# Erstellen und Verwenden eines Drittanbieterzertifikats in UCSM

# Inhalt

Einleitung
Voraussetzungen
Anforderungen
Verwendete Komponenten
Zu konfigurierende Schritte
Vertrauenspunkt konfigurieren
Schritt 1
Schritt 2
Schritt 3
Schlüsselbund und CSR erstellen
Schritt 1
Schritt 2
Schritt 3
Schritt 4
Anwenden des Keyrings
Schritt 1
Zugehörige Informationen

# 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 <u>http://localhost/certsrv/Default.asp</u> auf dem Zertifikatserver.
- Stellen Sie sicher, dass die Kodierung auf Basis 64 eingestellt ist.

Microsoft Active Directory Certificate Services - Enterprise CA-1	
Download a CA Certificate, Certificate Chain, or CRL	
To trust certificates issued from this certification authority, install this CA certificate.	
To download a CA certificate, certificate chain, or CRL, select the certificate and encoding method.	
CA certificate: Current [Enterprise CA-1(1)]	
Encoding method:	ø
⊙DER ⊛Base 64	P
Install CA certificate	.A.
Download CA certificate Download CA certificate Download latest base	

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.

.ili.ili. cisco	UCS Manager	ا 😢 ا	
æ	All 👻	All / Key Management / TP Trust-test	
	Locally Authenticated Users     Remotely Authenticated Users     Dolen	Actions &	Properties
55 =	✓ Key Management Key Ping default	Delete	Name : Trust-test Certificate Status : Valid
-	KeyRing Test_Keyring KeyRing ucsm_5108		MIIGLICCERagAwiBAgiKGbhUTAABAAa qJzANBgkqhkiG9w0BAQsFADBIMRgwF gYK
=	TP inter TP root		Certificate : AQBgoJkiaJk/IsZAEZFgJJTjEYMBYGA1 Chain
=	TP Trust-test  Communication Management		Fingerprint : SHA1 Fingerprint=72:3F:88:A7:A4:7D:FE:AE:D0:73:48:08:5D:10:8E:83:08:4F:08:02 SHA1 Fingerprint=A8:72:D4:4B:49:36:F1:1F:D7:61:17:62:08:A7:E3:A4:1B:0E:08:06 SHA1 Fingerprint=99:75:D8:9F:9C:B9:7E:35:C6:70:81:03:B5:80:63:4C:34:D9:53:60
40	Call Home Communication Services DNS Management		

### 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.

# Key Ring

Name :	3rd-party	
Modulus :	Mod2048 Mod2560 Mod3072 Mod3584	Mod4096

#### 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:

#### Microsoft Active Directory Certificate Services - Enterprise CA-1

#### Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC or PKCS #10 certificate request or PKCS #7 the Saved Request box.

Saved Request:				
Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):			< >	
	<		>	
Certificate Templa	ate:			
	User - ING	~		
Additional Attribu	ites:			
Attributes:	<	~ ~		
		Submit	>	

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.

Trusted Point :	Trust-test	Ψ.	
Certificate :	BEGIN CERT MIIGLJCCBRagAw 9w0BAQsFADBIM CZIMIZPyLGQBGF ZAEZFgJJTJEYMB AxMPRW50ZXJw	IFICATE BAgIKS4anFAABAAa RgwFgYK YlaW50cmFuZXQxE YGA1UE cmIzZSBDQS0xMB4)	DANBgkqhkiG QBgoJkiaJk/Is TE4MDUwOD

• 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:

cisco	UCS Manager	
æ	All	All / Communication Management / Communication Services
	<ul> <li>Locally Authenticated Users</li> <li>Remotely Authenticated Users</li> </ul>	Communication Services Events FSM Redirect HTTP to HTTPS : • Enabled O Disabled
쁆	<ul> <li>▶ Roles</li> <li>★ Key Management</li> </ul>	Telnet
Ξ.	KeyRing default	Admin State : Enabled  Disabled
Q	KeyRing Test_Keyring KeyRing ucsm_5108	Admin State : • Enabled Obisabled
=	TP inter TP root	Port : 443 Operational Port : 443
	TP Trust-test  Communication Management	Key Ring : KeyRing Test_Keyring ▼ Cipher Suite Mode : High Strength @ Medium Strength O Custom
1 <sub>0</sub>	Call Home	Cipher Suite : ALL:IDH:IEDH:IADH:IEXPORT40:IEXPORT56:ILOW:IR
	Communication Services DNS Management Management Interfaces	Allowed SSL Protocols :      default (Allow all except SSLv2 and SSLv3)      Only TLSv1.2  CIM XML

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

<u>Technischer Support und Dokumentation für Cisco Systeme</u>

#### 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.