Create and Use Third Party Certificate on UCSM

Contents

Introduction **P**rerequisites **Requirements Components Used** Steps to Configure **Configure Trust Point** Step 1 Step 2 Step 3 Create Keyring and CSR Step 1 Step 2 Step 3 Step 4 Apply the Keyring Step 1 **Related Information**

Introduction

This document describes the procedure to create and use third party certificates on Unified Computing System (UCS) for secure communication.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Access to CA Authority
- UCSM 3.1

Components Used

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Steps to Configure

Configure Trust Point

Step 1

• Download the certificate chain from the CA authority to create Trust-Point. Refer

to <u>http://localhost/certsrv/Default.asp</u> within the Cert Server.Make sure encoding is set to Base 64.

Microsoft Active Directo	y 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 certifica	te: Current [Enterprise CA-1(1)]	
Encoding m	nethod:	
	ODER	
	Base 64	
Install CA	certificate	
Download	CA certificate	
Download	CA certificate chain	
Download	latest base RL	
Download	latest delta CRL	

Download Certificate chain from CA Authority

Step 2

• The downloaded certificate-chain is in PB7 format.

Do you want to open or save certnew.p7b (4.83 KB) from

- Convert the .pb7 file to PEM format with OpenSSL tool.
- For example, in Linux, you can run this command in terminal to perform the conversion- openssl pkcs7 -print_certs -in <cert_name>.p7b -out <cert_name>.pem.

Step 3

- Create a Trust-Point on UCSM.
- Navigate to Admin > Key Management > Trustpoint.
- When you create the Trust-point, paste the complete contents of the .PEM file created in step 2 of this section in the certificate details space.

.1 1.1 1. CISCO	UCS Manager		Reci
ж 	All Locally Authenticated Users	All / Key Management / TP Trust-test General Events	
	 Remotely Authenticated Users Roles 	Actions Properties	
Ŧ	✓ Key Management KeyRing default	Delete Name : Trust-test Certificate Status : Valid	ails
Q	KeyRing Test_Keyring KeyRing ucsm_5108	MIIGLJCCBRagAwIBAGIKGDhUTAABAAa qJzANBgkqhkiG9w0BAQsFADBIMRgwF gYK	
=	TP inter TP root	CZImIZPyLGQBGRYIaW50cmFuZXQxEj Certificate : AQBg0JkiaJk/IsZAEZFgJJTjEYMBYGA1 // Chain	
	TP Trust-test Communication Management	Fingerprint : SHA1 Fingerprint=72:3F:88:A7:A4:7D:FE:AE:D0:73:48:0 Fingerprint=AB:72:D4:4B:49:36:F1:1F:D7:61:17:62:6B:A Fingerprint=99:75:D8:9F:9C:B9:7E:35:C6:70:81:03:B5:B	8:5D: 7:E3: 30:63

: This requires the local desktop to also use the certificate from the same CA authority as the UCSM.



Related Information

<u>Technical Support & Documentation - Cisco Systems</u>