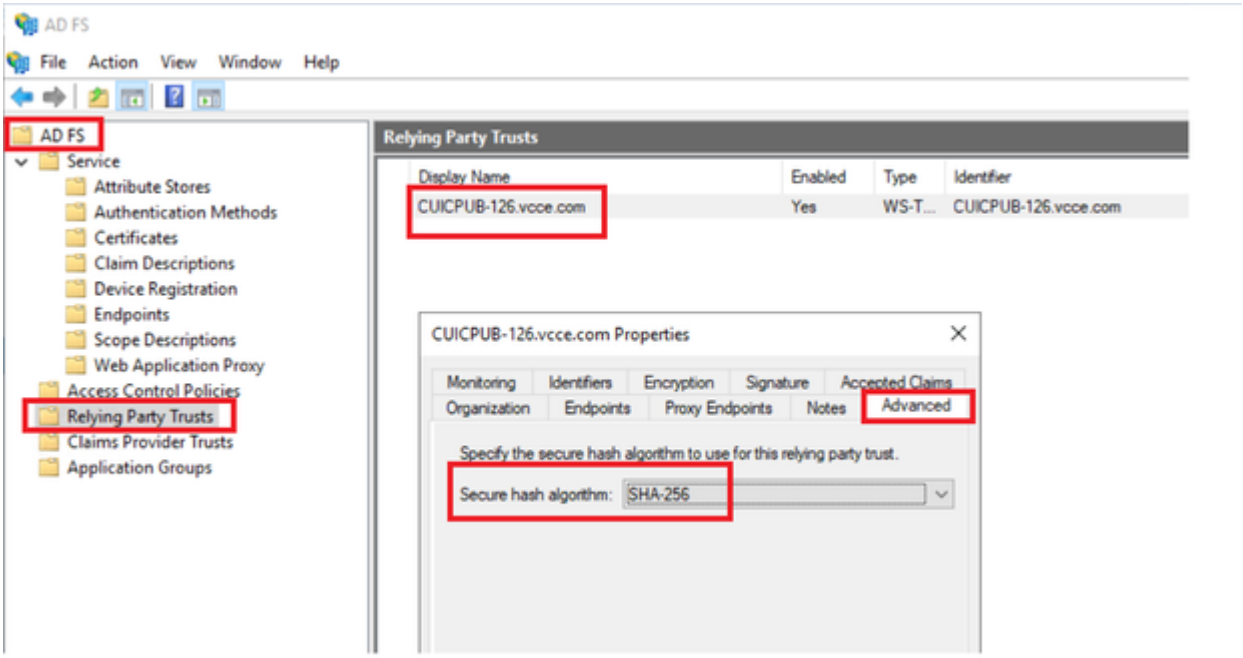
2. サーバーマネージャーを開き、[AD FS] > [ツール] > [AD FS管理]を選択します

3. 左側のツリーで、AD FSの下にある証明書利用者信頼を選択します

4. Cisco IdSサーバを右クリックし、Propertiesを選択します

5. 「拡張」タブにナビゲートします

6. [Secure Hash Algorithm]オプションは、AD FSサーバーで構成されているセキュアハッシュアルゴリズムを表示します。



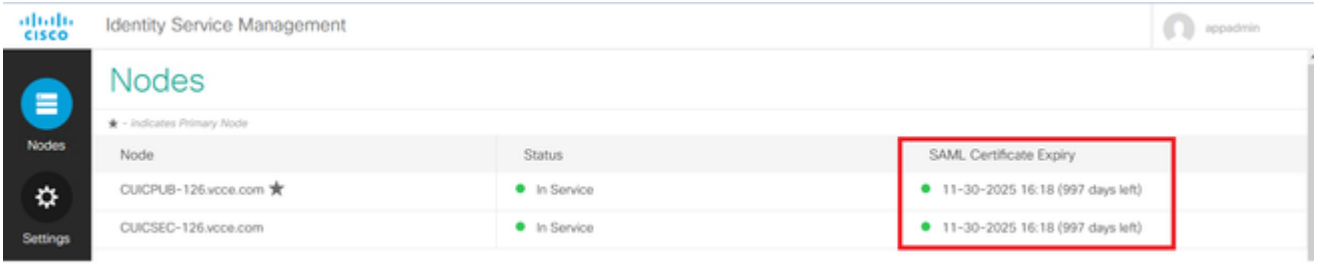
7. ドロップダウンメニューをクリックして、目的のセキュアハッシュアルゴリズムを選択します。

Cisco IdSサーバのSAML証明書の有効期限を確認する方法

1. アプリケーションユーザクレデンシャルを使用して、Cisco IdSサーバのパブリッシャまたはサブスクライバノードにログインします

2. 正常にログインすると、ページが[アイデンティティサービス管理] > [ノード]に移動します

3. Cisco IdSパブリッシャおよびサブスクライバノード、ステータス、およびSAML証明書の有効期限が表示されます。



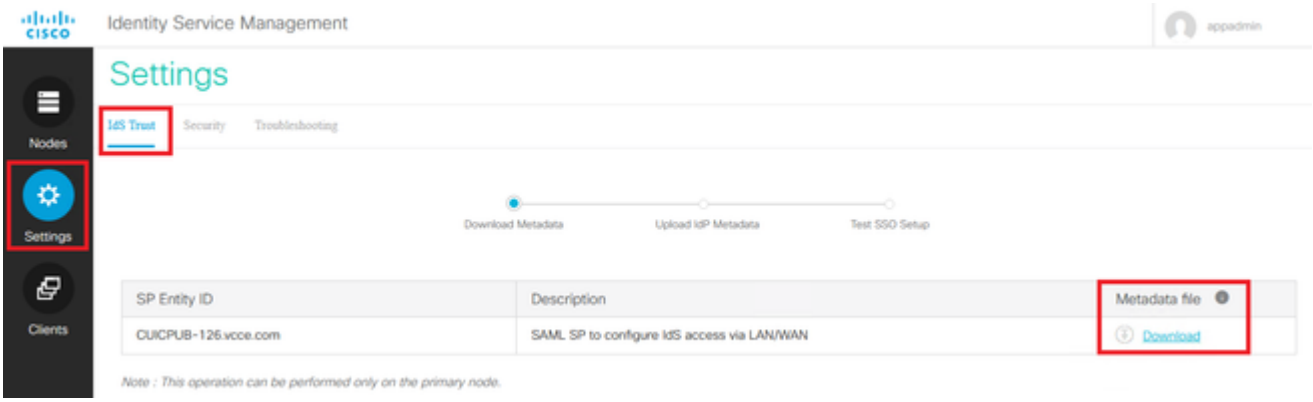
Cisco IdSサーバのメタデータをダウンロードする方法

1. アプリケーションユーザクレデンシャルを使用して、Cisco IdSパブリッシャノードにログインします

2. [設定]アイコンをクリックします。

3. 「IDS信頼」タブにナビゲートします

4. [ダウンロード]リンクをクリックして、Cisco IdSクラスタのメタデータをダウンロードします



sp.xmlファイルからのSAML証明書の取得方法

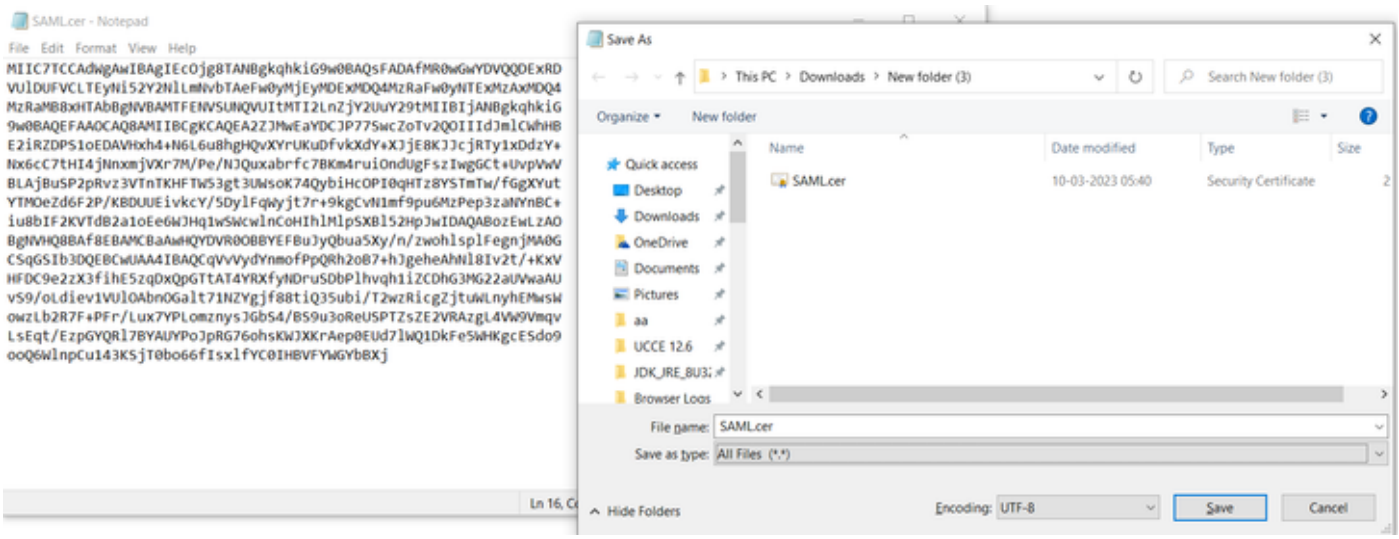
1. テキストエディタでsp.xmlファイルを開きます

2. ヘッダー<ds:X509Certificate></ds:X509Certificate>間で未加工データをコピーします

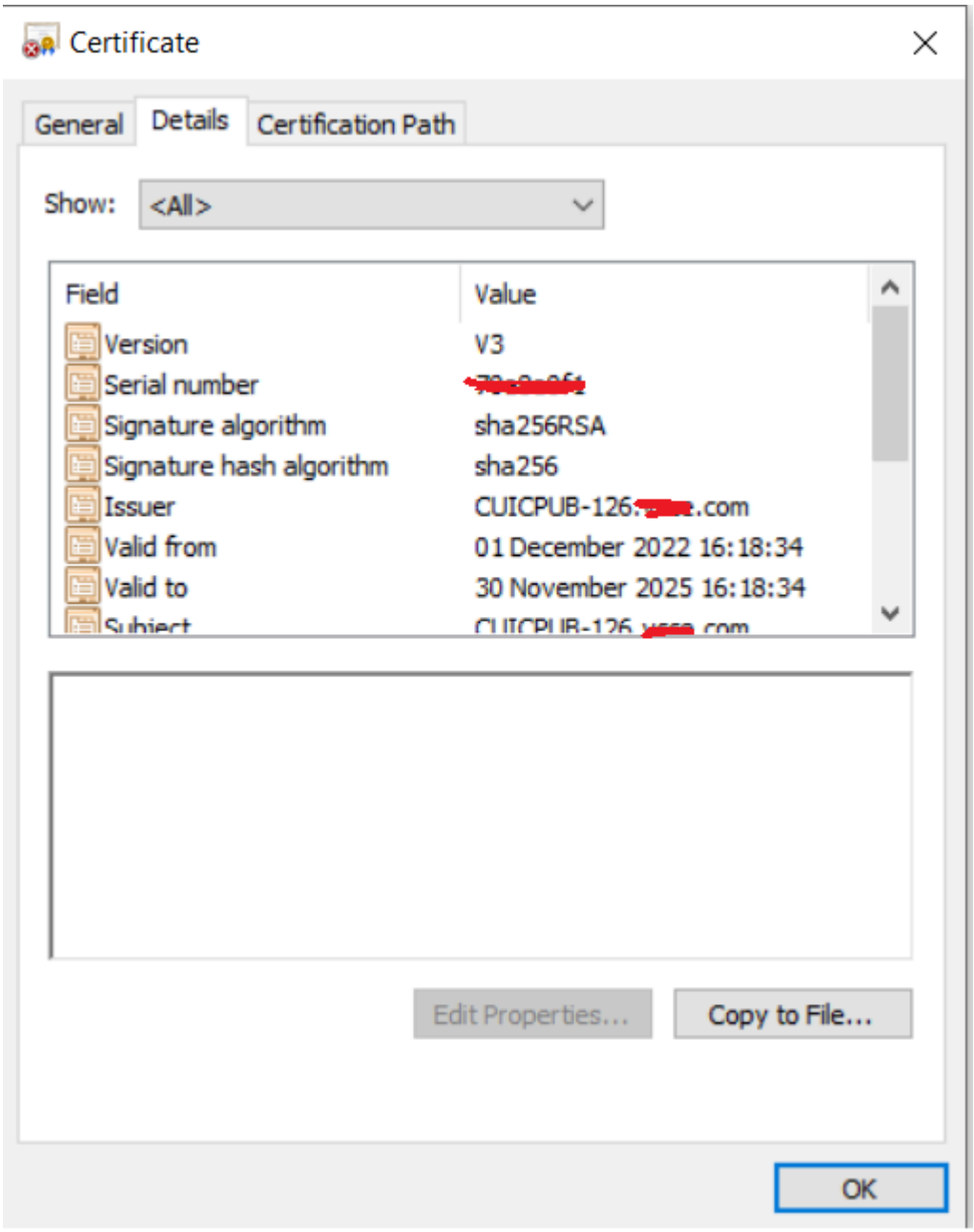
```
<ds:X509Certificate>MIIC7TCCAdWgAwIBAgIEcOjg8TANBgkqhkiG9w0BAQsFADAfMR0wGwYDVQQDExRD
VUlDUFVCLTEyNi52Y2NlLmNvbTAeFw0yMjEyMDExMDQ4MzRaFw0yNTExMzAxMDQ4
MzRaMB8xHTAbBgNVBAMTFENVSUNQVUItMTI2LnZjY2UuY29tMIIBIjANBgkqhkiG
9w0BAQEFAAOCAQ8AMIIBCgKCAQEA2ZJMwEaYDCJP77SwcZoTv2QOIIIdJmlCWhHB
E2iRZDPS1oEDAVHxh4+N6L6u8hgHQvXYrUKuDfvkXdY+XJjE8KJJcjRTy1xDdzY+
Nx6cC7tHI4jNnxmjVXr7M/Pe/NJQuxabrfc7BKm4ruiOndUgFszIwgGCt+UvpVwV
BLAjBuSP2pRvz3VTnTKHFTW53gt3UWsoK74QybiHcOPI0qHTz8YSTmTw/fGgXYut
YTMOeZd6F2P/KBDUUEivkcY/5DylFqWyjt7r+9kgCvN1mf9pu6MzPep3zaNYnBC+
iu8bIF2KVTdB2a1oEe6WJHq1wSWcwlnCoHIhlMlpSXBl52HpJwIDAQABozEwLzAO
BgNVHQ8BAf8EBAMCBaAwHQYDVR0OBBYEFBuJyQbua5Xy/n/zwohlsplFegnjMA0G
CSqGSIb3DQEBCwUAA4IBAQCqVvVydYnmofPpQRh2oB7+hJgeheAhNl8Iv2t/+KxV
HFDC9e2zX3fihE5zqDxQpGTtAT4YRXfyNDruSDbPlhvqh1iZCDhG3MG22aUVwaAU
vS9/oLdiev1VUlOAbnOGalt71NZYgjf88tiQ35ubi/T2wzRicgZjtuWLnyhEMwsW
owzLb2R7F+PFr/Lux7YPLomznysJGbS4/BS9u3oReUSPTZsZE2VRAzgL4VW9Vmqv
LsEqt/EzpGYQRl7BYAUYPoJpRG76ohsKWJXKrAep0EUd71WQ1DkFe5WHKgcESdo9
ooQ6WlnpCu143KSjT0bo66fIsxlfYC0IHBVFYWGYbBXj</ds:X509Certificate>
```

3. 別のテキストエディタを開き、コピーしたデータを貼り付けます

4. .CERファイル形式で保存します。



5. 証明書を開いて証明書情報を確認します



AD FSでSAML証明書を置き換える方法

1. sp.xmlから取得したSAML証明書ファイルをAD FSサーバーにコピーします

2. サーバーマネージャーを開き、[AD FS] > [ツール] > [AD FS管理]を選択します

3. 左側のツリーで、AD FSの下にある証明書利用者信頼を選択します

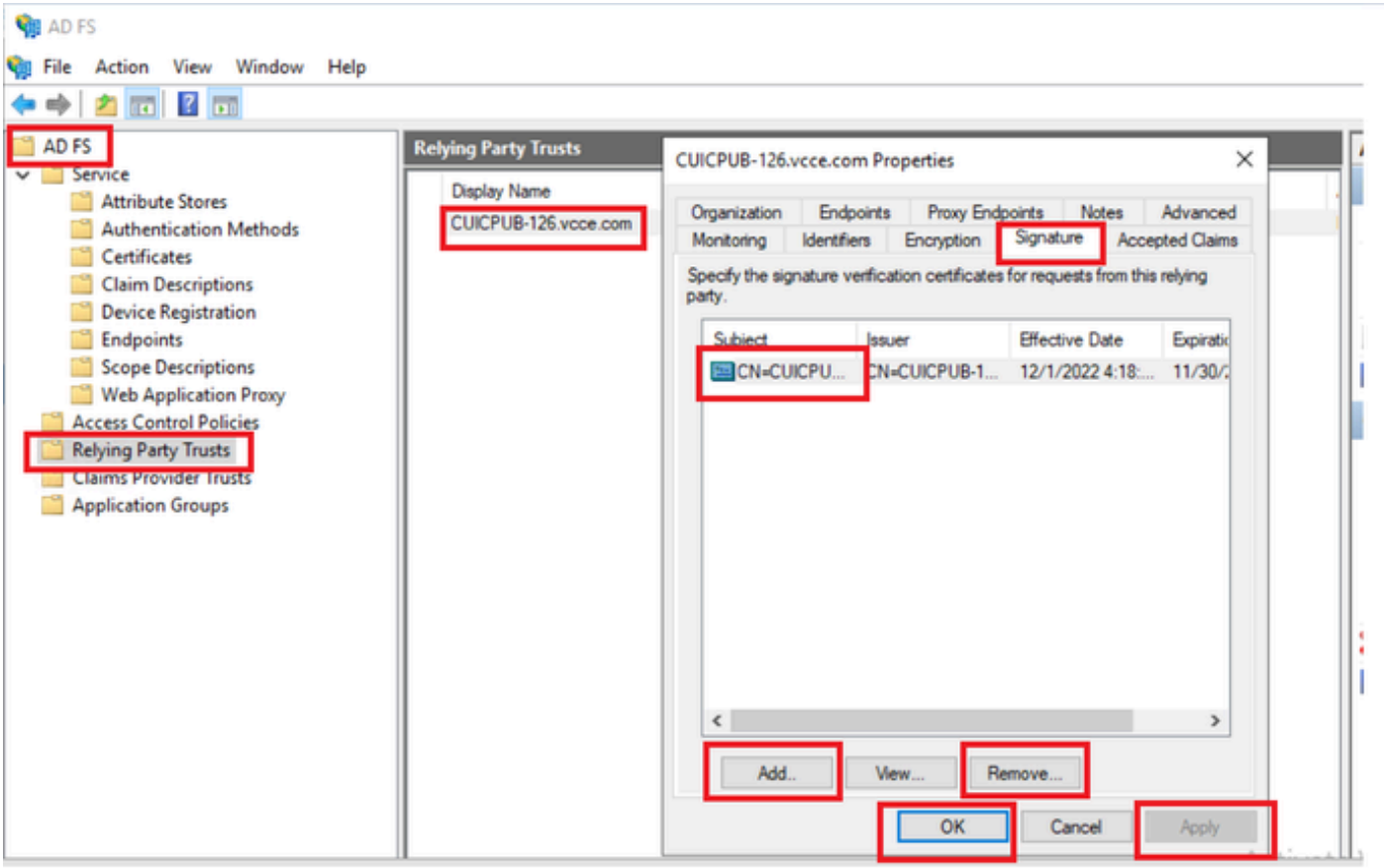
4. Cisco IdSサーバを右クリックし、Propertiesを選択します

5. 「署名」タブにナビゲートします

6. [追加]をクリックし、新しく生成されたSAML証明書を選択します

7. 古いSAML証明書を選択し、「削除」をクリックします

8. 適用して保存



Cisco IdSサーバでのSAML証明書の再生方法

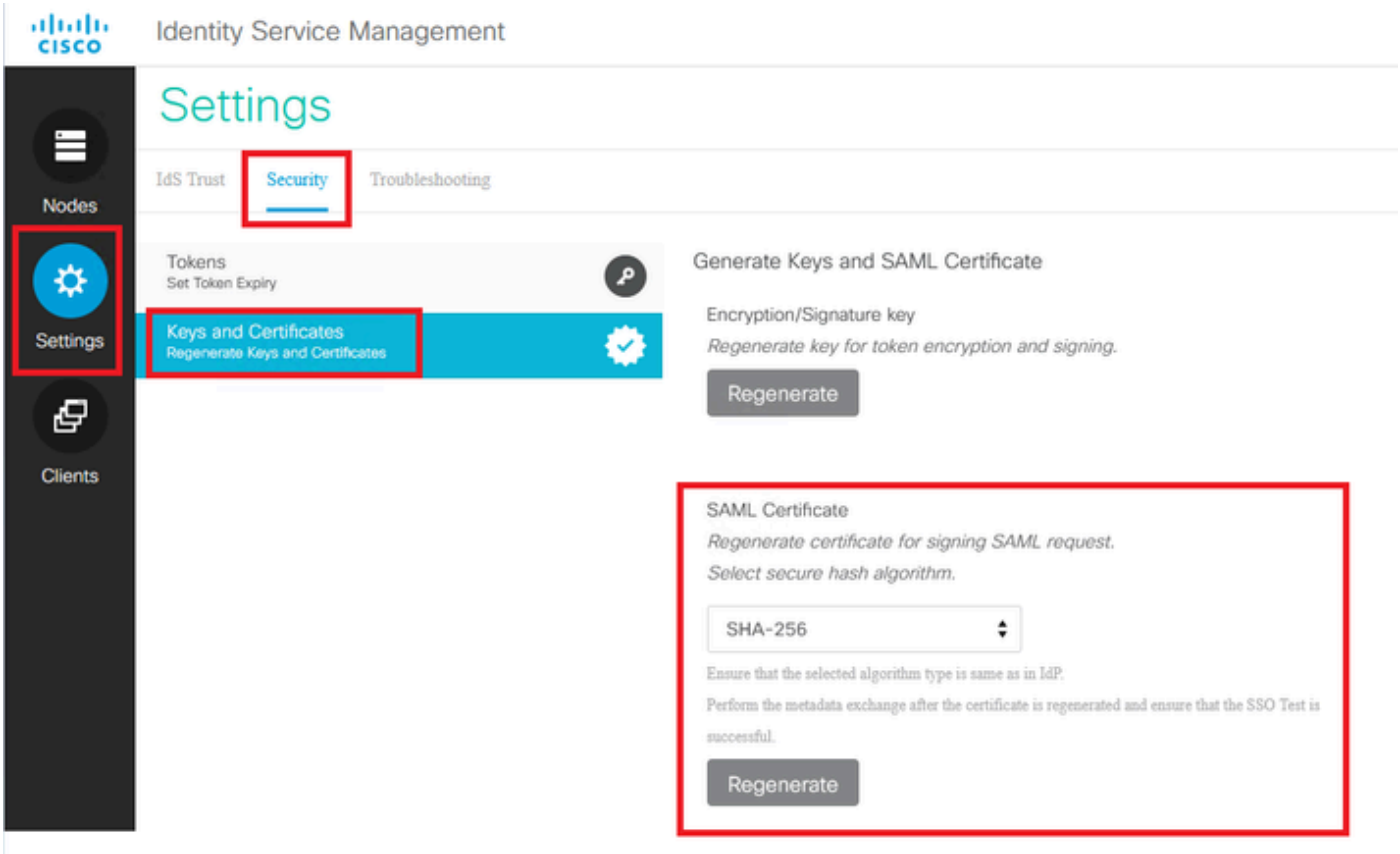
1. アプリケーションユーザクレデンシャルを使用して、Cisco IdSパブリッシャノードにログインします

2. [設定]アイコンをクリックします。

3. 「セキュリティ」タブにナビゲートします

4. [キーと証明書]オプションを選択します

5. SAML証明書セクション（強調表示）の下の「再生成」ボタンをクリックします。



SSOのテスト

SAML証明書に変更がある場合は常に、Cisco IdSサーバでTEST SSOが正常に実行されていることを確認し、CCEAdminページからすべてのアプリケーションを再登録してください。

1. プリンシパルAWサーバからCCEAdminページにアクセスします

2. adminレベルの権限でCCEAdminポータルにログインします。

3. [概要] > [機能] > [シングルサインオン]に移動します

4. Register with Cisco Identity Serviceの下にあるRegisterボタンをクリックします

5. テストSSOの実行

Azure証明書の再生成

1. IDSから証明書を再生成します。パブリッシャでのみ行います。パブリッシャとサブスクライバの両方で証明書が自動生成されます。
2. IDSからメタデータをダウンロードし、IDP/Azureにアップロードする
3. IDP/Azureから証明書を更新します。これにより、Azureからメタデータが完全に変更され、Microsoft Azureから署名され、.pfxのニーズが解決されます
4. IDP/AzureからCisco IDSにメタデータをアップロードします（パブリッシャのみ）
5. IDSからのSSOのテスト

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。