Fehlerbehebung: CCE-einmalige Anmeldung mit Identity Service (IDs)-Zertifikatsverwaltung

Inhalt

Einleitung

In diesem Dokument werden detaillierte Schritte zum Regenerieren und Austauschen von SAML-Zertifikaten in UCCE/PCCE beschrieben, um sichere und klare Prozesse zu gewährleisten.

Beitrag von Nagarajan Paramasivam, Cisco TAC Engineer.

Voraussetzungen

Anforderungen

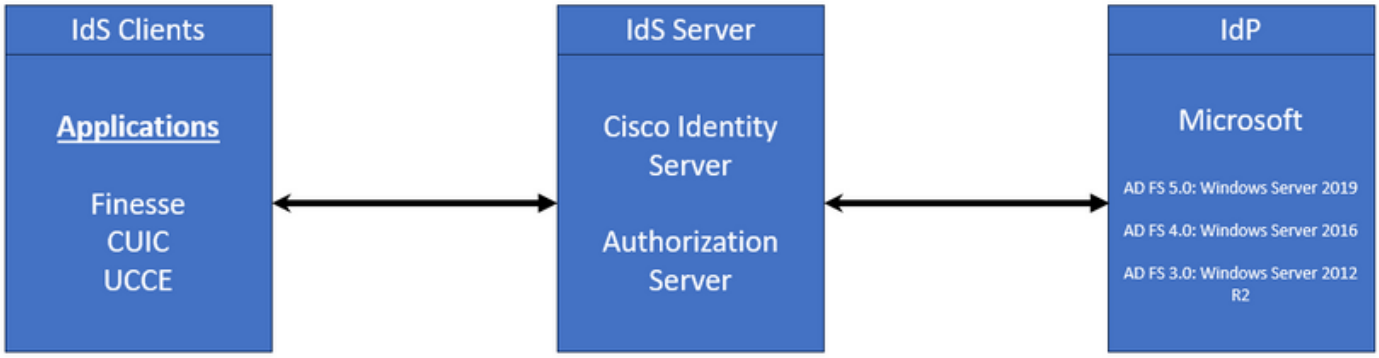
Cisco empfiehlt, dass Sie folgende Themen kennen:

- Packaged/Unified Contact Center Enterprise (PCCE/UCCE)
- Voice Operating System (VOS)-Plattform
- Zertifikatsverwaltung
- Security Assertion Markup Language (SAML)
- Secure Sockets Layer (SSL)
- Active Directory-Verbunddienste (AD FS)
- Single Sign-On (SSO)

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf folgenden Komponenten:

- Cisco Identity Service (Cisco IDs)
- Identity Provider (IdP) - Microsoft Windows ADFS



Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

In UCCE/PCCE stellt der Cisco Identity Service (Cisco IdS) die Autorisierung zwischen dem Identity Provider (IdP) und den Anwendungen bereit.

Wenn Sie die Cisco IDs konfigurieren, richten Sie einen Metadatenaustausch zwischen der Cisco IDs und der IdP ein. Dieser Austausch stellt eine Vertrauensstellung her, die es Anwendungen ermöglicht, die Cisco IDs für SSO zu verwenden. Sie stellen die Vertrauensbeziehung her, indem Sie eine Metadatendatei aus der Cisco IDs herunterladen und in die IdP hochladen.

Das SAML-Zertifikat ähnelt einem SSL-Zertifikat und muss ebenso aktualisiert oder geändert werden, wenn bestimmte Situationen eintreten. Wenn Sie das SAML-Zertifikat auf dem Cisco Identity Services (IdS)-Server neu generieren oder austauschen, kann dies zu einer Unterbrechung der vertrauenswürdigen Verbindung mit dem Identity Provider (IdP) führen. Diese Pause kann zu Problemen führen, wenn Clients oder Benutzer, die sich auf Single Sign-On verlassen, nicht die nötige Autorisierung erhalten, um auf das System zuzugreifen.

Dieses Dokument behandelt eine Vielzahl gängiger Situationen, in denen Sie ein neues SAML-Zertifikat auf dem Cisco IdS-Server erstellen müssen. Außerdem wird erläutert, wie das neue Zertifikat an den Identitätsanbieter (IdP) weitergegeben wird, damit die Vertrauensstellung wiederhergestellt werden kann. Dadurch können Clients und Benutzer Single Sign-On ohne Probleme weiterhin verwenden. Das Ziel ist es, sicherzustellen, dass Sie über alle Informationen verfügen, die Sie benötigen, um den Aktualisierungsprozess für Zertifikate reibungslos und ohne Verwirrung durchführen zu können.

Wichtige Punkte:

1. SAML-Zertifikat wird standardmäßig während der Cisco IdS-Serverinstallation mit einer Gültigkeitsdauer von 3 Jahren generiert

2. SAML-Zertifikat ist ein selbstsigniertes Zertifikat

3. SAML-Zertifikat ist ein SSL-Zertifikat, das sich auf dem Cisco IDS-Publisher und -Subscriber befindet.

4. Die SAML-Zertifikatregeneration konnte nur im Cisco IDS Publisher-Knoten durchgeführt werden.

5. Die verfügbaren Typen des sicheren Hashalgorithmus für das SAML-Zertifikat sind SHA-1 und SHA-256

6. SHA-1 Algorithmus wird auf IdS 11.6 und in früheren Versionen, der SHA-256 Algorithmus wird auf IdS 12.0 und in späteren Versionen verwendet

7. Identitätsanbieter (IdP) und Identitätsdienst (IdS) müssen denselben Algorithmustyp verwenden.

8. Das Cisco IdS SAML-Zertifikat konnte nur vom Cisco IdS Publisher-Knoten (sp-<Cisco IdS_FQDN>.xml) heruntergeladen werden.

9. Unter diesem Link finden Sie Informationen zur UCCE/PCCE-Konfiguration für einmalige Anmeldung. UCCE 12.6.1 - Funktionsleitfaden

SAML-Zertifikat abgelaufen

Das SAML-Zertifikat wird mit einer Gültigkeitsdauer von 3 Jahren (1095 Tage) generiert und muss

vor Ablauf des Zertifikats erneuert werden. Das abgelaufene SSL-Zertifikat gilt als ungültig und unterbricht die Zertifikatskette zwischen dem Cisco Identity Service (IdS) und dem Identity Provider (IdP).

Lösung

1. Überprüfen Sie das Ablaufdatum des SAML-Zertifikats.

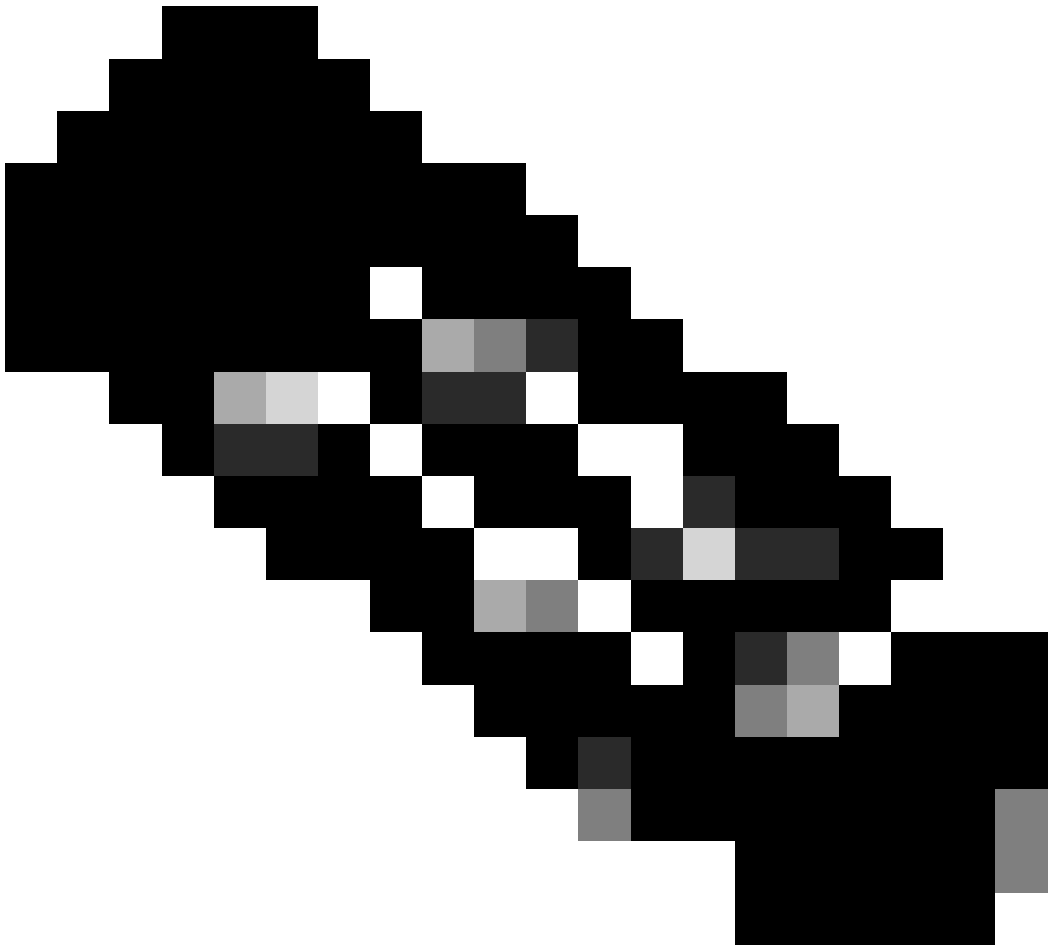
2. SAML-Zertifikat neu generieren

3. Laden Sie die sp.xml-Datei herunter.

4. SAML-Zertifikat aus der sp.xml-Datei abrufen

5. Ersetzen Sie das alte SAML-Zertifikat durch das neue SAML-Zertifikat in der IdP

6. Ausführliche Informationen hierzu finden Sie im Referenzabschnitt.



(Hinweis: {Da nur das SAML-Zertifikat geändert wurde, ist kein Austausch von IdS-Metadaten mit IdP erforderlich})

Änderung des sicheren Hash-Algorithmus im Identitätsanbieter (IdP)

Beispiel: in einer vorhandenen PCCE/UCCE-Umgebung mit Single-Sign-On. Für den IdP- und den Cisco IdS-Server wurde der sichere SHA-1-Hash-Algorithmus konfiguriert. In Anbetracht der Schwäche des SHA-1, die erforderlich ist, um den sicheren Hash-Algorithmus in SHA-256 zu ändern.

Lösung

1. Ändern Sie den Secure Hash-Algorithmus in der AD FS Relying Trust Party (SHA-1 zu SHA-256).

2. Ändern Sie den sicheren Hash-Algorithmus im IdS-Publisher unter Schlüssel und Zertifikat (SHA-1 in SHA-256).

3. Regenerieren Sie das SAML-Zertifikat im IdS-Publisher.

4. Laden Sie die sp.xml-Datei herunter.

5. SAML-Zertifikat aus der sp.xml-Datei abrufen

6. Ersetzen Sie das alte SAML-Zertifikat durch das neue SAML-Zertifikat in der IdP

7. Ausführliche Informationen hierzu finden Sie im Referenzabschnitt.

Cisco IdS-Server-IP-Adresse oder Hostnamensänderung - Neuaufbau des Co-Resident CUIC/LiveData/IdS Publisher oder des Standalone IdS Publisher - Neuaufbau des Co-Resident CUIC/LiveData/IdS Subscriber oder des Standalone IdS Subscribers

Diese Situationen treten nur selten auf, und es wird dringend empfohlen, mit der Single Sign-On (SSO)-Konfiguration neu zu beginnen, um sicherzustellen, dass die SSO-Funktionalität in der Produktionsumgebung schnell und effizient wiederhergestellt wird. Es ist wichtig, diese Neukonfiguration zu priorisieren, um Unterbrechungen der SSO-Dienste, von denen die Benutzer abhängen, auf ein Minimum zu reduzieren.

Lösung

1. Löschen Sie die vorhandene vertrauende Partei aus dem AD FS.

2. Laden Sie das AD FS SSL-Zertifikat in den Cisco IdS-Server hoch, um die Vertrauensstellung zu erhalten.

3. Laden Sie die sp.xml-Datei herunter.

4. Ausführliche Informationen hierzu finden Sie im Referenzabschnitt und im Funktionshandbuch.

5. Konfigurieren der vertrauenden Partei im AD FS

6. Anspruchsregeln hinzufügen

7. Signierte SAML-Assertion aktivieren

8. AD FS-Verbundmetadaten herunterladen

9. Laden Sie die Verbundmetadaten auf den Cisco IDs-Server hoch.

10. Test-SSO durchführen

Referenz

Hinzufügen einer vertrauenden Partei im ADFS oder

So aktivieren Sie eine signierte SAML-Assertion

Ausführliche Informationen hierzu finden Sie in diesem Dokument: UCCE 12.6.1 - Funktionshandbuch

So laden Sie das AD FS SSL-Zertifikat in die Cisco IdS-Vertrauensstellung hoch

1. Laden Sie das AD FS SSL-Zertifikat herunter, oder rufen Sie es ab.

2. Zugriff auf die Seite "Cisco IdS Publisher OS Administration"

3. Melden Sie sich mit den Anmeldeinformationen des Betriebssystemadministrators an.

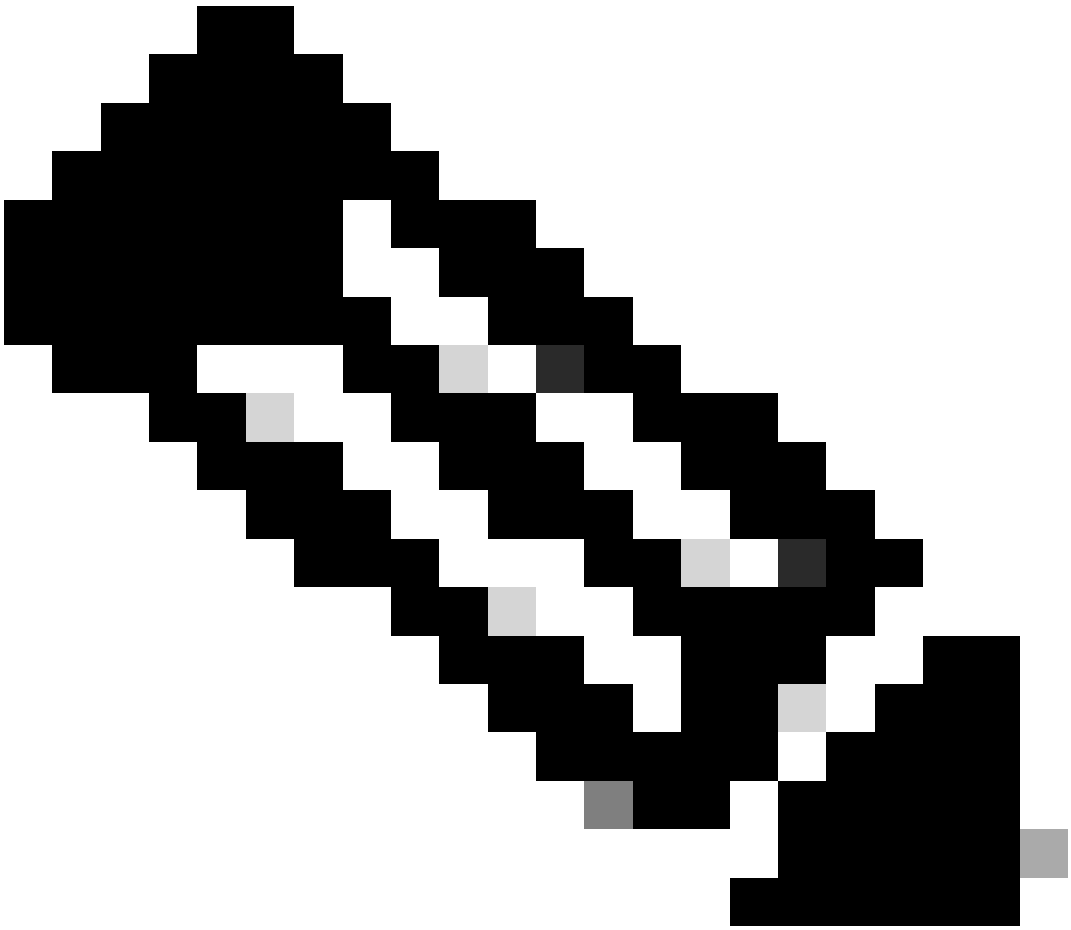
4. Navigieren Sie zu Sicherheit > Zertifikatsverwaltung

5. Klicken Sie auf Zertifikat hochladen/Zertifikatskette, und ein Popup-Fenster wird geöffnet

6. Klicken Sie auf das Dropdown-Menü, und wählen Sie "Kat-Vertrauenswürdigkeit für Zertifikatzweck" aus

7. Klicken Sie auf Durchsuchen und wählen Sie das AD FS SSL-Zertifikat aus.

8. Klicken Sie auf Hochladen



(Hinweis: {Die Vertrauenszertifikate werden auf die Subscriber-Knoten repliziert. Sie müssen den Upload nicht auf den Subscriber-Knoten durchführen.})

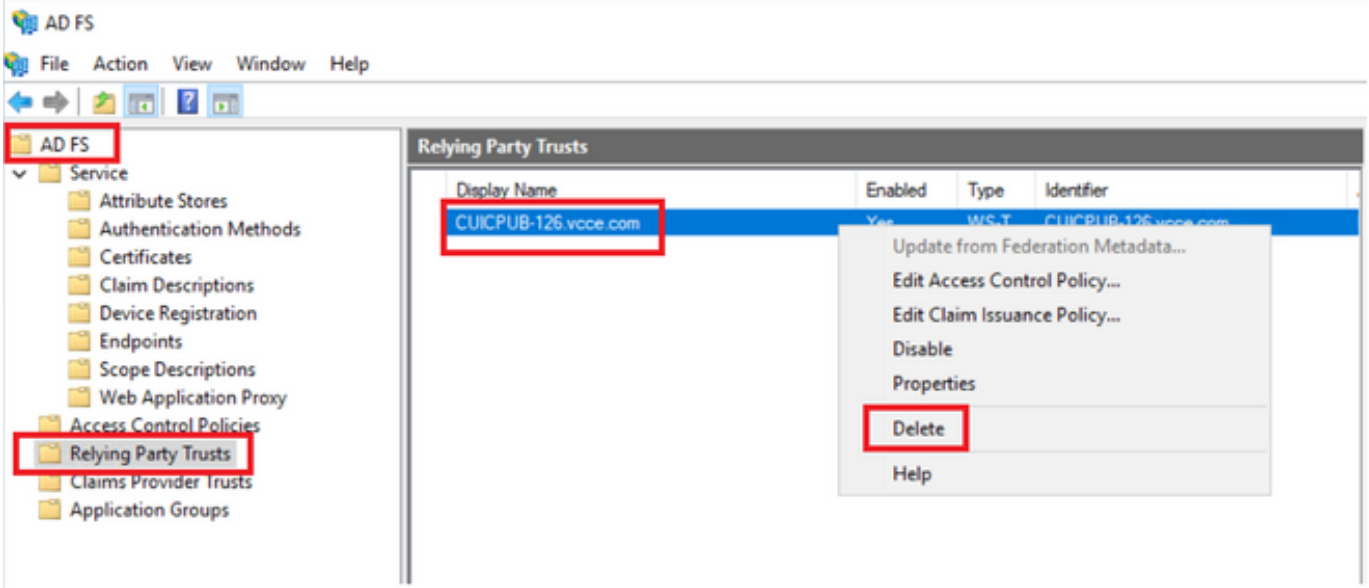
Löschen der vertrauenden Partei im AD FS

1. Melden Sie sich mit den Administratorberechtigungen beim Identity Provider (IdP)-Server an.

2. Öffnen Sie den Server Manager und wählen Sie AD FS > Tools > AD FS Management

3. Wählen Sie im linken Seitenbaum die Vertrauenswürdigkeit der vertrauenden Partei unter dem AD FS

4. Klicken Sie mit der rechten Maustaste auf den Cisco IDs-Server, und wählen Sie Löschen aus.



Überprüfen und Ändern des im Identity Provider (IdP) konfigurierten sicheren Hash-Algorithmus

1. Melden Sie sich mit den Administratorberechtigungen beim Identity Provider (IdP)-Server an.

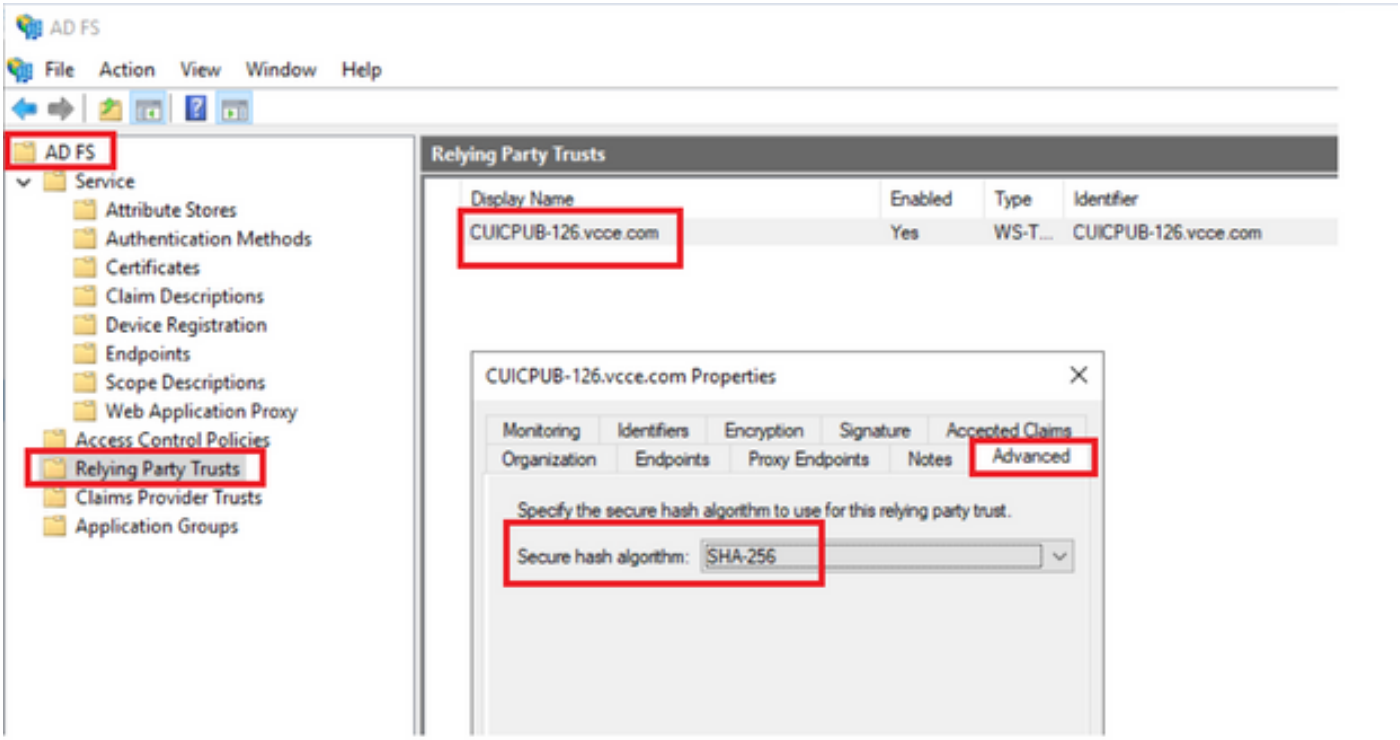
2. Öffnen Sie den Server Manager und wählen Sie AD FS > Tools > AD FS Management

3. Wählen Sie im linken Seitenbaum die Vertrauenswürdigkeit der vertrauenden Partei unter dem AD FS

4. Klicken Sie mit der rechten Maustaste auf den Cisco IdS-Server, und wählen Sie Eigenschaften aus

5. Navigieren Sie zur Registerkarte Erweitert

6. Die Option "Sicherer Hashalgorithmus" zeigt den im AD FS-Server konfigurierten sicheren Hashalgorithmus an.



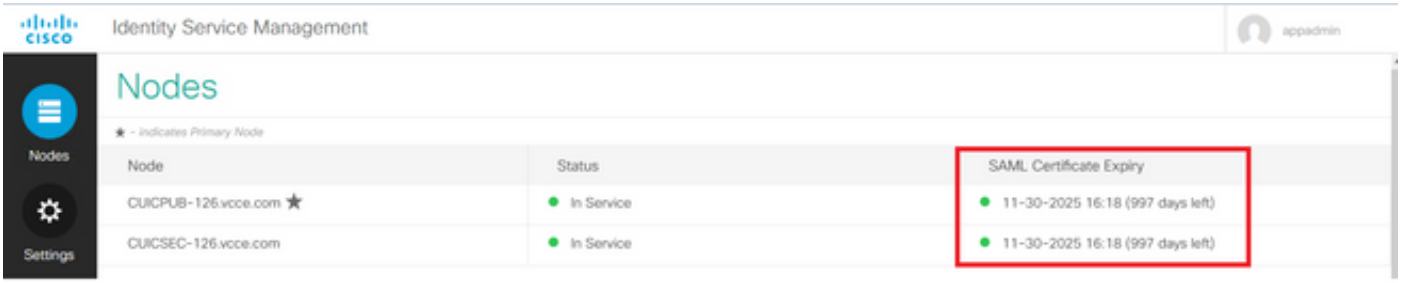
7. Klicken Sie auf das Dropdown-Menü, und wählen Sie den gewünschten sicheren Hash-Algorithmus aus.

Überprüfen des Ablaufdatums des SAML-Zertifikats des Cisco IdS-Servers

1. Melden Sie sich mit den Anmeldeinformationen des Anwendungsbenutzers beim Publisher- oder Subscriber-Knoten des Cisco IdS-Servers an.

2. Nach erfolgreicher Anmeldung landet die Seite bei Identity Service Management > Nodes

3. Zeigt den Knoten "Cisco IdS Publisher und Subscriber", den Status und das SAML-Zertifikatsablauf an.



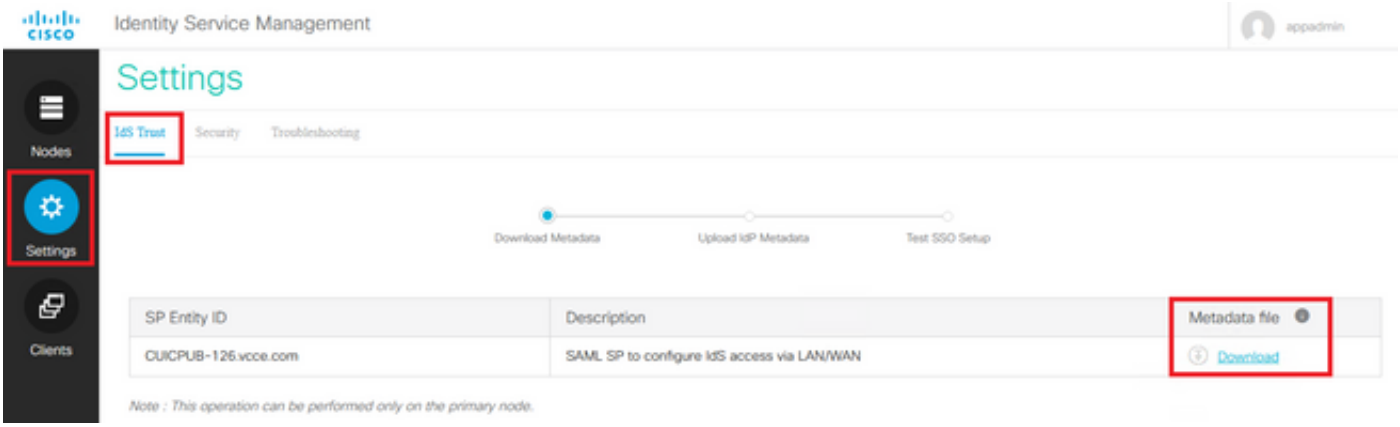
Herunterladen der Metadaten des Cisco IdS-Servers

1. Melden Sie sich mit den Anmeldeinformationen des Anwendungsbenutzers beim Cisco IdS Publisher-Knoten an.

2. Klicken Sie auf das Einstellungssymbol

3. Navigieren Sie zur Registerkarte IDS Trust (IDS-Vertrauen)

4. Klicken Sie auf den Link Download, um die Metadaten des Cisco IdS-Clusters herunterzuladen.



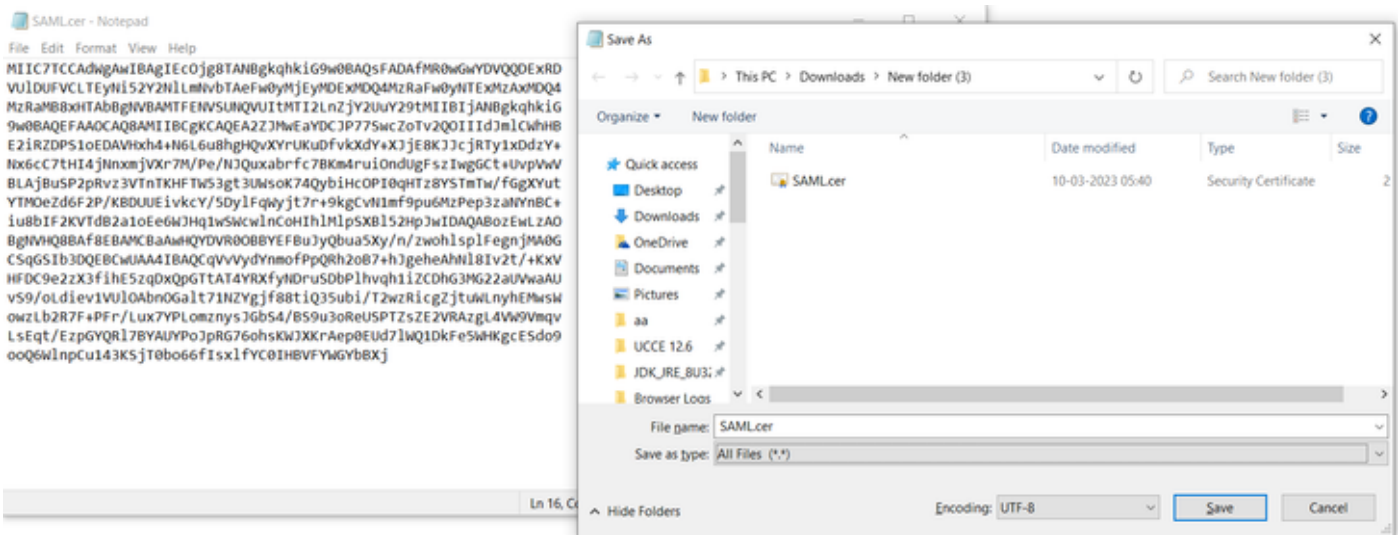
Abrufen des SAML-Zertifikats aus der sp.xml-Datei

1. Öffnen Sie die Datei sp.xml mit einem Texteditor.

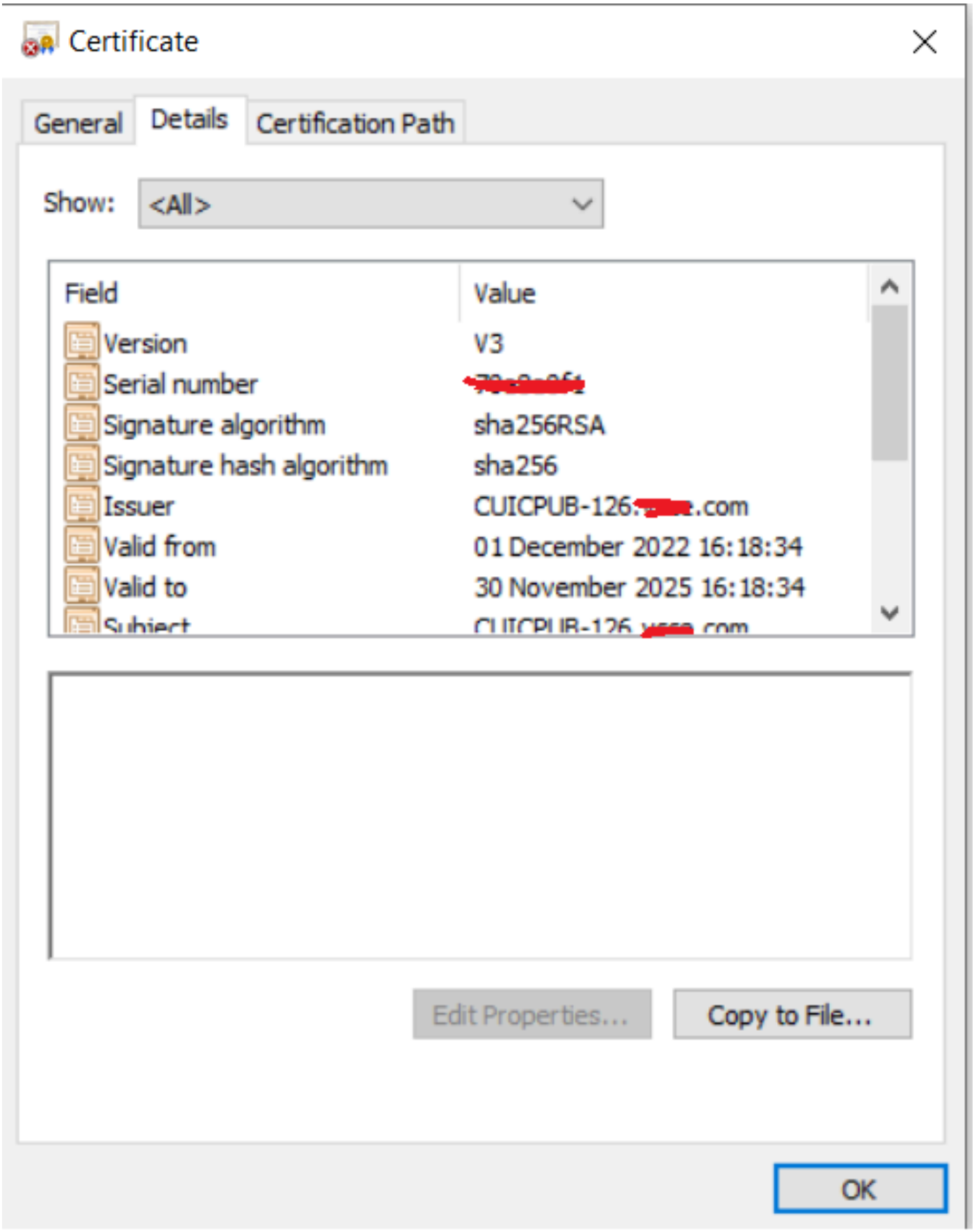
2. Kopieren Sie die Rohdaten zwischen den Header <ds:X509Certificate></ds:X509Certificate>

3. Öffnen Sie einen anderen Texteditor und fügen Sie die kopierten Daten ein

4. Speichern Sie die Datei im Format .CER



5. Öffnen Sie das Zertifikat, um die Zertifikatinformationen zu überprüfen.



Ersetzen des SAML-Zertifikats im AD FS

1. Kopieren Sie die SAML-Zertifikatsdatei auf den AD FS-Server, der aus dem sp.xml abgerufen wird.

2. Öffnen Sie den Server Manager und wählen Sie AD FS > Tools > AD FS Management

3. Wählen Sie im linken Seitenbaum die Vertrauenswürdigkeit der vertrauenden Partei unter dem AD FS

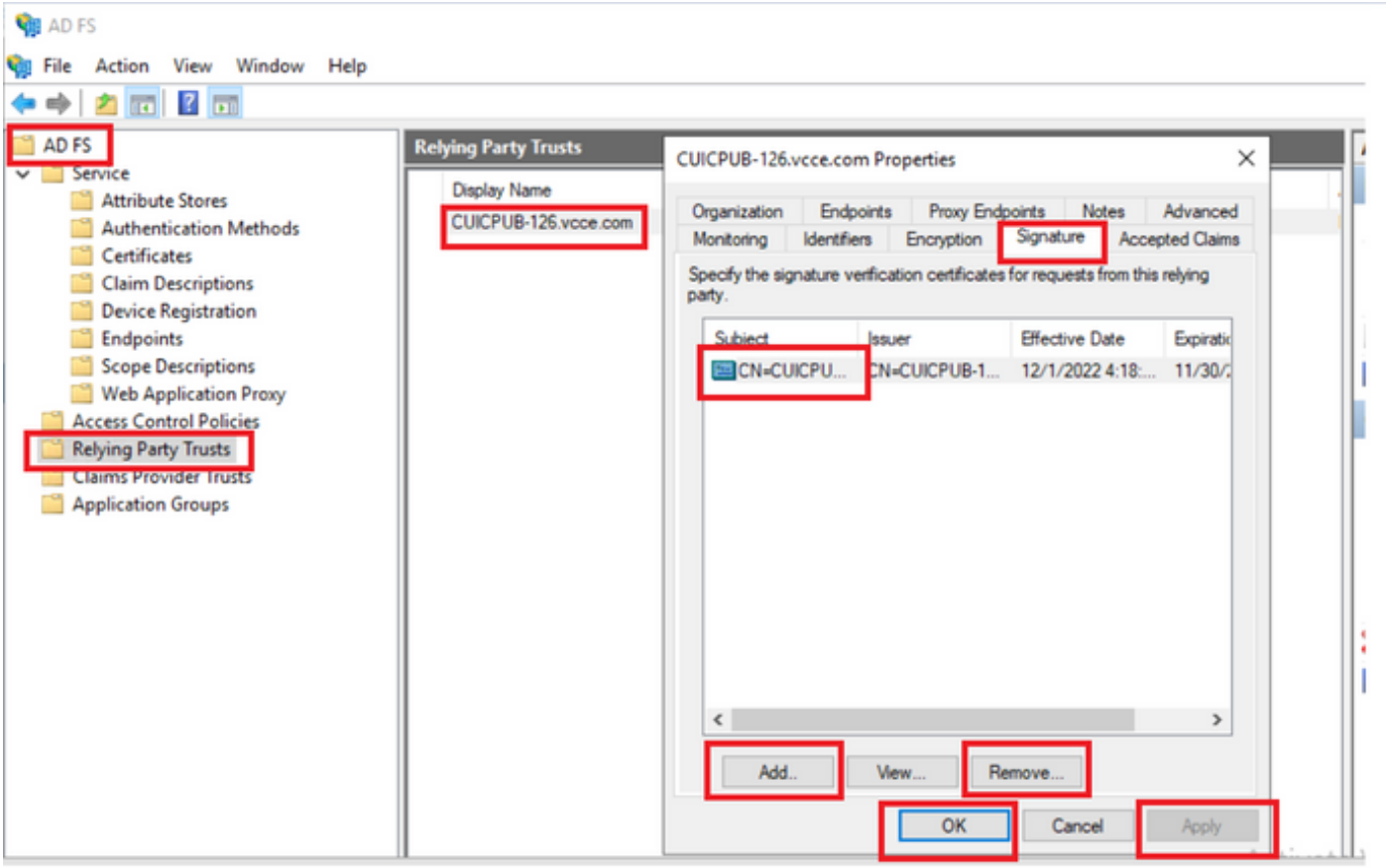
4. Klicken Sie mit der rechten Maustaste auf den Cisco IdS-Server, und wählen Sie Eigenschaften aus

5. Navigieren Sie zur Registerkarte Signatur.

6. Klicken Sie auf Hinzufügen und wählen Sie das neu generierte SAML-Zertifikat

7. Wählen Sie das alte SAML-Zertifikat und klicken Sie auf Entfernen

8. Anwenden und speichern



Neugenerierung des SAML-Zertifikats auf dem Cisco IdS-Server

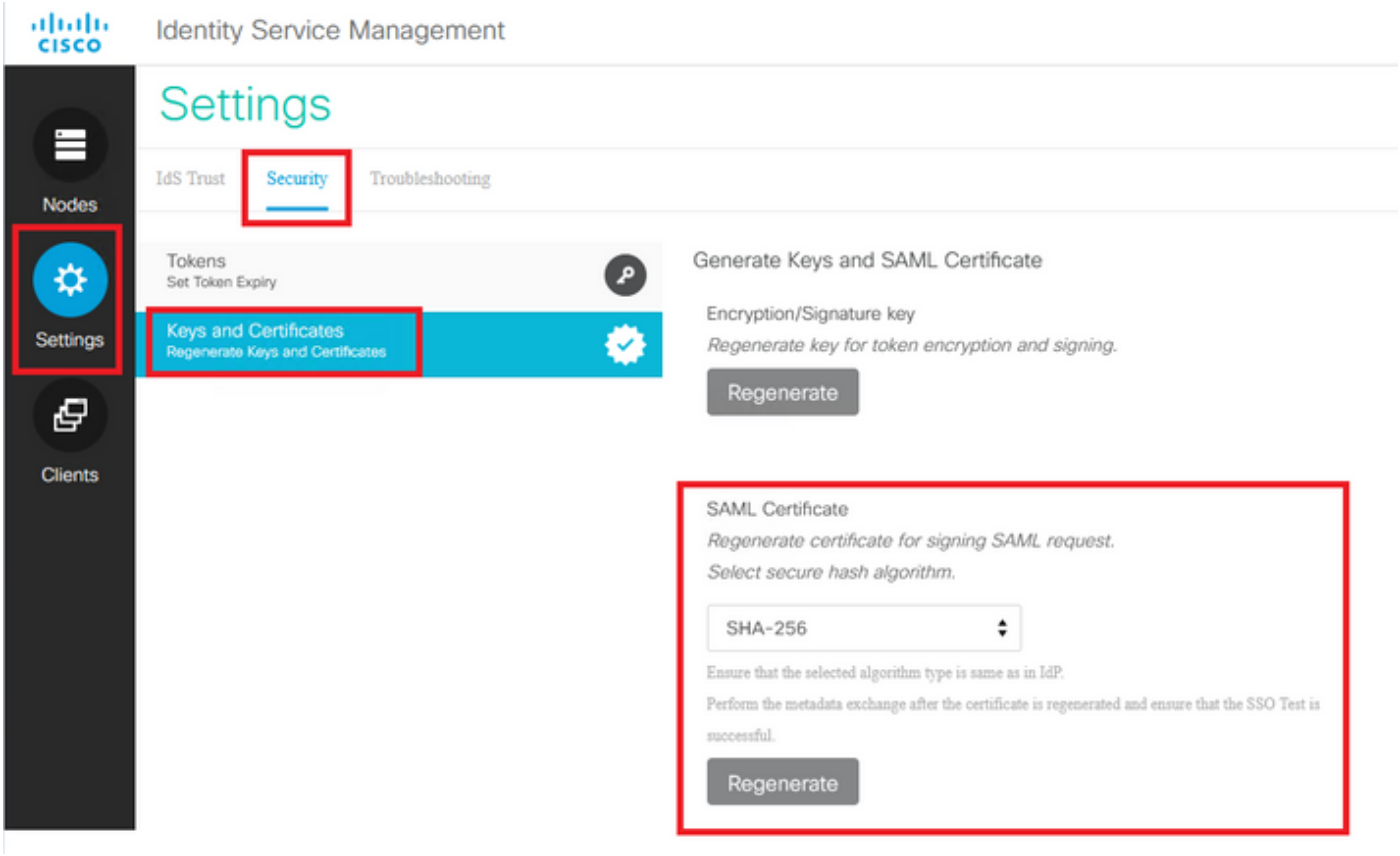
1. Melden Sie sich mit den Anmeldeinformationen des Anwendungsbenutzers beim Cisco IdS Publisher-Knoten an.

2. Klicken Sie auf das Einstellungssymbol

3. Navigieren Sie zur Registerkarte Sicherheit.

4. Wählen Sie die Option Schlüssel und Zertifikate

5. Klicken Sie auf die Schaltfläche Regenerieren unter dem SAML-Zertifikatabschnitt (hervorgehoben)



SSO testen

Bei jeder Änderung des SAML-Zertifikats stellen Sie sicher, dass TEST SSO erfolgreich auf dem Cisco IdS-Server ausgeführt wurde, und registrieren Sie alle Anwendungen von der CCEAdmin-Seite erneut.

1. Zugriff auf die CCEAdmin-Seite über den AW-Hauptserver

2. Melden Sie sich mit den Administratorberechtigungen beim CCEAdmin-Portal an.

3. Navigieren Sie zu Übersicht > Funktionen > Einmalige Anmeldung

4. Klicken Sie unter "Registrieren beim Cisco Identity Service" auf die Schaltfläche "Registrieren".

5. Test-SSO durchführen

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.