# Crea e utilizza certificato di terze parti su UCSM

# Sommario

Introduzione
Prerequisiti
Requisiti
Componenti usati
Passi da configurare
Configura trust point
Passaggio 1
Passaggio 2
Passaggio 3
Creazione di portachiavi e CSR
Passaggio 1
Passaggio 2
Passaggio 3
Passaggio 4
Applicazione della sequenza di tasti
Passaggio 1
Informazioni correlate

# Introduzione

Questo documento descrive la procedura per creare e utilizzare certificati di terze parti su Unified Computing System (UCS) per comunicazioni protette.

# Prerequisiti

### Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Accesso all'autorità CA
- UCS SM 3.1

### Componenti usati

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.

# Passi da configurare

### Configura trust point

Passaggio 1

- Scaricare la catena di certificati dall'autorità CA per creare il trust point. Fare riferimento a <u>http://localhost/certsrv/Default.asp</u> all'interno di Cert Server.
- Assicurarsi che la codifica sia impostata su Base 64.

Microsoft Active Directory Certificate Services - Enterprise CA-1	Recording_	00: 06 : 21	П	
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: ODER @ Base 64				() () () ()
Install CA certificate Download CA certificate Download latest base RL Download latest delta CRL				2°.

Scarica catena di certificati dall'autorità CA

#### Passaggio 2

• La catena di certificati scaricata è in formato PB7.



- Convertire il file .pb7 in formato PEM con lo strumento OpenSSL.
- Ad esempio, in Linux, è possibile eseguire questo comando in terminal per eseguire la conversione openssl pkcs7 -print\_certs -in <nome\_cert>.p7b -out <nome\_cert>.pem.

Passaggio 3

- Creare un trust point su UCSM.
- Passare ad Amministrazione > Gestione chiavi > Trustpoint.
- Quando si crea il trust point, incollare il contenuto completo del file PEM creato nel passaggio 2 di questa sezione nello spazio dei dettagli del certificato.



Creazione di portachiavi e CSR

#### Passaggio 1

- Passare a UCSM > Admin > Gestione tasti > Gruppo di chiavi.
- Scegliere il modulo necessario per il certificato di terze parti.

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

Passaggio 2

- Fare clic su Crea richiesta certificato e specificare i dettagli richiesti.
- · Copiare il contenuto del campo della richiesta.

	BEGIN CERTIFICATE REQUEST
	MIIC7zCCAdcCAQAwXzELMAkGA1UEBhMCSU4xETAP
	BgNVBAgMCEthcm5hdGFrMRIw
	EAYDVQQHDAICYW5nYWxvcmUxEzARBgNVBAoMCkV
	4aWRIIExpZmUxFDASBgNVBAMM
Demiest	CzEwLil2LiauMiAwMIIBIjANBakahkiG9w0BAQEFAAOC

Passaggio 3

Per generare il certificato, incollare la richiesta copiata dal passaggio 2 nello spazio indicato di seguito:

### 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 Templ	ate: User - ING	V	>		
Additional Attribu	ites:				
Attributes:	<	>			
		Subn	nit >		

Passaggio 4

 Una volta inviato, viene generato un nuovo certificato. Aprire il file e copiare tutto il contenuto del certificato appena generato nel campo del certificato sul keyring creato al passaggio 1 di questa sezione.

Trusted Point :	Trust-test	Ψ.	
Certificate :	BEGIN CERT MIIGLJCCBRagAwl 9w0BAQsFADBIMI CZImiZPyLGQBGR ZAEZFgJJTjEYMB AxMPRW50ZXJwo	IFICATE BAgIKS4anFAABAA RgwFgYK YIaW50cmFuZXQxE YGA1UE cmIzZSBDQS0xMB4	jDANBgkqhkiG QBgoJkiaJk/Is DTE4MDUwOD

• Scegliere il trust-point dall'elenco a discesa creato nel passaggio 3 di Crea keyring e CSR.

#### Applicazione della sequenza di tasti

#### Passaggio 1

Scegliere la sequenza di tasti creata nei servizi di comunicazione come illustrato di seguito:

cisco.	UCS Manager	
æ	All	All / Communication Management / Communication Services
-	<ul> <li>Locally Authenticated Users</li> <li>Remotely Authenticated Users</li> <li>Roles</li> <li>Key Management</li> </ul>	Communication Services Events FSM Redirect HTTP to HTTPS :  Events Communication Services Telnet
重	KeyRing default	Admin State : Enabled Disabled
Q	KeyRing Test_Keyring KeyRing ucsm_5108	Admin State :  Enabled  Disabled
=	TP inter TP root	Port : 443
	TP Trust-test  Communication Management	Key Ring : KeyRing Test_Keyring ▼
1 <sub>0</sub>	Call Home	Cipher Suite Mode : High Strength  Medium Strength  Low Strength  Custom Cipher Suite : ALL:!DH:!EDH:!ADH:!EXPORT40:!EXPORT56:!LOW:!R
	DNS Management Management Interfaces	Allowed SSL Protocols : ( default (Allow all except SSLv2 and SSLv3) Only TLSv1.2 CIM XML

Dopo la modifica della sequenza di tasti, la connessione HTTPS al modulo UCSM risulta protetta nel browser Web.



Nota: è necessario che anche il desktop locale utilizzi il certificato della stessa autorità CA del modulo UCSM.



### Informazioni correlate

<u>Documentazione e supporto tecnico – Cisco Systems</u>

#### 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).