# 排除MRA服務的Expressway流量伺服器證書驗證 故障

目錄
<u>簡介</u>
<u>必要條件</u>
採用元件
受信任的CA鏈
<u>SAN或CN檢查</u>
<u>行為變更</u>
低於X14.2.0的版本
<u>X14.2.0及更高版本</u>
<u>疑難排解案例</u>
<u>1. 簽署遠端證書的CA不受信任</u>
<u>2. 證書中不包含連線地址(FQDN或IP)</u>
如何輕鬆驗證
<u>解決方案</u>
相關資訊

# 簡介

本文檔介紹與思科漏洞ID <u>CSCwc69661</u>或思科漏洞ID <u>CSCwa25108</u>連結的Expressway版本 X14.2.0及更高版本的行為更改。

## 必要條件

#### 需求

思科建議您瞭解以下主題:

- Expressway基本配置
- MRA基本配置

採用元件

本文檔中的資訊基於X14.2及更高版本上的Cisco Expressway。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除(預設))的組態來啟動。如果您的網路運作中,請確保您瞭解任何指令可能造成的影響。



透過思科漏洞ID <u>CSCwc69661</u> 或思科漏洞ID <u>CSCwa25108</u>



標籤的行為更改,Expressway平台上的流量伺服器可執行對思科統一通訊管理器(CUCM)、思科統 一即時消息和線上狀態(IM&P)以及移動和遠端訪問(MRA)服務的Unity伺服器節點的證書驗證。此更 改可能會導致Expressway平台升級後的MRA登入失敗。

超文本傳輸協定安全(HTTPS)是一種使用傳輸層安全(TLS)加密通訊的安全通訊協定。它透過使用 TLS握手過程中交換的TLS證書來建立此安全通道。此伺服器有兩個用途:身份驗證(瞭解您連線 到的遠端方)和隱私(加密)。身份驗證可防止中間人攻擊,隱私可防止攻擊者竊聽和篡改通訊。

TLS(證書)驗證在看到身份驗證的情況下執行,並且允許您確保您已連線到正確的遠端方。驗證 包括兩個單獨的專案:

1. 受信任的證書頒發機構(CA)鏈

2. 主題替代名稱(SAN)或通用名稱(CN)

#### 受信任的CA鏈

要使Expressway-C信任CUCM/IM&P/Unity傳送的證書,它需要能夠建立從該證書到其信任的最頂 級(根)證書頒發機構(CA)的連結。此類連結是將實體證書連結到根CA證書的證書層次結構,稱為 信任鏈。為了能夠驗證這種信任鏈,每個證書包含兩個欄位:頒發者(或「頒發者」)和主體(或 「頒發者」)。

伺服器證書(例如CUCM傳送到Expressway-C的一個證書)在「Subject」(主題)欄位中通常包 含其CN中的完全限定域名(FQDN):

Issuer: DC=lab, DC=vngtp, CN=vngtp-ACTIVE-DIR-CA
Subject: C=BE, ST=Flamish-Brabant, L=Diegem, 0=Cisco, 0U=TAC, CN=cucm.vngtp.lab

CUCM cucm.vngtp.lab的伺服器證書示例。它在Subject欄位的CN屬性中具有FQDN,以及其他屬 性,如Country (C)、State (ST)、Location (L)、...此外,我們還可以看到,伺服器證書由名為 vngtp-ACTIVE-DIR-CA的CA分發(頒發)。

頂級CA(根CA)也可以頒發證書來標識自己。在此根CA證書中,我們可以看到Issuer和Subject具 有相同值:

Issuer: DC=lab, DC=vngtp, CN=vngtp-ACTIVE-DIR-CA
Subject: DC=lab, DC=vngtp, CN=vngtp-ACTIVE-DIR-CA

#### 它是根CA頒發的證書,用於標識自身。

在典型情況下,根CA不會直接頒發伺服器證書。相反,它們會為其他CA頒發證書。此類其他CA稱 為中繼CA。中繼CA反過來可以直接為其他中繼CA頒發伺服器證書或證書。我們可能會遇到這樣的 情況:中間CA 1會發行伺服器憑證,而中間CA 1會從中間CA 2取得憑證,以此類推。直到最後中 間CA直接從根CA獲得其證書:

Server certificate :
 Issuer: DC=lab, DC=vngtp, CN=vngtp-intermediate-CA-1
 Subject: C=BE, ST=Flamish-Brabant, L=Diegem, 0=Cisco, OU=TAC, CN=cucm.vngtp.lab
Intermediate CA 1 certificate :
 Issuer: DC=lab, DC=vngtp, CN=vngtp-intermediate-CA-2
 Subject: DC=lab, DC=vngtp, CN=vngtp-intermediate-CA-1
Intermediate CA 2 certificate :
 Issuer: DC=lab, DC=vngtp, CN=vngtp-intermediate-CA-3
 Subject: DC=lab, DC=vngtp, CN=vngtp-intermediate-CA-2
...
Intermediate CA n certificate :
 Issuer: DC=lab, DC=vngtp, CN=vngtp-ACTIVE-DIR-CA
 Subject: DC=lab, DC=vngtp, CN=vngtp-intermediate-CA-n
Root CA certificate :
 Issuer: DC=lab, DC=vngtp, CN=vngtp-ACTIVE-DIR-CA

現在,為了使Expressway-C信任CUCM傳送的伺服器證書,它需要能夠構建從該伺服器證書一直到 根CA證書的信任鏈。為此,我們需要在Expressway-C的信任儲存中上傳根CA證書,以及所有中間 CA證書(如果有,但根CA不會直接頒發CUCM的伺服器證書,則不存在這種情況)。

注意:雖然頒發者和主題欄位易於以易於閱讀的方式構建信任鏈,但CUCM在證書中不會使用 這些欄位。相反,它使用「X509v3授權金鑰識別符號」和「X509v3主題金鑰識別符號」欄位 來構建信任鏈。這些金鑰包含比使用Subject/Issuer欄位更準確的證書識別符號:可能有2個證 書具有相同的Subject/Issuer欄位,但其中一個證書已過期,還有一個證書仍然有效。它們都 有不同的X509v3主題金鑰識別符號,因此CUCM仍可確定正確的信任鏈。

但根據思科漏洞ID <u>CSCwa12905</u>,Expressway不會出現這種情況,並且無法將兩個不同(例 如自簽名)證書上傳到具有相同公用名(CN)的Expressway信任庫中。對此進行更正的方法是 CA簽名證書或使用不同的通用名稱,或者檢視它是否始終使用相同的證書(可能透過CUCM 14中的重複使用證書功能)。

#### SAN或CN檢查

第1步將簽出信任庫,但擁有由信任庫中的CA簽名的證書的任何人到那時都是有效的。這顯然不夠 。因此,還會進行額外的檢查,以驗證您專門連線的伺服器是否正確。它會根據發出請求的地址來 執行此操作。

在瀏覽器中也會發生相同型別的操作,因此讓我們透過一個示例來瞭解這一點。如果瀏覽到 <u>https://www.cisco.com</u>,您將在輸入的URL旁邊看到一個鎖圖示,表示它是受信任的連線。這基於 CA信任鏈(來自第一部分)以及SAN或CN檢查。如果我們打開證書(透過瀏覽器按一下鎖定圖示 ),您會看到「公用名」(見「頒發給:」欄位)設定為<u>www.cisco.com</u>,並且與我們想要連線的 地址完全對應。這樣可以確保我們連線到正確的伺服器(因為我們信任簽署證書並在分發證書之前 執行驗證的CA)。

ertificate	×		
neral Details Certification Path		cisco	Products and Servi
Certificate Information			
This certificate is intended for the following • Ensures the identity of a remote computer • Proves your identity to a remote computer • 2.16.840.1.113839.0.6.3 • 2.23.140.1.2.2	purpose(s):		
* Refer to the certification authority's statement for	details.		
Issued to: www.cisco.com			
Issued by: HydrantID Server CA O1			
Valid from 2/16/2022 to 2/16/2023			

當我們檢視證書的詳細資訊(尤其是SAN條目)時,我們會看到該詳細資訊與某些其他FQDN相同 :

	ZAUN		
now.	SAUZ		
Field		Value	^
🗊 Cer	tificate Policies	[1]Certificate Policy:	
CRI CRI	Distribution P	[1]CRL Distribution	
🔤 Sub	ject Alternativ	DNS Name=cisco-i	
🗟 Sub	ject Key Identi	b18ceccd49a5dfd74	
🗊 Enh	anced Key Usage	Server Authenticatio	
≣ SC1	f List	v1, adf7befa7cff10c	
Key	Usage	Digital Signature, Ke	
🗊 Thu	imbprint	0dddb6ce30b00bd7	
DNS N DNS N	ame=cisco-image ame=cisco.com	es.cisco.com	^
DNS N DNS N DNS N	ame=www-01.ds ame=www-02.ds ame=www-rtp.ci	sco.com sco.com	
DNS N DNS N DNS N	ame=www.cisco. ame=www.medi ame=www.static	.com afiles-cisco.com -cisco.com	
JNS N	ame=www1.csc	b.com	*
		Edit Properties	Copy to File

例如,這意味著,當我們請求連線到<u>https://www1.cisco.com</u>時,它將顯示為一個安全連線,因為它 包含在SAN條目中。

$tirst$ Cisco - Networking, Cloud, and $\subset$ X +	
$\leftrightarrow \rightarrow C$ $har www1.cisco.com$	
	cisco

但是,當我們不瀏覽<u>https://www.cisco.com</u>而直接瀏覽IP地址(<u>https://72.163.4.161</u>)時,它不會顯示 安全連線,因為它信任簽名的CA但顯示給我們的證書不包含我們用於連線到伺服器的地址 (72.163.4.161)。



在瀏覽器中,您可以繞過此設定,但您可在TLS連線上啟用不允許繞過此設定。因此,您的證書必 須包含遠端方計畫用於連線其的正確CN或SAN名稱。

## 行為變更

MRA服務嚴重依賴於CUCM/IM&P/Unity伺服器的Expressway上的多個HTTPS連線,以正確進行身 份驗證並收集登入客戶端的特定資訊。此通訊通常透過埠8443和6972進行。

#### 低於X14.2.0的版本

在低於X14.2.0的版本中,Expressway-C上處理這些安全HTTPS連線的流量伺服器未驗證遠端端提供的證書。這可能導致中間人攻擊。在MRA配置上,當您需要在Configuration > Unified Communications > Unified CM servers / IM and Presence Service nodes / Unity Connection servers下增加CUCM / IM&P / Unity伺服器時,有一個透過將「TLS驗證模式」配置為「開」進行 TLS證書驗證的選項。配置選項和相關資訊方塊以示例形式顯示,表明它確實驗證了SAN中的 FQDN或IP、證書的有效性以及證書是否由受信任CA簽署。

# CISCO Cisco Expressway-C

S	tatus >	System >	Configuration >	Applications >	Users >	Maintenance >
U	nified C	M servers				You are here: Configuration >
Г	Unified CI	M server looku	p	]		
	Unified CM	publisher addres	s	cucmpub.vngtp.la	ib	
	Username			* administrator		i
	Password			*		(i)
	TLS verify	mode		On v (i)		
	Deploymen	t		Default deploym	ent v (i	
	AES GCM :	support		Off v (i)		
	SIP UPDAT	E for session refr	resh	Off v i		
	ICE Passth	rough support		Off v i		

Save Delete Cancel

此TLS證書驗證檢查僅在發現CUCM/IM&P/Unity伺服器時進行,而不是在MRA登入期間查詢各種伺服器時進行。此配置的第一個缺點是,它只針對您增加的發佈伺服器地址驗證它。它不會驗證訂戶節點上的證書是否已正確設定,因為它從發佈伺服器節點的資料庫中檢索訂戶節點資訊(FQDN或IP)。此配置的第二個缺點是,由於連線資訊可能與在Expressway-C配置中設定的發佈伺服器地址不同,因此通告給MRA客戶端的內容。例如,對於CUCM,在System > Server下,您可以使用IP地址(例如10.48.36.215)向外部通告伺服器,然後MRA客戶端將使用該地址(透過代理的Expressway連線),但是您可以在Expressway-C上使用FQDN cucm.steven.lab增加CUCM。因此

,假設CUCM的tomcat證書包含cucm.steven.lab作為SAN條目而非IP地址,則將「TLS驗證模式」 設定為「開」的發現成功,但來自MRA客戶端的實際通訊可能會以不同的FQDN或IP為目標,從而 無法通過TLS驗證。

X14.2.0及更高版本

從X14.2.0版本開始,Expressway伺服器會對透過流量伺服器發出的每個HTTPS請求執行TLS證書

驗證。這意味著,在發現CUCM/IM&P/Unity節點期間,當「TLS驗證模式」設定為「關閉」時,它 也會執行此操作。驗證失敗時,TLS握手不會完成,請求也會失敗,這可能會導致功能喪失,例如 冗餘或故障轉移問題,或完全登入失敗。此外,如果將「TLS驗證模式」設定為「開」,則它不保 證所有連線都能按照後面的示例所述正常工作。

Expressway向CUCM/IM&P/Unity節點檢查的確切證書顯示在MRA指南部分中。

除了TLS驗證的預設值以外,X14.2中也引入了一個變更,該變更可能會通告密碼清單的其他偏好順 序,這取決於您的升級路徑。這可能會導致在軟體升級後出現意外的TLS連線,因為在升級之前 ,它可能要求來自CUCM(或任何其他具有單獨的ECDSA演算法證書的產品)的Cisco Tomcat或 Cisco CallManager證書,但在升級之後,它要求ECDSA變體(實際上比RSA更安全的密碼變體 )。Cisco Tomcat-ECDSA或Cisco CallManager-ECDSA證書可以由其他CA簽署,也可以僅由自簽 名證書簽署(預設)。

此密碼首選項順序的更改並非總是與您相關,因為它取決於升級路徑,如Expressway X14.2.1 <u>發行</u> <u>版本註釋</u>中所示。簡而言之,您可以從維護>安全>密碼中看到每個密碼清單是否列在「ECDHE-RSA-AES256-GCM-SHA384:」之前。如果沒有,則較新的ECDSA密碼優先於RSA密碼。如果是 ,則您會有RSA的先前行為,其優先順序高於先前行為。

Cipher Preferences - ECDSA Cipher Preference Over RSA ECDSA certificates are preferred over RSA.

# Important The following points lists the various upgrade path(s) that are mandatory for upgrading ciphers. In the following points lists the various upgrade path(s) that are mandatory for upgrading ciphers. When upgrading from version lower than 14.0 to 14.2, the ECDSA would be preferred. If you prefer RSA certificates over ECDSA, then prefix the cipher string with "ECDHE-RSA-AES256-GCM-SHA384:" When upgrading from version equal or higher than 14.0 to 14.2 or higher version, you have appended "ECDHE-RSA-AES256-GCM-SHA384:" to the default Ciphers List to prefer RSA certificates over ECDSA. If you prefer ECDSA certificates over ECDEA-RSA-AES256-GCM-SHA384:" from the cipher string using Web User Interface (Maintenance > Security > Ciphers) or CLI command (xConfiguration Ciphers). Any customer has a fresh install X14.2 image, ECDSA is being preferred. If you prefer RSA certificates over ECDSA, then prefix the cipher string with "ECDHE-RSA-AES256-GCM-SHA384:" using either Web User Interface (Maintenance > Security > Ciphers) or CLI command (xConfiguration Ciphers). Any customer has a fresh install X14.2 image, ECDSA is being preferred. If you prefer RSA certificates over ECDSA, then prefix the cipher string with "ECDHE-RSA-AES256-GCM-SHA384:" using either Web User Interface (Maintenance > Security > Ciphers) or CLI command (xConfiguration Ciphers).

在此場景中TLS驗證失敗的方式有兩種,稍後將詳細介紹:

#### 1. 簽署遠端證書的CA不受信任

a.自簽名證書

b.由未知CA簽名的證書

2. 證書中不包含連線地址(FQDN或IP)

#### 疑難排解案例

以下場景顯示在實驗室環境中出現類似場景,在將Expressway從X14.0.7升級到X14.2後,MRA登 入確實失敗。它們在日誌中有相似之處,但解析度不同。這些日誌只是由診斷日誌記錄(從維護>診 斷>診斷日誌記錄中)收集而來,MRA登入之前開始,MRA登入失敗後停止。尚未為其啟用其他調試 日誌記錄。

#### 1. 簽署遠端證書的CA不受信任

遠端證書可以由未包含在Expressway-C的信任儲存中的CA簽署,也可以是未增加到Expressway-C伺服器的信任儲存中的自簽名證書(實際上也稱為CA)。

在下面的示例中,您可以看到轉到CUCM (10.48.36.215 - cucm.steven.lab)的請求已在埠8443

(200 OK響應)上得到正確處理,但在TFTP連線的埠6972上引發錯誤(502響應)。

#### <#root>

===Success connection on 8443===

2022-07-11T18:55:25.910+02:00 vcsc traffic\_server[18242]: UTCTime="2022-07-11 16:55:25,910" Module="net

```
2022-07-11T18:55:25.917+02:00 vcsc traffic_server[18242]: Event="Request Allowed" Detail="Access allow
2022-07-11T18:55:25.917+02:00 vcsc traffic_server[18242]: UTCTime="2022-07-11 16:55:25,916" Module="netu
2022-07-11T18:55:25.955+02:00 vcsc traffic_server[18242]: UTCTime="2022-07-11 16:55:25,955" Module="netu
2022-07-11T18:55:25.956+02:00 vcsc traffic_server[18242]: UTCTime="2022-07-11 16:55:25,955" Module="netu
```

200

...

===Failed connection on 6972===

2022-07-11T18:55:26.000+02:00 vcsc traffic\_server[18242]: UTCTime="2022-07-11 16:55:26,000" Module="net

2022-07-11T18:55:26.006+02:00 vcsc traffic\_server[18242]: UTCTime="2022-07-11 16:55:26,006" Module="net 2022-07-11T18:55:26.016+02:00 vcsc traffic\_server[18242]: UTCTime="2022-07-11 16:55:26,016" Module="net 2022-07-11T18:55:26.016+02:00 vcsc traffic\_server[18242]: [ET\_NET 0]

WARNING: Core server certificate verification failed for

(cucm.steven.lab).

Action=Terminate Error=self signed certificate server=cucm.steven.lab(10.48.36.215)

depth=0

2022-07-11T18:55:26.016+02:00 vcsc traffic\_server[18242]: [ET\_NET 0]

ERROR: SSL connection failed for

'cucm.steven.lab': error:1416F086:

SSL routines:tls\_process\_server\_certificate:certificate verify failed

```
2022-07-11T18:55:26.024+02:00 vcsc traffic_server[18242]: UTCTime="2022-07-11 16:55:26,024" Module="net
```

502 connect failed

..

「證書驗證失敗」錯誤表明Expressway-C無法驗證TLS握手。其原因顯示在警告行上,因為它指示 自簽名證書。如果深度顯示為0,則其為自簽名證書。當深度高於0時,意味著它具有證書鏈,因此 由未知CA簽名(從Expressway-C的角度來看)。

當我們檢視透過文本日誌中提及的時間戳收集的pcap檔案時,您可以看到CUCM將帶有CN的證書 顯示為cucm-ms.steven.lab(由steven-DC-CA簽名為SAN),並以steven-DC-CA的簽名形式顯示 到埠8443上的Expressway-C。

it was no capture margine partons relation	pry wvreless Tools Help				
(@  🖡 🗄 🕱 🗒 🧣 + 😫 🐺 🗄 📰 🚺	<u> </u>				
5+644Q					
Time	Source	Src port Destination	Deat port Protocol	DSCP VLAN	Length Info
4691 2022-07-11 16:55:25.916680	10.48.36.46	35622 10.48.36.215	8443 TCP	CS0	74 35622 + 8443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=878570435 TSecr=0 WS=128
4692 2022-07-11 16:55:25.916953	10.48.36.215	8443 10.48.36.46	35622 TCP	CS0	74 8443 * 35622 [SYN, ACK] Seq=0 ACk+1 Min+28960 Len+0 MSS+1460 SACK_PERM=1 TSV81+343633230 TSecr+878570435 MS+128
4693 2022-07-11 16:55:25.916973	10.48.36.46	35622 10.48.36.215	8443 TCP	C58	66 35622 + 8443 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=878570435 TSecr=343633230
4694 2022-07-11 16:55:25.917832	10.48.36.46	35622 10.48.36.215	8443 TLSv1.2	CSB	583 Client Hello
4695 2022-07-11 16:55:25.938356	10.48.36.215	8443 10.48.36.46	35622 TLSv1.2	CS0	1514 Server Hello
4696 2022-07-11 16:55:25.938390	10.48.36.46	35622 10.48.36.215	8443 TCP	CS0	66 35622 + 8443 [ACK] Seq=518 ACk=1449 Win=64128 Len=0 TSval=878570457 TSecr=343633251
4697 2022-07-11 16:55:25.938409	10.48.36.215	8443 10.48.36.46	35622 TLSv1.2	CS0	1470 Certificate, Server Key Exchange, Server Hello Done
4698 2022-07-11 16:55:25.938419	10.48.36.46	35622 10.48.36.215	8443 TCP	C58	66 35022 + 8443 [ACK] Seq#S18 ACK+2853 W1n+63488 Len+0 TSval+878570457 TSecr=343633251
4699 2022-07-11 16:55:25.940107	10.48.36.46	35622 10.48.36.215	8443 TLSv1.2	CS0	192 Client Key Exchange, Change Clpher Spec, Encrypted Handshake Message
4700 2022-07-11 16:55:25.943034	10.48.36.215	8443 10.48.36.46	35622 TLSV1.2	CS0	300 New Session Ticket, Change Cipher Spec, Encrypted Handshake Hessage
4701 2022-07-11 16:55:25.943051	10.45.36.46	35622 10.48.36.215	8443 TCP	CS0	66 35622 + 8443 [ACK] Seq+644 ACK+3095 kin+64128 Len+0 TSval+878570461 TSecr+343633256
4702 2022-07-11 16:55:25.943277	10.45.36.46	35622 10.48.36.215	8443 TL5V1.2	CSB	2543 Application Data
4783 2822-87-11 16:55:25.943476	10.48.36.215	8443 10.48.56.46	35622 TCP	C58	66 8445 + 35622 [ACK] 560=3095 ACK=3121 W1N=35072 L0N=0 T5V01=345633256 T50CP=878570462
4707 2022-07-11 16:55:25.954796	10.48.36.215	8443 10.48.36.46	35622 TCP	CS0	1514 8443 + 35622 [ACK] Seq=3095 ACK=3121 W1n=35072 Lem=1448 T5va1=343633268 TSecr=878570462 [TCP segment of a reassemb
4708 2022-07-11 16:55:25.954842	10.45.36.46	35622 10.48.36.215	8443 TCP	C50	66 35922 + 8443 [ACK] SEQ#3121 ACK#4543 WINH64128 LENHE TSV81+878578473 TSECF#343633268
4709 2022-07-11 16:55:25.954061	10.48.36.215	5443 10.45.36.46	35622 TL5V1.2	cse	1257 Application Data
4710 2022-07-11 16:55:25.954873	10.45.36.46	35622 10.48.36.215	8443 TCP	C58	66 35022 + 8443 [ACK] 560=3121 ACK=5734 W1N=63488 Len=0 TSV81=878578473 TSeCF=343633268
4711 2022-07-11 16:55:25.955712	10.48.36.46	35622 10.48.36.215	8443 TLSV1.2	CS0	97 Encrypted Alert
4/12 2022-07-11 10:55:25.955/50	10.48.36.46	35622 10.48.36.215	8443 TCP	C20	66 35922 + 8493 [FIN, ACK] 560+3152 ACK+5/36 Win+64128 LEn+6 TSV81+8/85/04/4 TSECF+343633268
4714 2022-07-11 16:55:25.956123	10.45.36.215	5443 10.45.36.46	35622 TL5V1.2	CS0	97 Encrypted Alert
4/15 2022-07-11 16:55:25.9501/0	10.45.30.46	35622 10.46.36.215	8443 TOP	C58	54 35622 * 8443 [KS1] 56043153 HINKE LENKE
4716 2022-07-11 16:55:25.956252	10.48.50.215	8443 10.48.50.40	55622 TCP	CS0	00 8445 + 55022 [FIN, ACK] 563+5705 ACK+5155 HIN+55072 LEN+0 TSV81+545053209 TSECT+878570474
Certificates (3433 bytes) Certificate Length: 1507 Certificate: 302505/30204C7300302081 version: v3 (2) serialbumber: 0x4500000120560582 > signature (shalkithRSAEncryption)	1242134500000122056058d3 (id 1245608442000200000122	•at-commonName <mark>«cucm-ms.steven.la</mark>	<mark>b</mark> ,id-at-organizationalU	nitName=TAC,id	;at-organizationwame=Cisco,id-at-localitywame=Dieges,id-at-stateOrProvinceWame=Belgius,id-at-countrywa
<pre>Certificates (2423 bytes) Certificate Length: 1507 v crtificate: 3026567300204730030201 v signedCertificate version: v3 (2) s signature (shalithtSekroyption) &gt; issuer: edstequence (0) &gt; validit &gt; subject: rdstequence (0) &gt; subject: rdstequence (0) &gt; subject: rdstequence (0)</pre>	128213450000012205605653 (id 1346605442000200000122	-at-commonName <mark>xcucm-ms,steven.la</mark>	p,id-at-organizationalu	nitWame=TAC,id	:-st-organizationName-Cisco,id-at-localityName=Diegen,id-at-stateOrProvinceName=Belgium,id-at-countryNa
Certificates (1423 bytes) Certificate Length: 1507 Vertificate: 180256/180266/180140201 v SignetCertificate serialsumber: dws6000012056655 > signature (3halithM546cryption > issuer: inds6000rec (0) > vulidity > subject: nds6000rec (0) > subject: nds6000rec (0) > subject: nds6000rec (0) > subject: nds6000rec (0) > subject: nds6000rec (0)	220213450000012205565583 (id 13455685442000200000122	-at-componiane- <mark>cucm-ms.steven.la</mark>	<mark>ə</mark> ,id-at-organizationalu	nitName∗TAC,id	-at-organizationwame-Cisco,id-at-localitywame-Diegem,id-at-stateOrfrovinceWame-Belgium,id-at-countryWa
Certificates (2423 bytes) Certificate Length: 1509 v Certificate: 180265/1802864780930201 v signedcertificate version: v3 (2) serialhumber: devide000012050605 v signeture (shaulthtskenryption > issuer: rdsGeuence (0) > validit > subject: rdsGeuence (0) >	120213450000012205505853 (1d 1348568442000200000122	-at-componiano <mark>«cuca-us,steven.la</mark>	b,id-at-organizational∪	nitName=TAC,id	:-at-organizationName-Cisco,id-at-localityName-Diegen,id-at-stateOrProvinceName-Belgium,id-at-countryNa
Certificates (1423 bytes) Certificate Length: 1507 Vertificate: 180256/180286/1802804/2801201 v Signetcerificate serialsuber: doc6000012056655 > signeture (3halitht545ccryption > issuer: indecember (0) > vulidity > subject: indecember (0) > subject: in	202134500001220560583 (1d 134568844200020000122	-at-componiane- <mark>cute-ns_steven_la</mark>	9,id-ət-organizətionəlu	nitName=TAC,id	:-at-organizationName=Cisco,id-at-localityName=Diegem,id-at-stateOrProvinceName=Belgium,id-at-countryNa
Certificates (2423 bytes) Certificate Length: 1507 v Certificate: 180265/1802864780930301 v signedcertificate version: v3 (2) serialNumber: devide00001206065 v signeture (shaulthtskneryption > issuer: rdsGeuence (0) v subject: rdsGeuence (0) v stemsion (14-ce-krysigg) v Extension (14-ce-krysigg) v Extension (14-ce-krysigg)	22021345000001220560583 (1d 134860844200020000122 1 0	-at-componiano <mark>«cuca-as,steven.la</mark>	9,id-at-organizationalu	nitwame=TAC,id	:-st-organizationName-Cisco,id-at-localityName=Diegen,id-at-stateOrProvinceName=Belgium,id-at-countryNa
Certificates (242) bytes) Certificate Length: 1507 Vertificate: 180256/180286/180204028040280 vignator:162.000 signature (2MalkithStateryption ) issuer: indicemence (0) ) validity ) subject:ValidityInfo vertension: 9 lens ) Extension (14-ce-extropusage) vertension (14-ce-vicyusage) vertension (14-ce-vicyusage) vertension (14-ce-vicyusage)	202134500001220560583 (1d 134560844200020000122 e) ce-subjectAltName)	-at-componiane- <mark>cute-ms_steven_la</mark>	9,id-ət-organizətionəlu	nitwame=TAC,id	-at-organizationName=Cisco,id-at-localityName=Dieges,id-at-stateOrProvinceName=Belgius,id-at-countryNa
Certificates (2423 bytes) Certificate Length: 1507 v Certificate: 180265/180286/180492081 v signedcertificate version: v3 (2) serialNumber: devide00001206065 v signeture (shaulthtskneryption > issuer: rdsGeuence (0) v subject: rdsGeuence (0) v stension (16.c-e.vtsgubge) v Extension (16.c-e.vtsgubge) v Extension (16.c-e.vtsgubget) v Extension (16.c-e.vtsgubget) v Extension (16.c-e.vtsgubget) v Extension (16.c-e.vtsgubget) v Extension (16.c-e.vtsgubget) v Extension (16.c-e.vtsgubget) v Extension (16.c-e.vtsgubget)	22021345000001220560583 (1d 134860844200020000122 ) e) ce-subjectAltName)	-at-componiano <mark>«cuca-us,steven.la</mark>	9,id-at-organizationalu	nitWame=TAC,id	:at-organizationName-Cisco,id-at-localityName=Diegen,id-at-stateOrProvinceName=Belgiun,id-at-countryNa
Certificates (242) bytes) Certificate Length: 580 V certificate: 180285/180286/18028040780930201 v signator:162.04 vision: 18 (2) Signature (2MANLIDHSAGENER) vision: 18 (2) vision: 18 (2) vision: 18 (2) vision: 18 (2) vision: 18 (2) vision: 16	22021345000001220560583 (1d 1345608442000200000122 ) c) c.subjectAltName)	-at-componiane- <mark>cute-ms_steven_la</mark>	9,id-at-organizationalu	nitwame⇒TAC,id	:-at-organizationName=Cisco,id-at-localityName=Dieges,id-at-stateOrProvinceName=Belgius,id-at-countryNa
Certificates (2423 bytes) Certificate Length: 1507 v Certificate: 1802856/1802864780912081 v SignedCertificate version: v3 (2) serialNumber: dxideMethEncryption > issuer: ndSquence (0) > validit > subject: ndSquence (0) > subject: ndSquence (0	220213450000012205605833 (id [346568442000200000122 ] e) ce.subjectAltName)	-st.comconane- <mark>cute-ss.steven.la</mark>	9,id-ət-organizətionəlu	nitWame=TAC,id	:-st-organizationName-Cisco,id-at-localityName=Diegen,id-at-stateOrProvinceName=Belgiun,id-at-countryNa
Certificates (342) bytes) Certificate (ength: 1507 Vertificate: 180256/180266/180930201 viginderrificate version: v3 (2) serialmoter: distributions isser: rodscente: (0) validity validity subject/ublickyinfo vertension (id-ce-extrepuisage) attension (id-ce-extrepuisage) textension (id-ce-extrepuisage) vertension (id	22021345000001220560583 (1d 1345608442000200000122 e) cc.subjectAltName) 0	-at-componianca <mark>cute-ms_steven_la</mark>	9,id-at-organizationalu	nitxame=TAC,id	:-at-organizationName=Cisco,id-at-localityName=Dieges,id-at-stateOrProvinceName=Belgius,id-at-countryNa
Certificates (342) bytes) Certificate (segth: 1807 Vertificate: 1802/86/780286/780010201 vertificate: 1802/86/7802864/78010201 vertificate: 1802/86/78080000000000 ) signature (shallthMSdencryption) ) issue: indiscence (0) ) subject: indiscence (0) vertificate: i	2221345000001220566583 (id 194668442000200000122 e) cc.subjectAltName) 0	-st-componiume= <mark>cute-ss_steven_la</mark>	9,1d-ət-organizətionəlu	nitvame+TAC,id	:=at-organizationName=Cisco,id-at-localityName=Diegem,id-at-stateOrProvinceName=Belgium,id-at-countryNa
Certificates (3423 bytes) Certificate (angth: 1507 v signedcrificate version: 30256/1002046/20010205 signedcrificate version: 30 (2) signedcrificate version: 30 (2) subjective (consistance) validity subjectivelicate (o) subjectivelicate (o) versions (o) subjectivelicate (o	22021345000001220560583 (1d 134560844200020000122 e) cc.subjectAltName)	-at-componiance <mark>cute-as-steven-la</mark>	9,id-at-organizationalu	nitwame=TAC,id	:-at-organizationName=Cisco,id-at-localityName=Dieges,id-at-stateOrProvinceName=Belgium,id-at-countryNa
Certificates (1423 bytes) Certificate uength: 1507 vertificate uength: 1507 vertificate uength: 1507 standownificates) seralbumber: dosdeedel2006055 > signature (bhaluthHSdecryption) > subject: ndsdepunce (0) > subject: ndsdepunc	2021345000001220566583 (id 1345668442000200000122 ° ° ° ° ° ° ° ° ° ° °	-st-componianes <mark>cute-no,steven.la</mark>	9,id-ət-organizətionəlu	nitwame-TAC,id	:-at-organizationwame-Cisco,id-at-localitywame-Diegen,id-at-stateOrProvincewame-Belgium,id-at-countrywa
Certificates (3423 bytes) Certificate (angth: 1507 Vertificate: 180256/180286/180490202 signadcertificate version: v3 (2) serialmoter: doxide000220266658 vignature (domaintaisacryption) vignature (domaintaisacryption) vigna	202134500001220560583 (1d 134560844200020000122 e) cc.subjectAltName) b a tiffer)	-at-componiance <mark>cute-as-steven-la</mark>	9,id-at-organizationalu	nitwame-TAC,id	:-at-organizationName-Cisco,id-at-localityName-Dieges,id-at-stateOrProvinceName-Belgium,id-at-countryNa
Certificates (342) bytes) Certificate (segne: 1507 vertificate: 180256/180286/1801804 signature: 180256/180286/1801804 serialumber: desdeemeiling signature (shallith#Steeryption ) issue: indecemence (0) ) subject: indecemence (0) ) strension (16:-ce-attronged) vertension (16:-ce-attronged) vertension (16:-ce-attronged) vertension (16:-ce-attronged) vertension (16:-ce-attronged) vertension (16:-ce-attronged) ) Extension (16:-ce-attronged) ) Extension (16:-ce-attronged) ) Extension (16:-ce-attronged) ) Extension (16:-ce-attronged)	2021345000001220560583 (id 1345608442000200000122 e) cc-subjectAltname) b tiffar) dtiffar)	-at-componiane- <mark>cute-ns.steven.la</mark>	9,id-ət-organizətionəlu	nitwame-TAC,id	:-at-organizationwame-Cisco,id-at-localitywame-Diegem,id-at-stateOrProvinceWame-Belgium,id-at-countrywa
Certificates (3423 bytes) Certificate (angth: 1507 Vertificate: 180256/180266/180910201 v signdcertificate version: v3 (2) serialmoter: doxide000212856551 vigntver (shalithSiderryption) vigntver (shalithSiderryption	202134500001220560583 (1d 134560844200020000122 c) cc-subjectAltName) 0 0 1(fier) offifer) omfifier)	-at-componiance <mark>cute-ms.steven.la</mark>	9,id-at-organizationalu	nitwame+TAC,id	:-at-organizationName-Cisco,id-at-localityName-Dieges,id-at-stateOrProvinceName-Belgium,id-at-countryNa
Certificates (1423 bytes) Certificate uength: 1507 vertificate length: 1507 vertificate length: 1507 signature (1518 serialumber: docemence (0) > signature (1518 > signature (1518 > signature (1518 > subject: ndisequence (0) > strension (161:-6:-extSplusge) we ceneralumer: dockme (1) odosmer: strens.10 > Extension (161:-6:-extSpluse) > Extension (161:-6:-extSpluse)	2021345000001220560583 (id 1345688442000200000122 e) cc-subjectAltname) b fifier) settfier) settfier) settfier) settfier)	-at-componiane <mark>-cute-ns_steven_la</mark>	9,id-ət-organizətionəlu	nitvane-TAC,id	:-at-organizationwame-Cisco,id-at-localitywame-Diegem,id-at-stateOrProvinceWame-Belgium,id-at-countrywa
Certificates (3423 bytes) Certificate (angth: 1509 V signedcertificate version: 30256/7002046/700910201 vignedcertificate version: 30 (2) serialumber: 60x40000120265655 vignety (SmailthSigneryplin) vignety (SmailthSigneryplin) vignety (SmailthSigneryplin) subject: AndSuperce (0) subject: AndSuperce (0) subje	202134500001220560583 (1d 134560844200020000122 c) cc.subjectAltName) b officr) offi	-at-componiance <mark>cute-as-steven-la</mark>	9,id-at-organizationalu	nitvame-TAC,id	:=at-organizationName=Cisco,id-at-localityName=Dieges,id=at-stateOrProvinceName=Belgium,id=at-countryNa
Certificates (1423 bytes) Certificate (1423 bytes) Certificate (1425 bytes) Certificate (1425 bytes) Sendorrificate serialumber: doc60001206655 signature (1411 bits) signature (1411 bits) signature (1411 bits) subject: radisquence (0) validity validity bitser: radisquence (0) subject: radisquence (0) subject: radisquence (0) bitser: radisquence (0) bitser: radisquence (0) certension (14-ce-extropuisque) bitser: radisquence (0) certension (14-ce-extropuisque) bitser: radisquence (0) certension (14-ce-extropuisque) certension (14-ce-extropuisque) certension (14-ce-extropuisque) bitser: (14-ce-extropuiste) certension (14-ce-extropuiste) bitser: (14-ce-extropuiste) certension (14-ce-extropuiste) bitser: (14-ce-extropuiste) certension (14-ce-extropuiste) bitser: (	<pre>&gt;</pre>	-at-componiane- <mark>cute-ns_steven_la</mark>	9,id-at-organizationalu	nitvane-TAC,id	:-at-organizationwame=Cisco,id-at-localitywame=Oiegem,id-at-stateOrProvinceWame=Belgium,id-at-countrywa
Certificates (3423 bytes) Certificate (angth: 1509 V signedcertificate version: 30256/7002046/70090201 vignedcertificate version: 30 (2) serialumber: 6045000012056655 vignet(content) vignet(content) vignet(content) vignet(content) subjectrublickyInfo vertension (id-ce-extrepusage) vertension (id-ce-extre	22221345000001220566583 (id 2345668442000200000122 cc-subjectAltname) 0 0 0 0 0 0 0 0 0 0 0 0 0	-at-componiance <mark>cute-as-steven-la</mark>	9,1d-ət-organizətionəlu	nitvame-TAC,id	:=at-organizationName=Cisco,id-at-localityName=Dieges,id=at-stateOrProvinceName=Belgium,id=at-countryNa
Certificates (242) bytes) Certificates (242) bytes) Certificate Length: 1507 V signator: 180266/780206728090201 v signature: (380266/780206728090201 signature: (38026000122066555 signature: (38026000122066555 signature: (3802600012066555 v signature: (380260001206655 ) subjectivalicates (380 v stension (16-ce-subjectalitume certainion (16-ce-subjectalitume certainion (16-ce-subjectalitume v deneraliames: (doilane (3) dd0Same: (spo.stener).) v deneraliames: (doilane (3) dd0Same: (spo.stener).) v deneraliames: (doilane (3) dd0Same: (spo.stener).) v deneraliames: (doilane (3) dd0Same: (spo.stener).) v stension (16-ce-subjectave) v stension (16-ce-subjecta	<pre>&gt;</pre>	-at-commonName <mark>-cute-ns_steven_la</mark>	9,id-at-organizationalu	nitwame-TAC,id	-at-organizationwame-Cisco,id-at-localitywame-Diegem,id-at-stateOrProvinceWame-Belgium,id-at-countrywa
Certificates (3423 bytes) Certificate (ength: 1507 Vertificate: 180256/180286/18018026/18018000000000000000000000000000000000	<pre>22021345000001220566583 (id D145668442000200000122 cc-subjectAltName) 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0</pre>	-st.comcontante <mark>cute-str.jteven.la</mark>	9,id-ət-organizətionəlu	nitwame.TAC,id	;∙at-organizationName-Cisco,id-at-localityName=Olegen,id-at-stateOrProvinceName=Belgium,id-at-countryNa
<pre>Certificates (1423 bytes) Certificates (1423 bytes) Certificate Length: 1507 Vertificate: 150256/1202046/23091201 vigenderrificate verden in the subsolution of the subsolution &gt; signature (the subsolution of the subsolution &gt; signature (the subsolution of the subsolution &gt; subject: rddsequence (0) &gt; subject: rddsequence (0) oddsmer: vgcn.subsolution v Generaliance (vgcn.subsolution &gt; ddsmer: vgcn.subsolution &gt; subsolution (14.ce + vgcn.subsolution v Generaliance (vgcn.subsolution ) oddsmer: vgcn.subsolution &gt; subsolution (14.ce + vgcn.subsolution &gt; ddsmer: vgcn.subsolution &gt; subsolution (14.ce + vgcn.subsolution &gt; subsolications (14.ce + vgcn.subsolution &gt; subsolications (14.ce + vgcn.subsolution &gt; subsolications (14.ce + vgcn.subsolution &gt; subsolications (14.ce + vgcn.subsolication &gt; subsolications (14.ce + vgcn.subsolications (14.ce + vgc</pre>	<pre>&gt;</pre>	-at-compositione- <mark>cutin-ms_steven_la</mark>	9,id-at-organizationalu	nitwame-TAC,id	:-at-organizationName=Cisco,id-at-localityName=Olegen,id-at-stateOrProvinceName=Belgiun,id-at-countryNa

# 但是,當我們檢查埠6972上顯示的證書時,您可以看到它是一張自簽名證書(頒發者自身),其中的CN設定為cucm-EC.steven.lab。EC擴展表明這是CUCM上設定的ECDSA證書。

<pre>eth0_diagnostic_logging_tcpdump00_vcsc_2022-07-11;</pre>	_16_55_44.pcap				
File Edit View Go Capture Analyze Statistics Telepho	ny Wireless Tools Help				
🖌 🗏 🖉 🖡 🗁 🎗 🗖 🔍 🗢 🕾 Ŧ 🛓 🚍 📘					
trp.porte=6972					
No. Time	Source	Src port Destination	Dest port Protocol	DSCP VLAN	Length Drfs
4730 2022-07-11 16:55:26.006608	10.48.36.46	31576 10.48.36.215	6972 TCP	CS0	74 31576 + 6972 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=878570525 TSecr=0 WS=128
4731 2022-07-11 16:55:26.006851	10.48.36.215	6972 10.48.36.46	31576 TCP	CS0	74 6972 + 31576 [SYN, ACK] Seq+0 ACk=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=343633320 TSecr=878570525 WS=128
4732 2022-07-11 16:55:26.006892	10.48.36.46	31576 10.48.36.215	6972 TCP	CSB	66 31576 → 6972 [ACK] Seq=1 ACK=1 W1n+64256 Len+0 TSV01=878570525 TSecr=343633320
4734 2022-07-11 16:55:26.016350	10.48.36.215	6972 10.48.36.46	11576 TLSV1.2	C50	305 Calent main 1514 Server Wello, certificate, Server Key Exchance
4735 2022-07-11 16:55:26.016391	10.48.36.46	31576 10.48.36.215	6972 TCP	CSB	66 31576 + 6972 [ACK] Seq=518 Ack=1449 kin=64128 Len=0 TSval=878570535 TSecr=343633329
4736 2022-07-11 16:55:26.016408	10.48.36.215	6972 10.48.36.46	31576 TLSv1.2	CSB	499 Certificate Request, Server Hello Done
4737 2022-07-11 16:55:26.016419	10.48.36.46	31576 10.48.36.215	6972 TCP	cse	66 31576 + 6972 [ACK] Seq=S18 Ack=1882 kin=63744 Len=0 TSval=878578535 TSecr=343633329
4735 2022-07-11 16:55:26.016703	10.48.36.46	31576 10.48.36.215	6972 TL5V1.2	CS0	73 Alert (Level: Fata), Description: Unknown CA) 24 31518 a 6273 [Svil] Sena Nin-Galad Hamad Missian Sary Debust Toyal-Disenant Toyang Missian
4740 2022-07-11 16:55:26.016965	10.48.36.46	31576 10.48.36.215	6972 TCP	<b>CS0</b>	66 31576 + 6972 [ST] SCHE HINDERE LENE CONTRES SKILLER TOTAL STATES
4741 2022-07-11 16:55:26.016984	10.48.36.215	6972 10.48.36.46	31578 TCP	CS0	74 6972 + 31578 [SYN, ACK] Seq+0 Ack+1 Min+28960 Len+0 MSS+1460 SACK_PERM+1 TSval+343633330 TSecr+878570535 MS+128
4742 2022-07-11 16:55:26.017009	10.48.36.46	31578 10.48.36.215	6972 TCP	CS0	66 31578 + 6972 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=878570535 TSecr=343633330
4743 2022-07-11 16:55:26.017101	10.48.36.215	6972 10.48.36.46	31576 TCP	CSB	66 6972 + 31576 [FIN, ACK] Seq=1882 Ack=525 Win=30080 Len=0 TSval=343633330 TSecr=878570535
L 4744 2022-07-11 16:55:26.017121	10.48.36.46	31576 10.48.36.215	6972 TCP	CS8	54 31576 + 6972 [R5T] Seq=S25 WIn+0 Len+0
4745 2022-07-11 16:55:26.01/218	10.48.36.215	51578 10.48.36.215	31578 TLSV1.2	csa	sas Litent Milo Certificate. Server Key Evchange
4747 2022-07-11 16:55:26.024265	10.48.36.46	31578 10.48.36.215	6972 TCP	cse	66 31578 + 6972 [ACK] SequSIB ACK=1449 Win=64128 Len=0 TSval=878570543 TSecr=343633337
4748 2022-07-11 16:55:26.024298	10.48.36.215	6972 10.48.36.46	31578 TLSv1.2	CS0	500 Certificate Request, Server Hello Done
4749 2022-07-11 16:55:26.024309	10.48.36.46	31578 10.48.36.215	6972 TCP	CSB	66 31578 → 6972 [ACK] Seq=518 Ack=1883 Win+63744 Len+0 TSval+878570543 TSecr+343633337
4750 2022-07-11 16:55:26.024548	10.48.36.46	31578 10.48.36.215	6972 TLSv1.2	CSB	73 Alert (Level: Fatal, Description: Unknown CA)
4767 2022-07-11 16:55:26.023159	10,48,36,46	315/0 10.40.30.215	6972 TCP	CSB	06 31376 * 0772 [%3], ALL] SEQUSI ALKAIDOS HIMMANIO LENNA 105 CINA SYSTEMS (STORA) 1261 *343633337 74 31580 * 6072 [%3], Secue Nin-46240 Lenna Missildo Sack PENNA TSystemStored TSystems (Store Nin-128
<					
v fatura fockate i suan					
<pre>content type: manusize (2) version (15 1.2 (2008)) Length: 607 v mandbask Protocol: Certificate mandbask Protocol: Certificate Certificate (2008) Certificate (2008) vertificate (2008) vertificate (2008) vertificate (2008) version: 03 (2) version: 04 (2) version: 04</pre>	202107470ee62271e3d1346 (id 6155946f0a3bf1d :alityName=Diegem,id=at=stateOr itifier) ts) ) ce-subjectAltName)	∙at-localityName+Diegen,id-at-st ProvinceName+Belgium,id-at-commo	ateOrProvinceName=Belgi nName= <mark>Cucm=EC,steven.l</mark>	um,id-at-comm no <mark>n</mark> id-at-organ	nName- <mark>curm-EC;steven.188</mark> ,14-at-organizationalunitName=TAC,14-at-organizationName=Cisco,14-at-countryNa izationalunitName=TAC,14-at-organizationName=Cisco,14-at-countryName=88)
<ul> <li>GeneralName: Jakkamet (2) dkNamet: cucs.steven.lai</li> <li>algorithmidentifler (ecks-with-Swa) Padding: 0</li> <li>encrypted: 3e64e230012543bdsebe745700</li> <li>TLSv1.2 Record Layer: Handshake Protocol: Serv</li> </ul>	b 154) 21171eb489ff03b060cd80d8 ver Key Exchange				

在Cisco Unified OS Administration下的CUCM上,您可以檢視Security > Certificate Management下的現有證書,如下例所示。它顯示了一個不同的tomcat和tomcat-ECDSA證書,其中tomcat是CA簽

名的(並受Expressway-C信任),而tomcat-ECDSA證書是自簽名的,不受Expressway-C信任。

cisco For Cisco	Unified Operating Sys	stem Adn	ninistra	ition			Nerripation Caso Unified OS Administration administration administration
Show * Settings * 1	Security · Software Upgrades · Ser	vices + Help					
Contraction to be						_	
Certificate List							
Generate Self-signe	d 📲 Upload Certificate/Certificate ch	ain 🧃 Dowrs	load CTL 🧯	Generate CSR 🔋 Download CSF			
Status							
0							
43 records found							
Certificate List	(1 - 43 of 43)						Rows per
Find Certificate List wh	ere Certificate v begins with	. v		Find Clear Filter 💠 👄			
Certificate *	Common Name	Type	Key Type	Distribution	Issued By	Expiration	Description
authg	AUTHZ cucm.steven.lab	Self-signed	RSA	cucm.steven.lab	AUTHZ cucm.steven.lab	07/21/2038	Self-signed certificate generated by system
CaliManager	cucm.steven.lab	CA-signed	RSA	cucm.steven.lab	steven-DC-CA	07/13/2022	Centificate Signed by steven-DC-CA
CalManager-ECDSA	cucm-EC.steven.lab	Self-signed	EC.	cucm.steven.lab	cucm-EC.steven.lab	02/18/2024	Self-signed certificate generated by system
CaliManager-trust	steven-DC-CA	Self-signed	RSA	steven-DC-CA	steven-DC-CA	06/01/2025	Signed Certificate
CaliManager-trust	NOMAT-AD-CA	Self-signed	RSA	NOMAT-AD-CA	NOMAT-AD-CA	04/23/2028	Signed Certificate
CaliManager-trust	CAP-RTP-002	Self-signed	RSA	CAP-RTP-002	CAP-RTP-002	10/10/2023	This certificate was used to sign the MIC installed on Cisco endpoint. Presence of this certificate allows the end point to communicate securely with UCM using the MIC when associated with a secure profile.
CaliManager-trust	CAPF-eb2c64d8	Self-signed	RSA	CAPF-eb2c64d8	CAPF-eb2c64d8	04/12/2020	
CaliManager-trust	ms-AD2-CA-1	Self-signed	RSA	ms-AD2-CA-1	ms-AD2-CA-1	09/11/2024	vngtp CA
CallManager-trust	CAP-RTP-001	Self-signed	RSA	CAP-RTP-001	CAP-RTP-001	02/07/2023	This certificate was used to sign the MIC installed on Cisco endpoint. Presence of this certificate allows the end point to communicate securely with UCH using the MIC when associated with a secure profile.
CallManager-trust	NOMAT-CA-10	Self-signed	RSA	NOMAT-CA-10	NOMAT-CA-10	08/11/2027	Signed Certificate
CallManager-trust	Cisco Root CA M2	Self-signed	RSA	Cisco_Root_CA_M2	Cisco_Root_CA_M2	11/12/2037	This certificate was used to sign the MIC installed on Cisco endpoint. Presence of this certificate allows the end point to communicate securely with UCH using the MIC when associated with a secure profile.
CaliManager-trust	ACT2_SUDI_CA	CA-signed	RSA	ACT2_SUDI_CA	Cisco_Root_CA_2048	05/14/2029	This certificate was used to sign the MIC installed on Cisco endpoint. Presence of this certificate allows the end point to communicate securely with UCH using the MIC when associated with a secure profile.
CallManager-trust	vingtp-ACTIVE-DIR-CA	Self-signed	RSA	vngtp-ACTIVE-DIR-CA	vngtp-ACTIVE-DOR-CA	02/10/2024	VNGTP-CA
CaliManager-trust	Cisco_Root_CA_2048	Self-signed	RSA	Cisco_Root_CA_2048	Cisco_Root_CA_2048	05/14/2029	This certificate was used to sign the MIC installed on Cisco endpoint. Presence of this certificate allows the end point to communicate securely with UCH using the MIC when associated with a secure profile.
CaliManager-trust	Cisco Manufacturing CA	CA-signed	RSA	Cisco_Manufacturing_CA	Cisco_Root_CA_2048	05/14/2029	This certificate was used to sign the MIC installed on Cisco endpoint. Presence of this certificate allows the end point to communicate securely with UCH using the MIC when associated with a secure profile.
CaliManager-trust	Cisco Hanufacturing CA SHA2	CA-signed	RSA	Cisco_Manufacturing_CA_SHA2	CISCO_ROOT_CA_M2	11/12/2037	This certificate was used to sign the MIC installed on Cisco endpoint. Presence of this certificate allows the end point to communicate securely with UCM using the MIC when associated with a secure profile.
CalManager-trust	dccomics-wonderwoman-ca	Self-signed	RSA	docomics-wonderwoman-ca	dccomics-WONDERWOMAN-CA	09/19/2037	CA-dvanturn
Calimanager-trust	CAPT-0104210c	Self-signed	RSA	CAPF-6164210c	CAPF-6164210c	07/12/2025	foll-sized cettificate execution by notem-
CARE-Invel	C40-870-003	Ser-signed	REA	CAD 875-003	C40-870-003	10/10/2023	perception concerning generation by system.
CAREADIN	CARE ADDIE AND	Cold signed	BEA.	CARE about the	C105-sh246448	04/13/2023	The definition was using the rac maximum of calco expone. Hearing of the definition of the point of calling the rac when associated with a second prime.
CARE-trust	C49-878-001	Self-signed	REA	CAD STD 001	C49-879-001	02/07/2023	This cartificate was used to size the MIC installed on Cisco endocies. Researce of this cartificate allows the and point to communicate securate with UCM using the MIC when approximated with a secure profile
CARE-trust	Cisco Root CA M2	Self-sinned	PSA .	Cisco Boot CA M2	Circo Boot CA M2	11/12/2017	This certificate was used to spin the maximum on Case exponent Presence of this certificate allows the and note to communicate security with UCH using the Heal III while a service or this certificate was used on the UCH while the UCH when associated with a service or this certificate.
CARE-trust	ACT2 SUDI CA	Chairmed	PSA	ACT2 SUDL CA	Citro Root CA 2045	05/14/2029	This particular was used to size the MIC installed on Cisco and/oriot. Despace of this particular allows the and point to communicate security with ICM using the MIC when associated with a secure config
CAPE-trust	Cisco Root CA 2048	Self-signed	RSA	Cisco Boot CA 2048	Cisco Root CA 2048	05/14/2029	This certificate was used to sign the MIC installed on Cisco engineer. Presence of this certificate allows the end point to communicate securely with UCH using the MIC when associated with a secure profile.
CAPF-trust	Cisco Manufacturing CA	CA-signed	RSA	Cisco Manufacturing CA	Cisco Root CA 2048	05/14/2029	This certificate was used to sign the MIC installed on Cisco endopint. Presence of this certificate allows the end point to communicate securely with UCH using the MIC when associated with a secure profile.
CAPF-trust	Cisco Manufacturing CA SHA2	CA-signed	RSA	Cisco Manufacturing CA SHA2	Cisco Root CA M2	11/12/2037	This certificate was used to sign the MIC installed on Cisco endpoint. Presence of this certificate allows the end point to communicate securely with UCM using the MIC when associated with a secure profile.
CAPF-trust	CAPF-616421bc	Self-signed	RSA	CAPF-616421bc	CAPF-616421bc	07/12/2025	
ipsec	cucm.steven.lab	Self-signed	RSA	cucm.steven.lab	cuom.steven.lab	07/12/2025	Self-signed certificate generated by system
ipsec-trust	cucm.steven.lab	Self-signed	RSA	cucm.steven.lab	cuom.steven.lab	07/12/2025	Trust Certificate
ITLRecovery	ITLRECOVERY_cuom.steven.lab	Self-signed	RSA	cucm.steven.lab	ITURECOVERY_cuom.steven.lab	02/14/2039	Self-signed certificate generated by system
torncat	cuom.steven.lab	CA-signed	RSA	cucm.steven.lab	steven-DC-CA	07/10/2024	Certificate Signed by steven-DC-CA
tomcat-ECDSA	cucm-EC.steven.lab	CSR Only	EC	cucm.steven.lab			
tomcat-ECDSA	cucm-EC.steven.lab	Self-signed	EC .	cucm.steven.lab	cucm-EC.steven.lab	07/25/2023	Self-signed certificate generated by system
tomcat-trust	steven-DC-CA	Self-signed	RSA	steven-DC-CA	steven-DC-CA	06/01/2025	Trust Certificate
tomcat-trust	NOMAT-AD-CA	Self-signed	RSA	NOMAT-AD-CA	NOMAT-AD-CA	04/23/2028	Signed Certificate
tomcat-trust	cucm-EC.steven.lab	Self-signed	EC	cucm.steven.lab	cucm-EC.steven.lab	07/25/2023	Trust Certificate
tomcat-trust	cucm.steven.lab	CA-signed	RSA	cucm.steven.lab	steven-DC-CA	07/10/2024	Trust Certificate
tomcat-trust	cups-EC.steven.lab	Self-signed	BC .	cups.steven.lab	cups-EC.steven.lab	07/25/2023	Trust Gettilicate
tomcat-trust	NOMAT-CA-10	Self-signed	RSA	NOMAT-CA-10	NOMAT-CA-10	08/11/2027	Signed Certificate
tomcat-trust	yngtp-Ac Trye-olR-CA	Ser-signed	RSA	vngtp-ACTIVE-DIR-CA	vngtp-ACTEVE-OOR-CA	02/10/2024	Trut Certificate
tomcat-crust	OCCOMICS-WONDERWOMAN-CA	Ser-signed	R5A	occomics-wonderwoman-ca	occomics-wondERWOMAN-CA	09/19/2037	CA BYING
	Sector Contractor	Den Angel	nan	Constitution of the second	CONTRACTOR LAND	J178474923	an shua an na shua shua shua shua shua shua shua shu

2. 證書中不包含連線地址(FQDN或IP)

除了信任儲存之外,流量伺服器還驗證MRA客戶端向哪個連線地址發出請求。例如,如果您在 CUCM上的System > Server下設定了CUCM的IP地址(10.48.36.215),則Expressway-C會將此情況 通告給客戶端,並且來自客戶端(透過Expressway-C代理)的後續請求會定向到此地址。

當伺服器憑證中不包含該特定連線位址時,TLS驗證也會失敗,並且擲回502錯誤,導致例如 MRA登入失敗。

<#root>

```
2022-07-11T19:49:01.472+02:00 vcsc traffic_server[3916]: UTCTime="2022-07-11 17:49:01,472" Module="netw
HTTPMSG:
|GET http://vcs_control.steven.lab:8443/c3RldmVuLmxhYi9odHRwcy8xMC400C4zNi4yMTUvODQ0Mw/cucm-uds/user/em
...
2022-07-11T19:49:01.478+02:00 vcsc traffic_server[3916]: UTCTime="2022-07-11 17:49:01,478" Module="netw
2022-07-11T19:49:01.478+02:00 vcsc traffic_server[3916]: UTCTime="2022-07-11 17:49:01,478" Module="netw
HTTPMSG:
|GET /cucm-uds/user/emusk/devices?max=100 HTTP/1.1
...
2022-07-11T19:49:01.491+02:00 vcsc traffic_server[3916]: [ET_NET 2]
```

WARNING: SNI (

10.48.36.215

) not in certificate

. Action=Terminate server=10.48.36.215(10.48.36.215) 2022-07-11T19:49:01.491+02:00 vcsc traffic\_server[3916]: [ET\_NET 2]

ERROR: SSL connection failed for

'10.48.36.215': error:1416F086:

#### SSL routines:tls\_process\_server\_certificate:certificate verify failed

其中c3RldmVuLmxhYi9odHRwcy8xMC40OC4zNi4yMTUvODQ0Mw轉換(base64)為 steven.lab/https/10.48.36.215/8443,這表示它必須連線至10.48.36.215作為連線地址,而不是連線 至cucm.steven.lab。如資料包捕獲所示,CUCM tomcat證書不包含SAN中的IP地址,因此會引發錯 誤。

## 如何輕鬆驗證

您可以驗證是否透過後續步驟輕鬆實現此行為更改:

1. 在Expressway E和Expressway C伺服器上啟動診斷日誌記錄(最好啟用TCPDumps),方法是 透過維護>診斷>診斷日誌記錄(如果是集群,則僅從主節點啟動即可)

2. 在升級後嘗試MRA登入或測試中斷的功能

 等待直到失敗,然後停止Expressway E和Expressway C伺服器上的診斷日誌記錄(如果是群集 ,請確保分別從群集的每個節點收集日誌)

4. 上傳和分析<u>合作解決方案分析器工具</u>上的日誌

5. 如果您遇到問題, 它會針對每個受影響的伺服器挑選與此變更相關的最新警告與錯誤訊息

Â	Collaboration Solutions Analyze CISCO Log Analyzer	Mer Dreview Outc Me	? 0
Tools >	Diagnostic overview	Issues found No Issue Not applicable Missing Information Potential problem	
Log Acalyter T Ubbead Basentites II Acalytes	Q. Search         Image: Category A         Image: Category A	Table To the problem of t	Intguration Intguration Intguration Integration Integration

n Home	Collaboration Solutions Analyzer	Preview O UTC	<b>14</b> ? Ö
Tools	Diagnostic overview		
Toos	serch Result Category ^ Configuration (39) Defects only (1)	<pre>set for a loss is to applicable is</pre>	Contguration Contguration Contguration Contguration MINA discovering
			*

SNI診斷簽名

# 解決方案

長期的解決方案是確保TLS驗證運行良好。要執行的動作取決於顯示的警告訊息。

當您看到WARNING: Core server certificate verification failed for (<server-FQDN-or-IP>)時。 Action=Terminate Error=self signed certificate server=cucm.steven.lab(10.48.36.215) depth=x消息 ,則需要相應地更新Expressway-C伺服器上的信任庫。使用簽名此證書的CA鏈(深度> 0)或使用 維護>安全>受信任CA證書中的自簽名證書(深度= 0)。請確定在叢集的每個伺服器上執行此動作 。另一個選項是透過Expressway-C信任儲存上的已知CA對遠端證書進行簽名。

◆ 注意:Expressway不允許將兩個不同的(例如自簽名)證書上傳到Expressway的信任儲存中 ,這些證書與思科漏洞ID <u>CSCwa12905</u>具有相同公用名(CN)。要更正此問題,請轉到CA簽名 的證書或將CUCM升級到版本14,您可以在此為Tomcat和CallManager重複使用相同的(自 簽名)證書。

觀察警告: SNI (<server-FQDN-or-IP>) not in certificate 消息時,該消息表示此伺服器FQDN或 IP未包含在已顯示的證書中。您可以調整證書以包括此資訊,也可以修改配置(例如,在System > Server上的CUCM上修改為伺服器證書中包含的內容),然後刷新Expressway-C伺服器上的配置 ,以便考慮該配置。

## 相關資訊

短期解決方案是應用所記錄的解決方法,以回退至X14.2.0之前的運作方式。您可以透過 Expressway-C伺服器節點上的CLI使用新引入的命令來執行此操作: xConfiguration EdgeConfigServer VerifyOriginServer: Off

lt

#### 關於此翻譯

思科已使用電腦和人工技術翻譯本文件,讓全世界的使用者能夠以自己的語言理解支援內容。請注 意,即使是最佳機器翻譯,也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準 確度概不負責,並建議一律查看原始英文文件(提供連結)。