Erstellen und Verwenden eines Drittanbieterzertifikats in UCSM

Inhalt

Einleitung

In diesem Dokument wird das Verfahren zum Erstellen und Verwenden von Zertifikaten von Drittanbietern auf dem Unified Computing System (UCS) für die sichere Kommunikation beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Zugang zur Zertifizierungsstelle
- UCSM 3.1

Verwendete Komponenten

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,

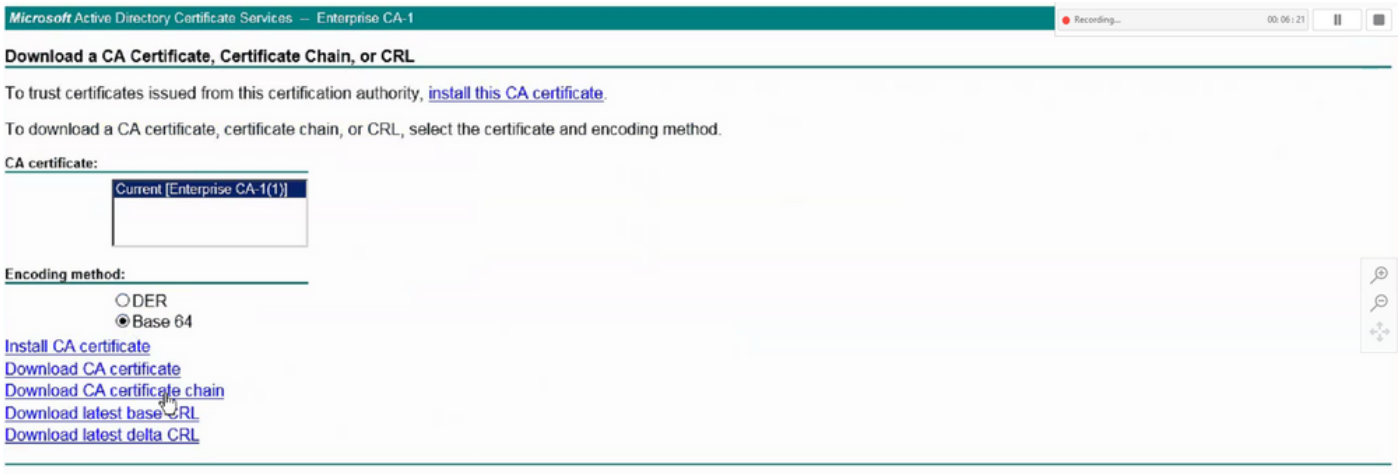
dass Sie die möglichen Auswirkungen aller Befehle kennen.

Zu konfigurierende Schritte

Vertrauenspunkt konfigurieren

Schritt 1

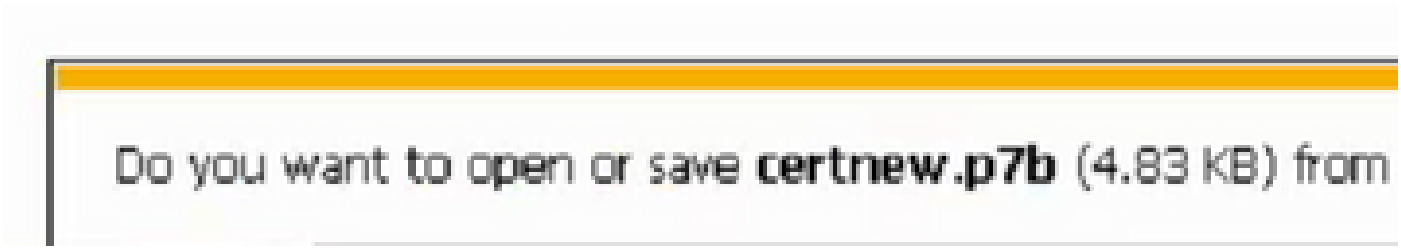
- Laden Sie die Zertifikatkette von der Zertifizierungsstelle herunter, um einen Vertrauenspunkt zu erstellen. Weitere Informationen finden Sie unter http://localhost/certsrv/Default.asp auf dem Zertifikatserver.
- Stellen Sie sicher, dass die Kodierung auf Basis 64 eingestellt ist.



Zertifikatskette von Zertifizierungsstelle herunterladen

Schritt 2

- Die heruntergeladene Zertifikatskette ist im PB7-Format.

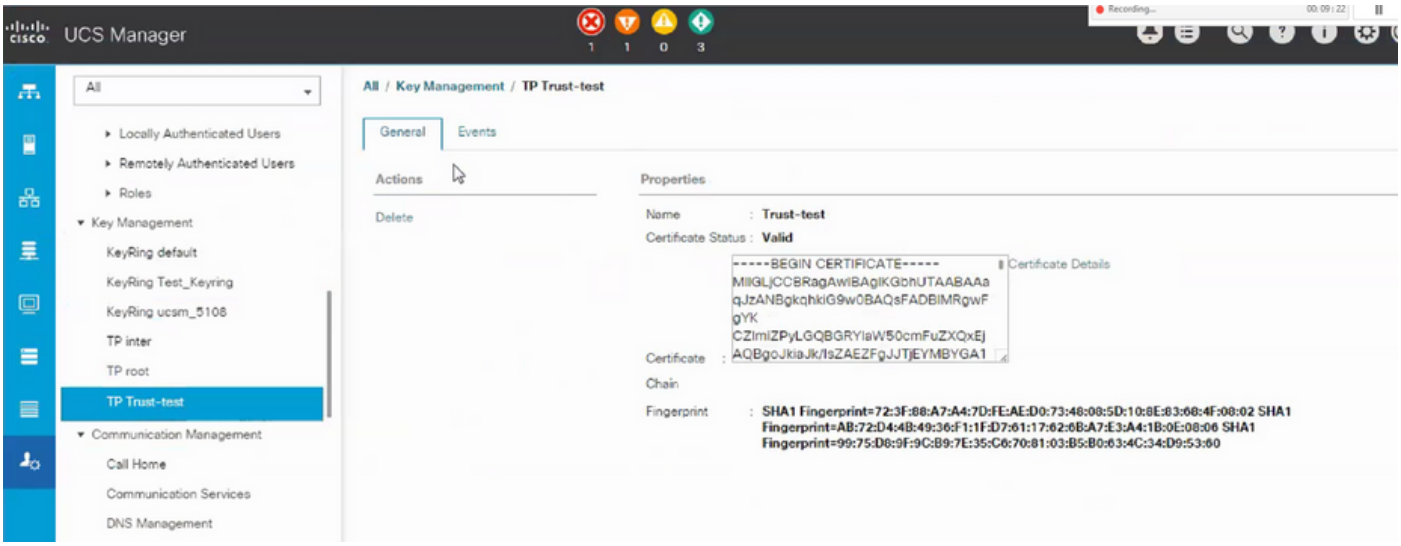


- Konvertieren Sie die .pb7-Datei in das PEM-Format mit dem OpenSSL-Tool.
- In Linux können Sie diesen Befehl beispielsweise in Terminal ausführen, um die Konvertierung durchzuführen: openssl pkcs7 -print_certs -in <cert_name>.p7b -out <cert_name>.pem.

Schritt 3

- Erstellen Sie einen Vertrauenspunkt für UCSM.
- Navigieren Sie zu Admin > Key Management > Trustpoint.

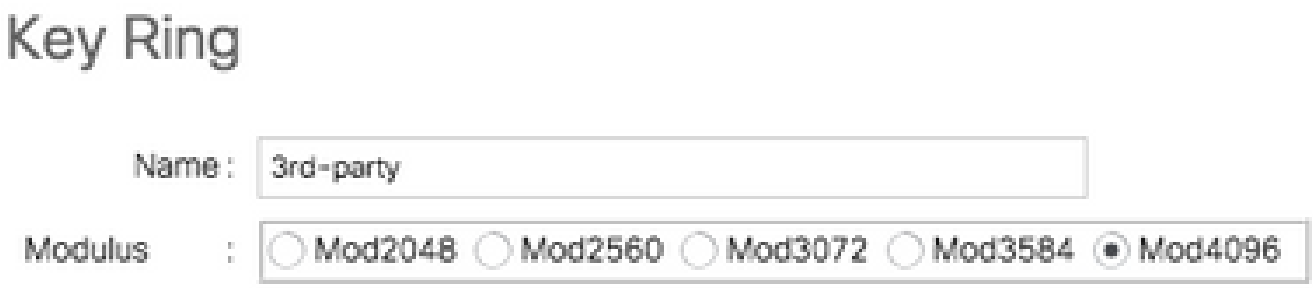
- Wenn Sie den Vertrauenspunkt erstellen, fügen Sie den gesamten Inhalt der PEM-Datei, die in Schritt 2 dieses Abschnitts erstellt wurde, im Zertifikatdetailbereich ein.



Schlüsselbund und CSR erstellen

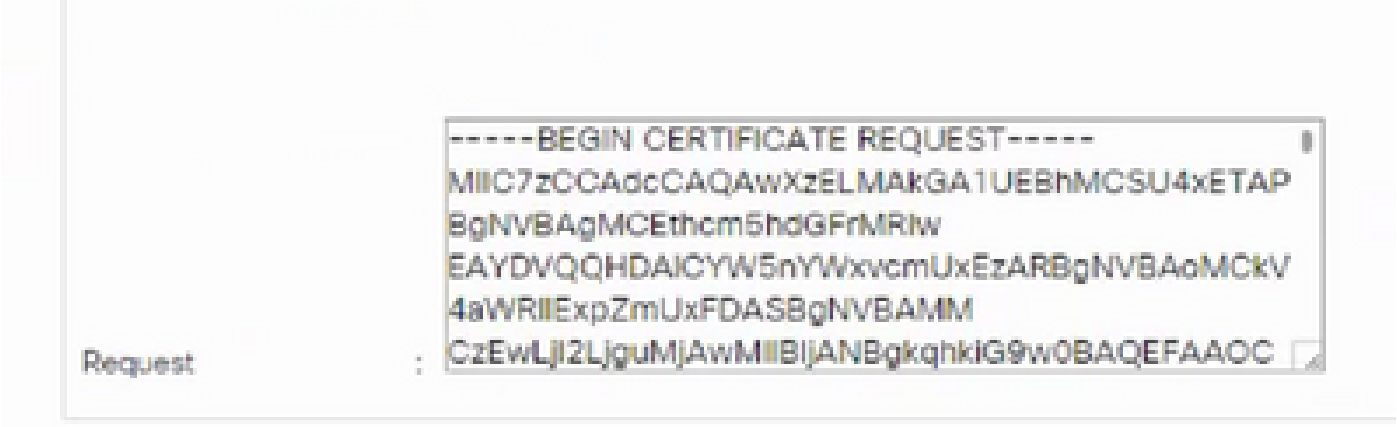
Schritt 1

- Navigieren Sie zu UCSM > Admin > Key Management > Keyring.
- Wählen Sie das Modul aus, das für das Drittanbieterzertifikat benötigt wird.



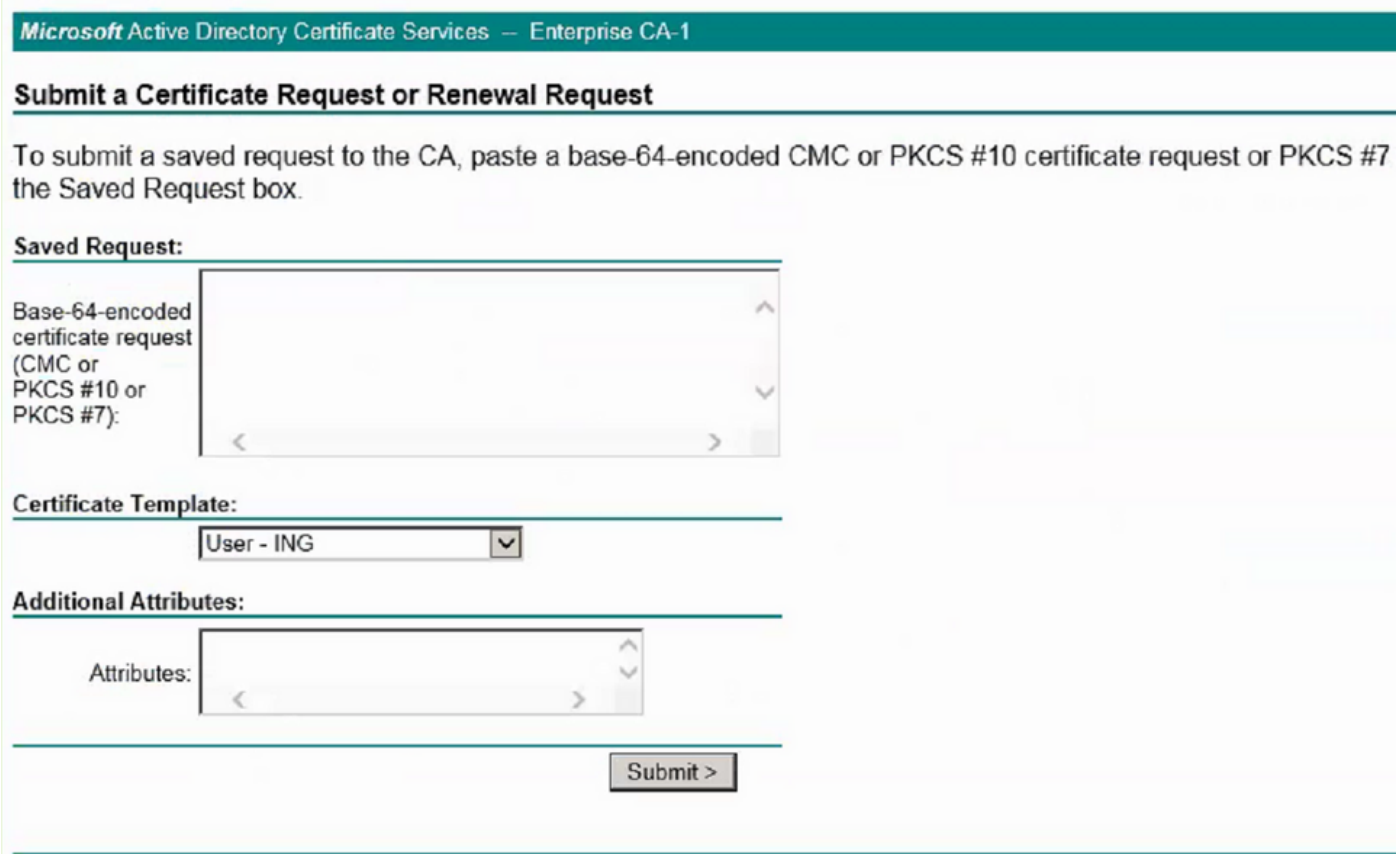
Schritt 2

- Klicken Sie auf Zertifikatsanforderung erstellen, und geben Sie die erforderlichen Details ein.
- Kopieren Sie den Inhalt des Anforderungsfelds.



Schritt 3

Fügen Sie zum Generieren des Zertifikats die kopierte Anforderung aus Schritt 2 in den unten angezeigten Bereich ein:



Schritt 4

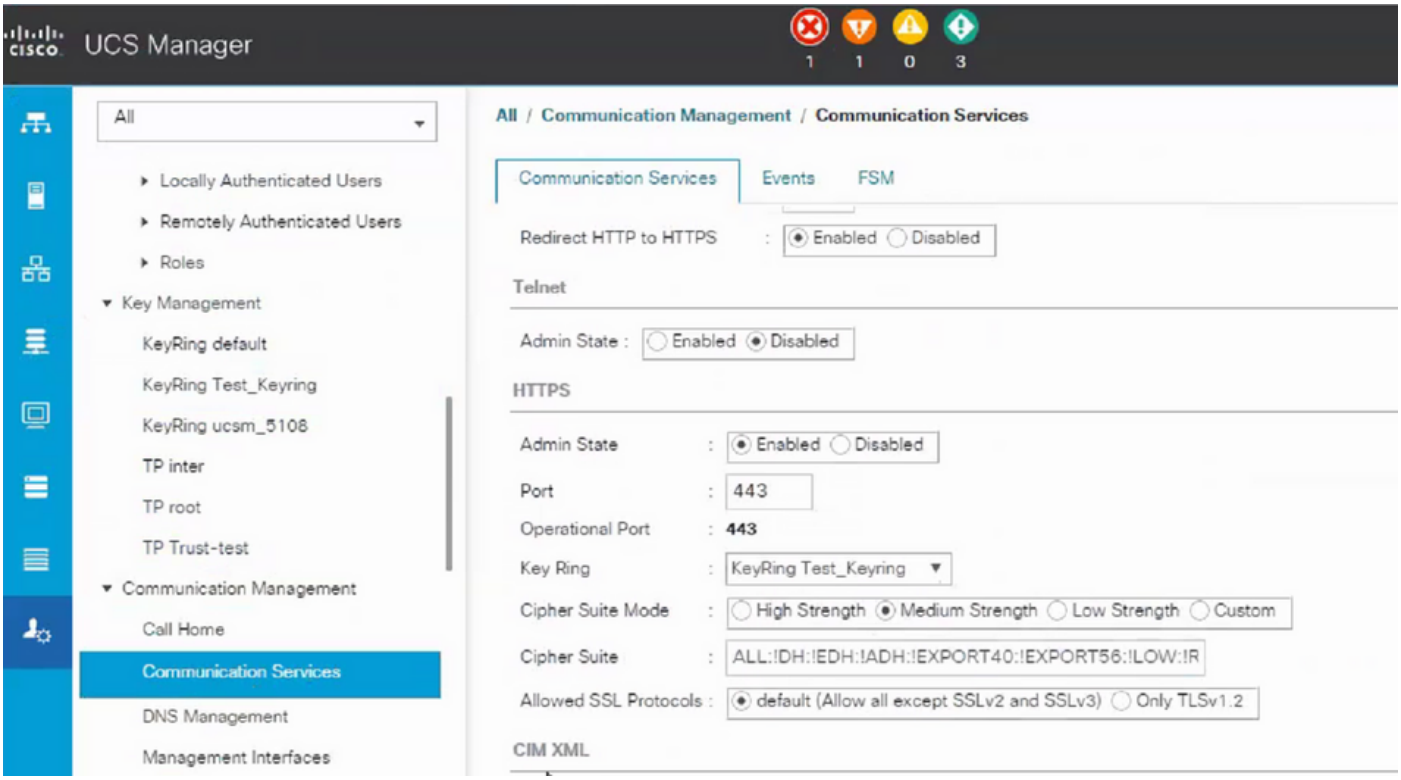
- Nach dem Absenden wird ein neues Zertifikat generiert. Öffnen Sie die Datei, und kopieren Sie den gesamten Inhalt des neu erstellten Zertifikats in das Zertifikatfeld des in Schritt 1 dieses Abschnitts erstellten Keyrings.

- Wählen Sie den Vertrauenspunkt aus der Dropdown-Liste aus, die in Schritt 3 von Create Keyring (Schlüsselbund erstellen) und CSR erstellt wurde.

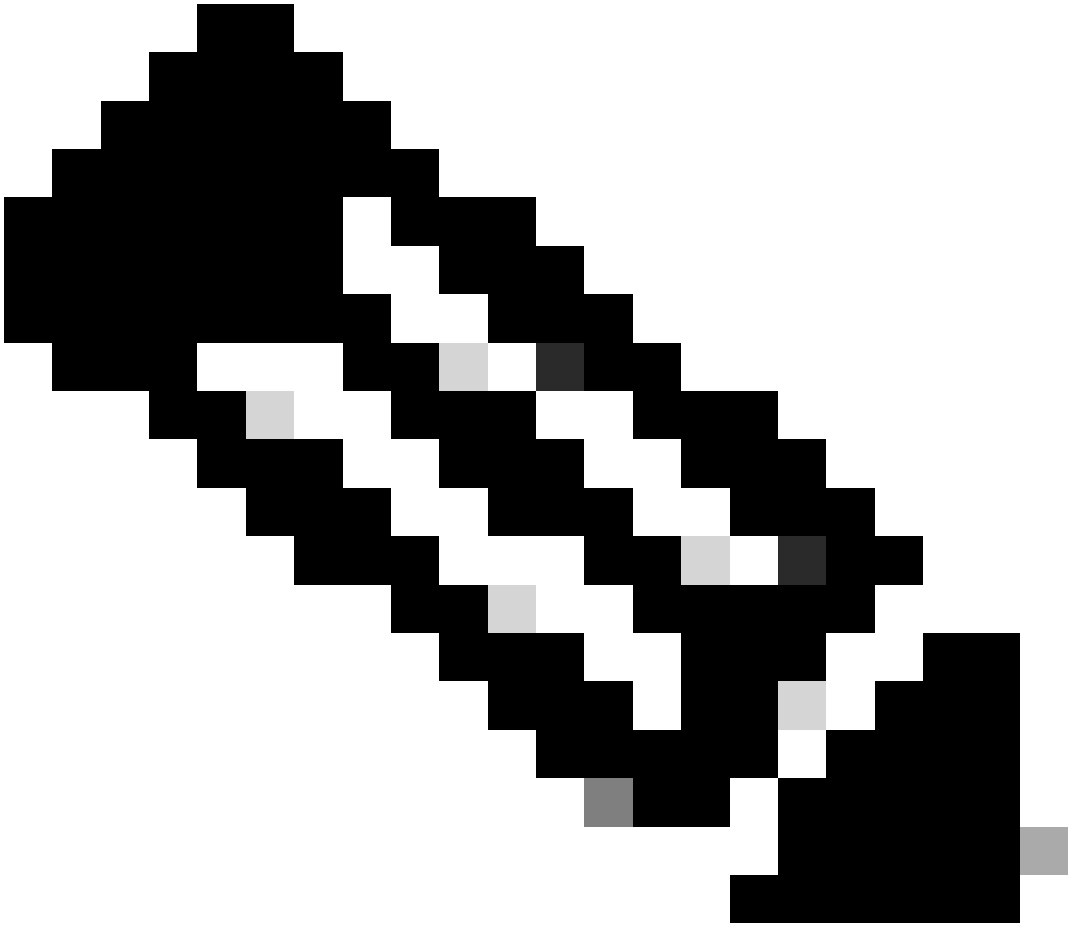
Anwenden des Keyrings

Schritt 1

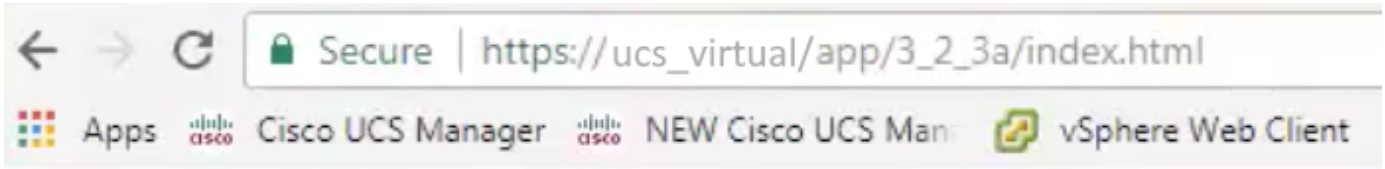
Wählen Sie den erstellten Keyring in den Kommunikationsdiensten wie unten gezeigt:



Nach der Änderung des Keyrings wird die HTTPS-Verbindung zum UCSM in Ihrem Webbrowser als sicher angezeigt.



Hinweis: Dazu muss der lokale Desktop das Zertifikat derselben Zertifizierungsstelle wie UCSM verwenden.



Zugehörige Informationen

- Technischer Support und Dokumentation für Cisco Systeme

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.