排除MRA服務的Expressway流量伺服器證書驗證故障

目錄

簡介

本文檔介紹與思科漏洞ID CSCwc69661或思科漏洞ID CSCwa25108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：

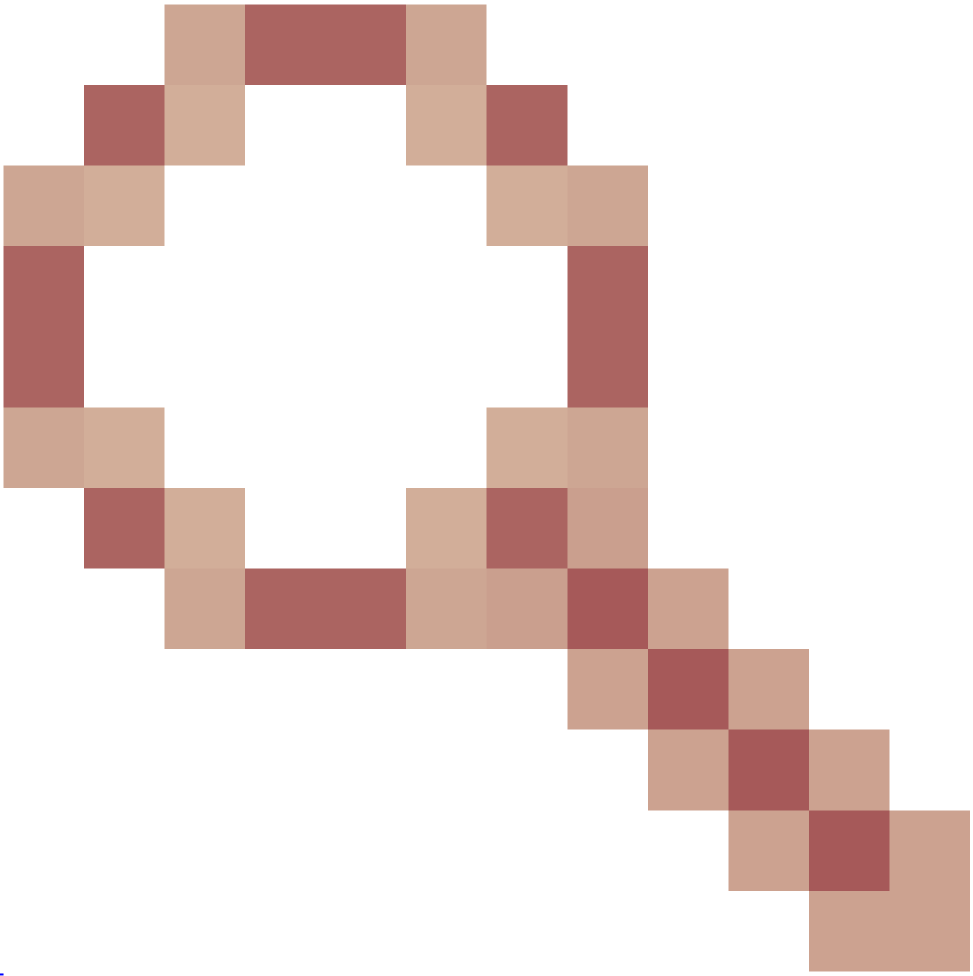
- Expressway基本配置
- MRA基本配置

採用元件

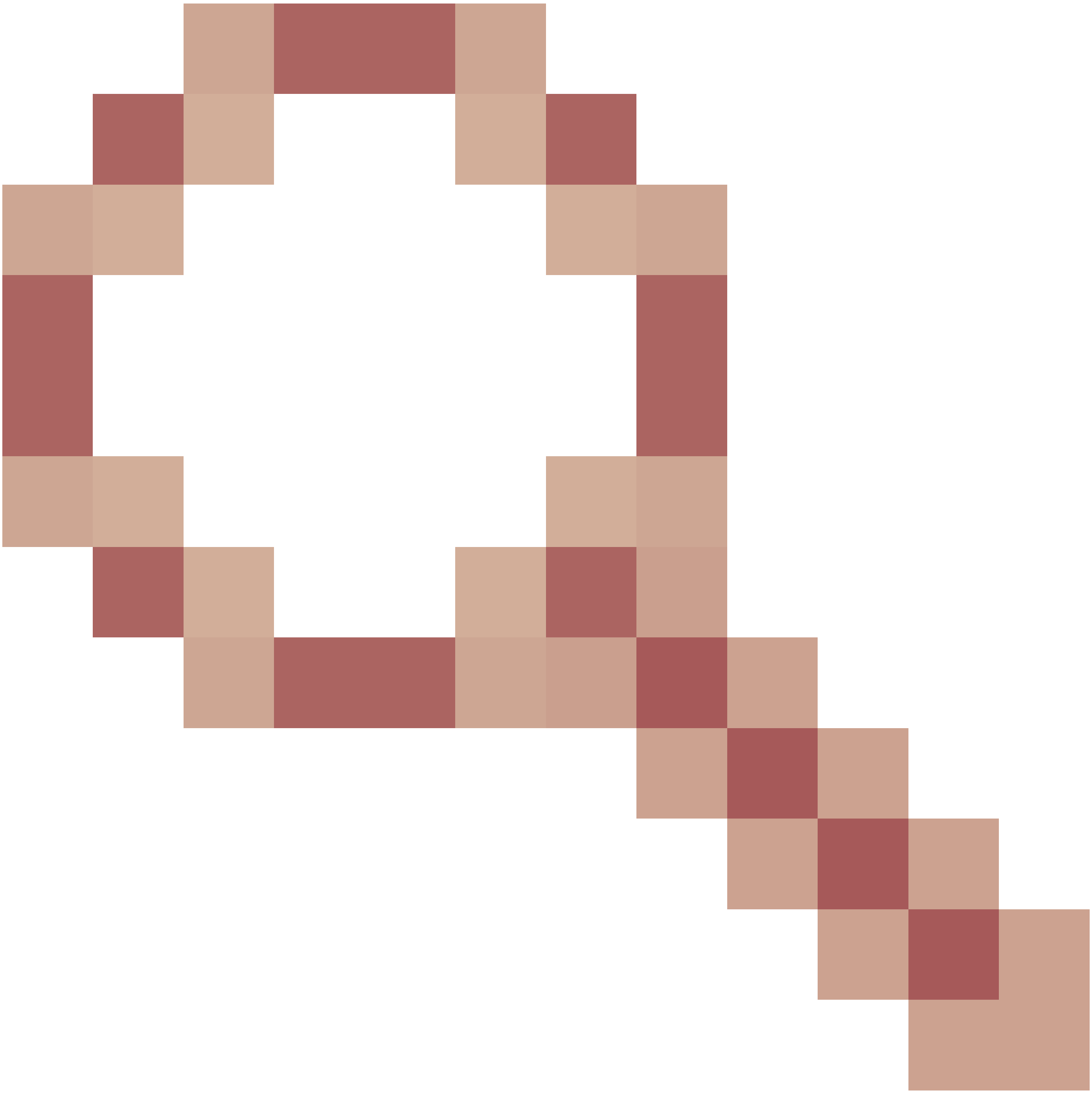
本文檔中的資訊基於X14.2及更高版本上的Cisco Expressway。

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。

背景資訊



透過思科漏洞ID CSCwc69661
或思科漏洞ID CSCwa25108



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, O=Cisco, OU=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, O=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
```

```
    Subject: DC=lab, DC=vngtp, CN=vngtp-ACTIVE-DIR-C
```

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）。

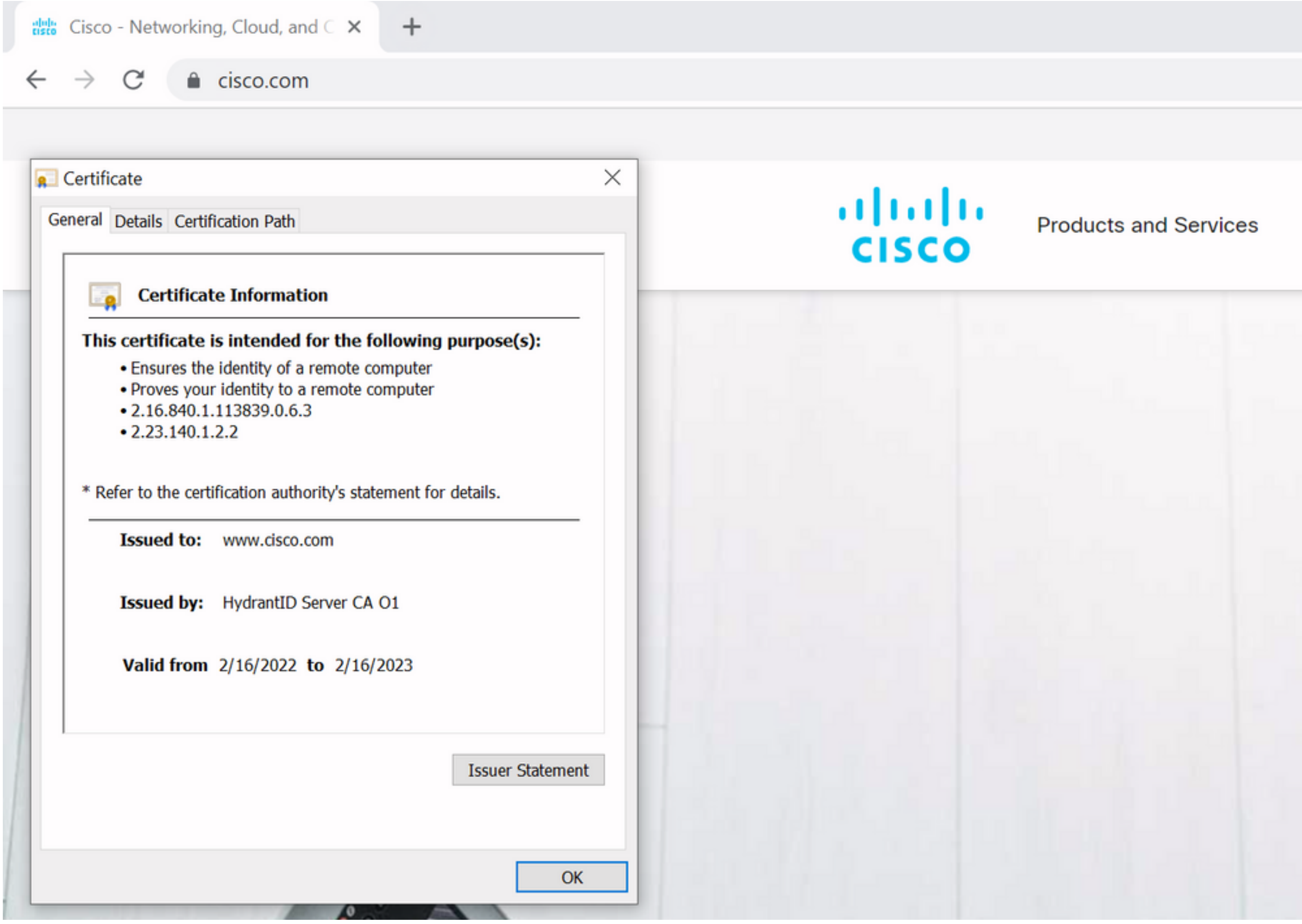
注意：雖然頒發者和主題欄位易於以易於閱讀的方式構建信任鏈，但CUCM在證書中不會使用這些欄位。相反，它使用「X509v3授權金鑰識別符號」和「X509v3主題金鑰識別符號」欄位來構建信任鏈。這些金鑰包含比使用Subject/Issuer欄位更準確的證書識別符號：可能有2個證書具有相同的Subject/Issuer欄位，但其中一個證書已過期，還有一個證書仍然有效。它們都有不同的X509v3主題金鑰識別符號，因此CUCM仍可確定正確的信任鏈。

但根據思科漏洞ID CSCwa12905，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https://www.cisco.com，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www.cisco.com，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）。



Certificate Information

This certificate is intended for the following purpose(s):

- 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

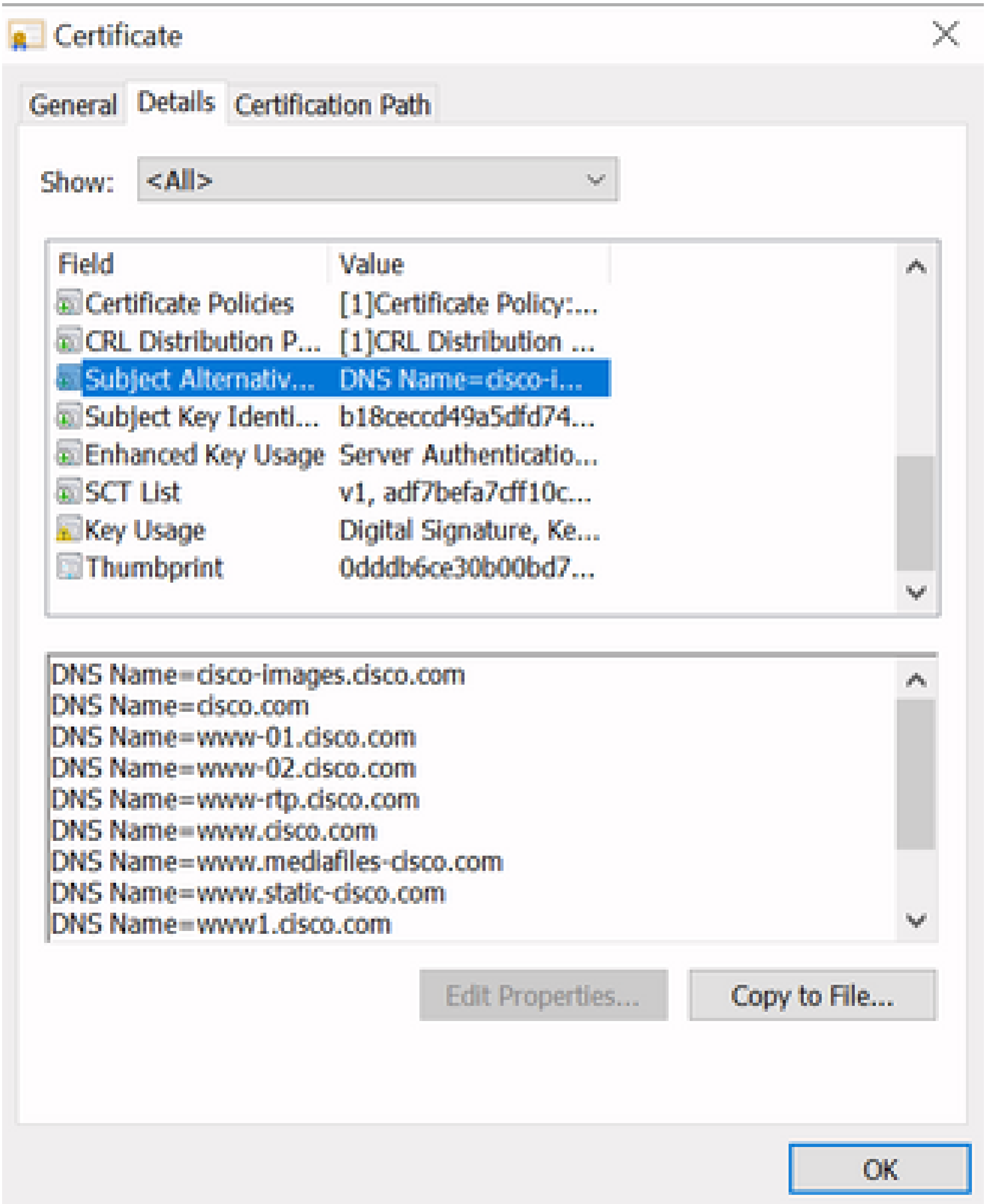
* Refer to the certification authority's statement for details.

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：

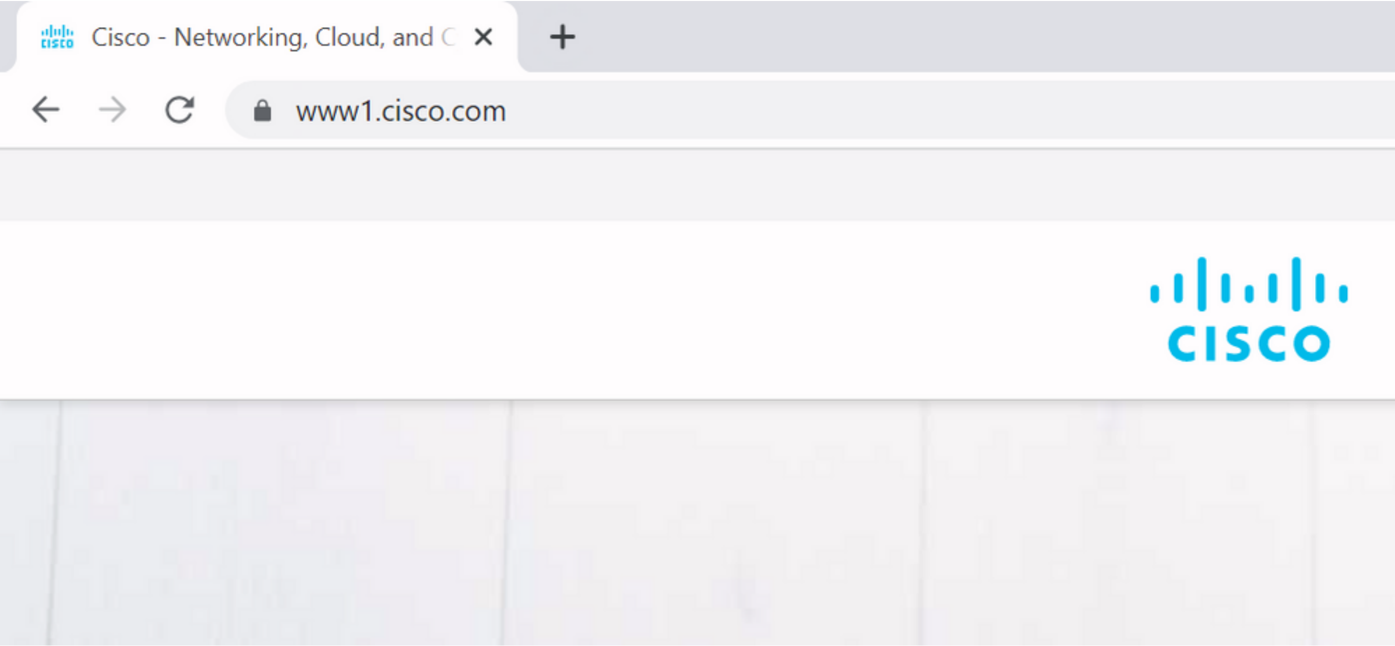


Show: <All>

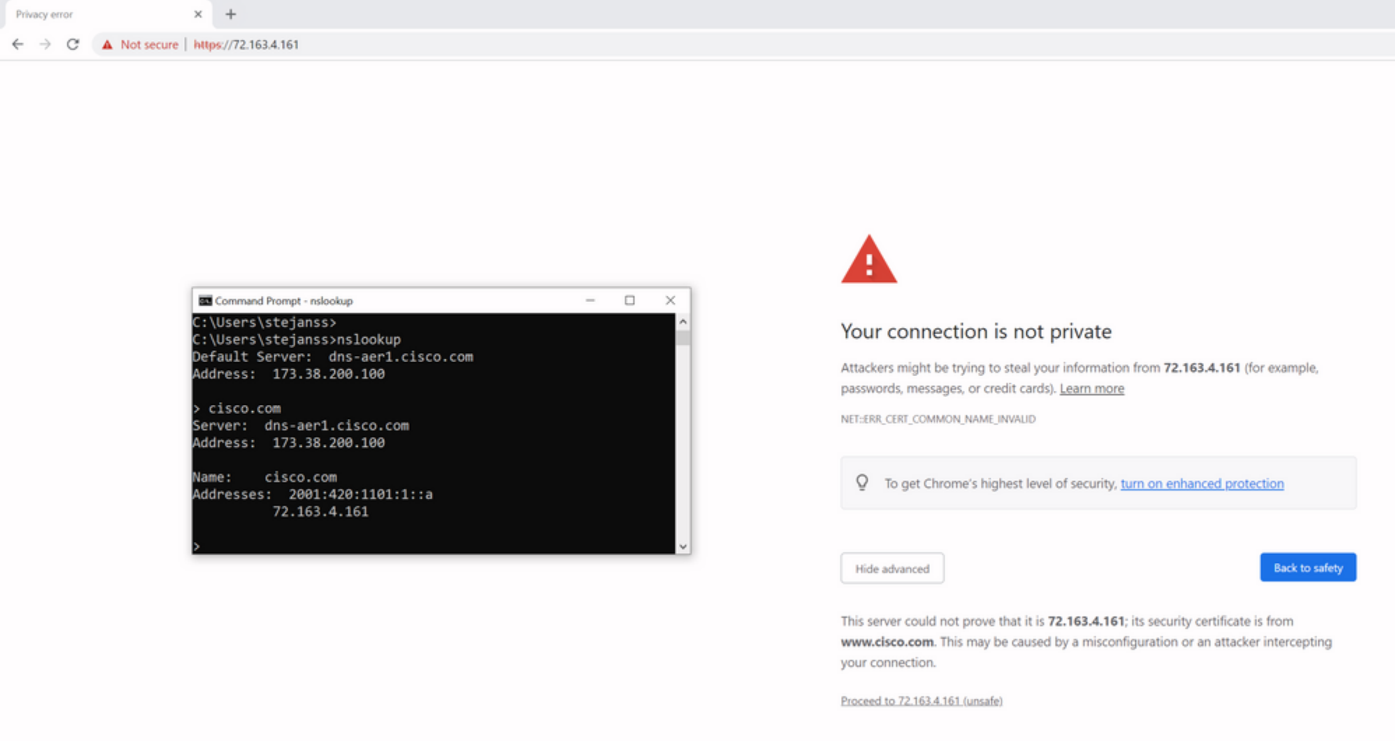
Field	Value
Certificate Policies	[1]Certificate Policy:...
CRL Distribution P...	[1]CRL Distribution ...
Subject Alternativ...	DNS Name=cisco-i...
Subject Key Identi...	b18ceccd49a5dfd74...
Enhanced Key Usage	Server Authenticatio...
SCT List	v1, adf7befa7cff10c...
Key Usage	Digital Signature, Ke...
Thumbprint	0dddb6ce30b00bd7...

```
DNS Name=cisco-images.cisco.com
DNS Name=cisco.com
DNS Name=www-01.cisco.com
DNS Name=www-02.cisco.com
DNS Name=www-rtp.cisco.com
DNS Name=www.cisco.com
DNS Name=www.mediafiles-cisco.com
DNS Name=www.static-cisco.com
DNS Name=www1.cisco.com
```

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



但是，當我們不瀏覽https://www.cisco.com而直接瀏覽IP地址(https://72.163.4.161)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)。



```
C:\Users\stejanss>
C:\Users\stejanss>nslookup
Default Server:  dns-aer1.cisco.com
Address:  173.38.200.100

> cisco.com
Server:  dns-aer1.cisco.com
Address:  173.38.200.100

Name:    cisco.com
Addresses:  2001:420:1101:1::a
          72.163.4.161

>
```

Your connection is not private

Attackers might be trying to steal your information from **72.163.4.161** (for example, passwords, messages, or credit cards). Learn more

NET::ERR_CERT_COMMON_NAME_INVALID

To get Chrome's highest level of security, turn on enhanced protection

This server could not prove that it is **72.163.4.161**; its security certificate is from **www.cisco.com**. This may be caused by a misconfiguration or an attacker intercepting your connection.

Proceed to 72.163.4.161 (unsafe)

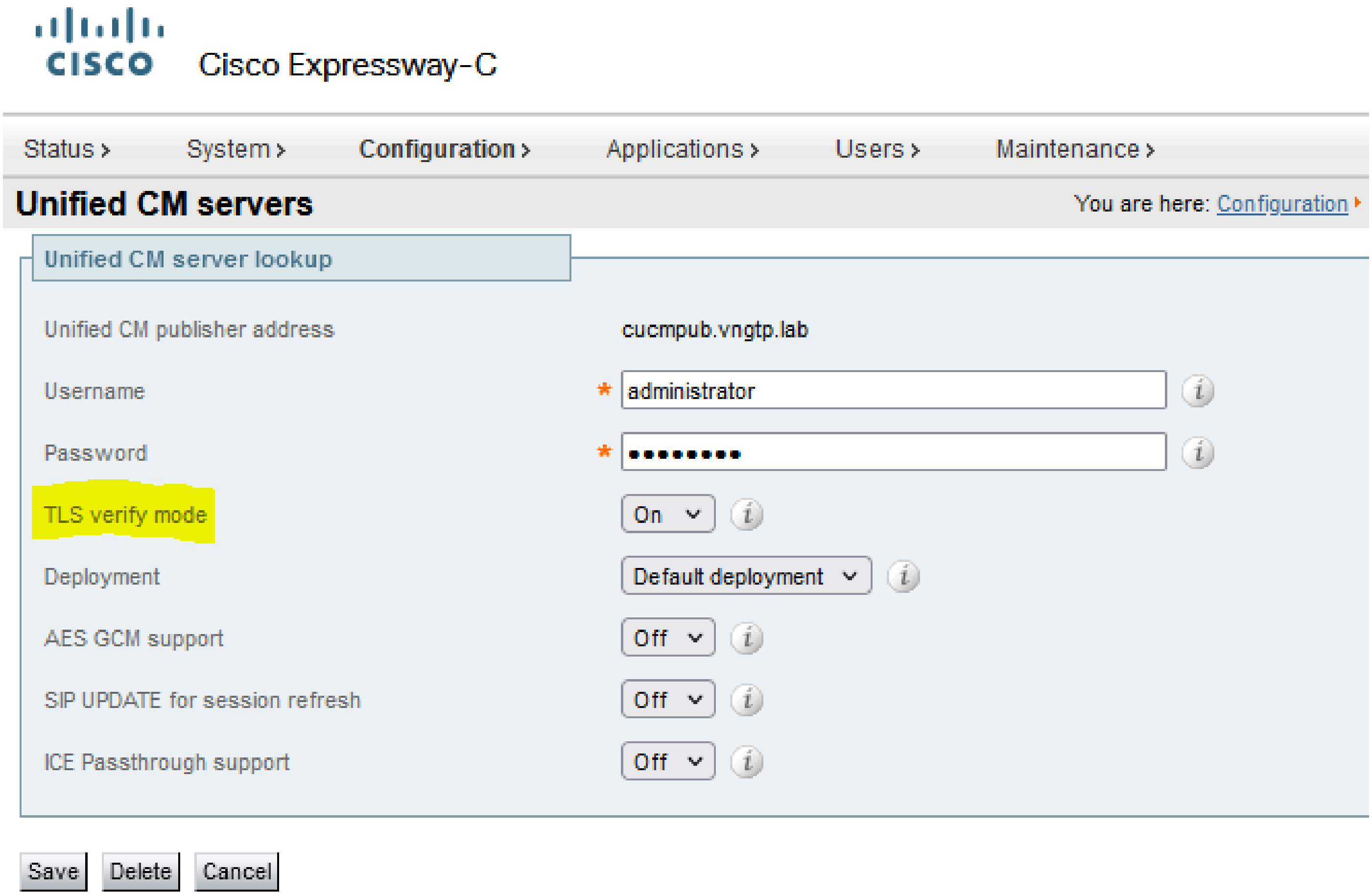
在瀏覽器中，您可以繞過此設定，但您可在TLS連線上啟用不允許繞過此設定。因此，您的證書必須包含遠端方計畫用於連線其的正確CN或SAN名稱。

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 Expressway-C
Status > System > Configuration > Applications > Users > Maintenance >
You are here: Configuration ▸
Save Delete Cancel

Unified CM servers

Unified CM server lookup

Unified CM publisher address	cucmpub.vngtp.lab
Username	* administrator
Password	* ●●●●●●●●●
TLS verify mode	On
Deployment	Default deployment
AES GCM support	Off
SIP UPDATE for session refresh	Off
ICE Passthrough support	Off

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

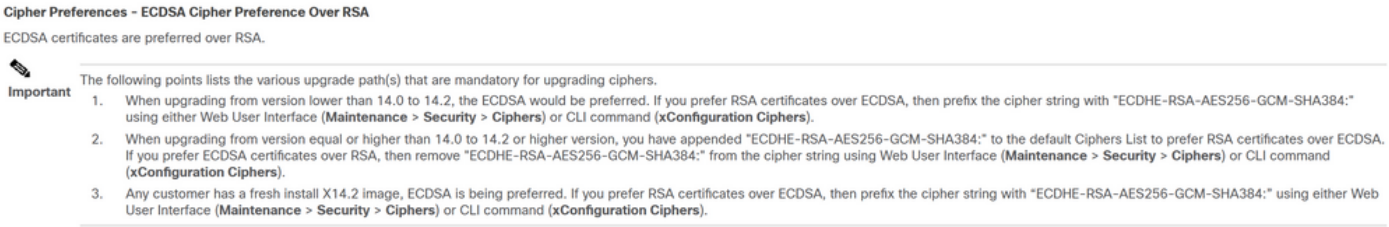
從X14.2.0版本開始，Expressway伺服器會對透過流量伺服器發出的每個HTTPS請求執行TLS證書

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 發行版本註釋中所示。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.

1. 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:" using either Web User Interface (**Maintenance** > **Security** > **Ciphers**) or CLI command (**xConfiguration Ciphers**).
2. 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 RSA, then remove "ECDHE-RSA-AES256-GCM-SHA384:" from the cipher string using Web User Interface (**Maintenance** > **Security** > **Ciphers**) or CLI command (**xConfiguration Ciphers**).
3. 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

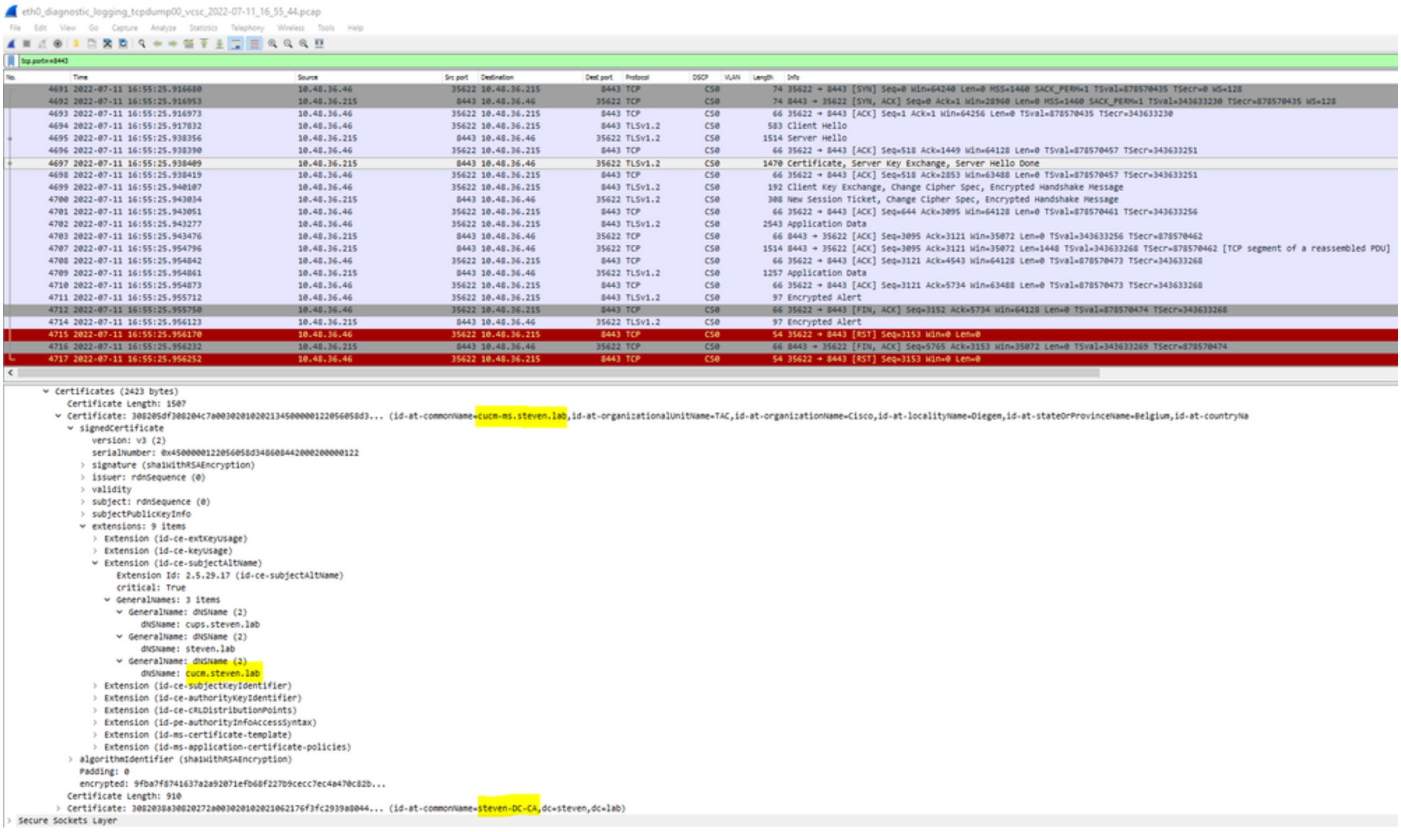
（200 OK響應）上得到正確處理，但在TFTP連線的埠6972上引發錯誤（502響應）。

<#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="netw

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

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="netw

2022-07-11T18:55:26.006+02:00 vcsc traffic_server[18242]: UTCTime="2022-07-11 16:55:26,006" Module="netw
2022-07-11T18:55:26.016+02:00 vcsc traffic_server[18242]: UTCTime="2022-07-11 16:55:26,016" Module="netw
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="netw

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。

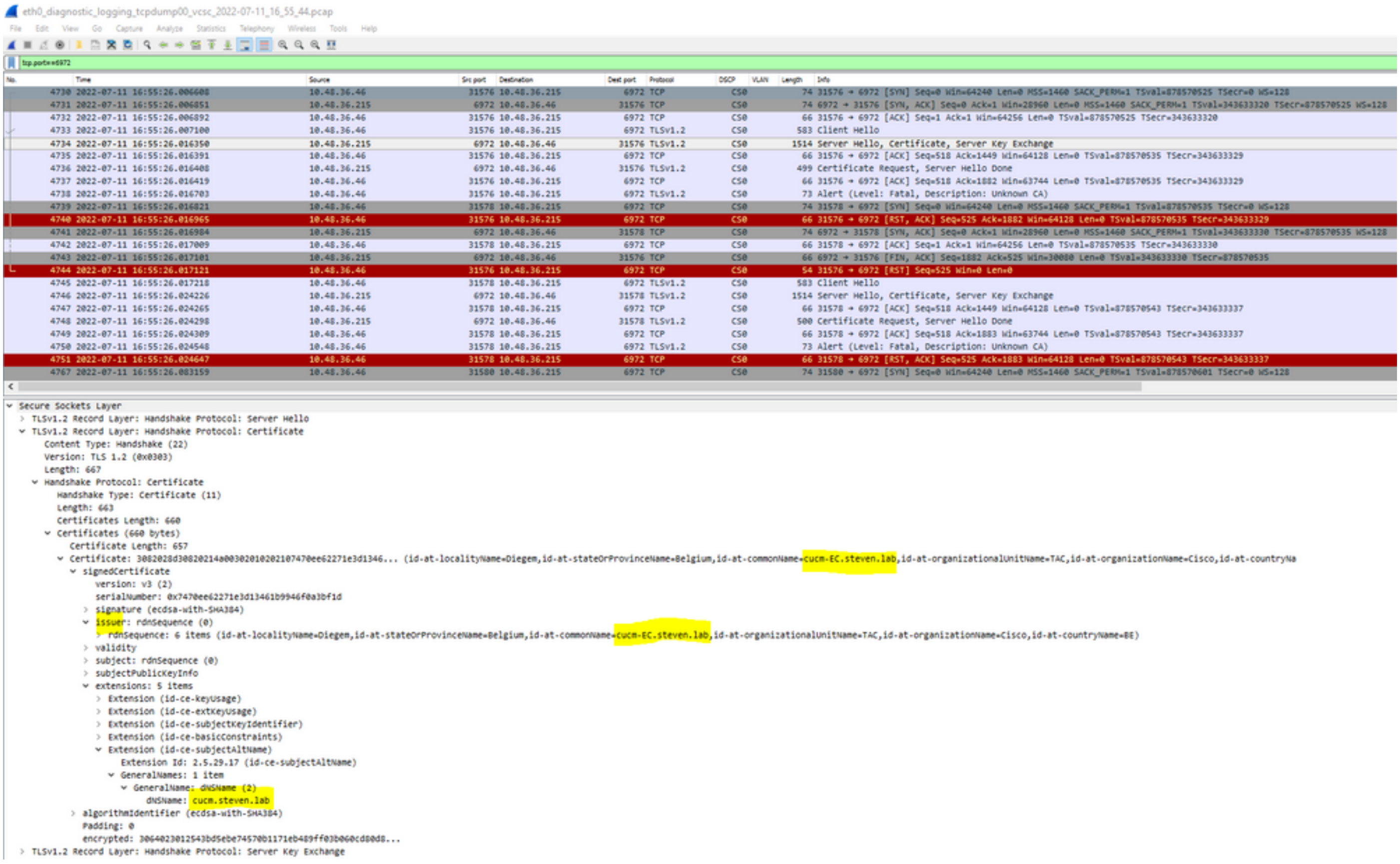


```
tcp.port==8443
```

```
No.   Time                        Source        Src port Destination  Dest 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 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=343633230 TSecr=878570435 WS=128
 4693 2022-07-11 16:55:25.916973  10.48.36.46     35622 10.48.36.215     8443 TCP      CS0          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  CS0         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      CS0          66 35622 → 8443 [ACK] Seq=518 Ack=2853 Win=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 Cipher 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         308 New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
 4701 2022-07-11 16:55:25.943051  10.48.36.46     35622 10.48.36.215     8443 TCP      CS0          66 35622 → 8443 [ACK] Seq=644 Ack=3095 Win=64128 Len=0 TSval=878570461 TSecr=343633256
 4702 2022-07-11 16:55:25.943277  10.48.36.46     35622 10.48.36.215     8443 TLSv1.2  CS0        2543 Application Data
 4703 2022-07-11 16:55:25.943476  10.48.36.215     8443 10.48.36.46     35622 TCP      CS0          66 8443 → 35622 [ACK] Seq=3095 Ack=3121 Win=35072 Len=0 TSval=343633256 TSecr=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 Win=35072 Len=1448 TSval=343633268 TSecr=878570462 [TCP segment of a reassembled PDU]
 4708 2022-07-11 16:55:25.954842  10.48.36.46     35622 10.48.36.215     8443 TCP      CS0          66 35622 → 8443 [ACK] Seq=3121 Ack=4543 Win=64128 Len=0 TSval=878570473 TSecr=343633268
 4709 2022-07-11 16:55:25.954861  10.48.36.215     8443 10.48.36.46     35622 TLSv1.2  CS0        1257 Application Data
 4710 2022-07-11 16:55:25.954873  10.48.36.46     35622 10.48.36.215     8443 TCP      CS0          66 35622 → 8443 [ACK] Seq=3121 Ack=5734 Win=63488 Len=0 TSval=878570473 TSecr=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
 4712 2022-07-11 16:55:25.955750  10.48.36.46     35622 10.48.36.215     8443 TCP      CS0          66 35622 → 8443 [FIN, ACK] Seq=3152 Ack=5734 Win=64128 Len=0 TSval=878570474 TSecr=343633268
 4714 2022-07-11 16:55:25.956123  10.48.36.215     8443 10.48.36.46     35622 TLSv1.2  CS0          97 Encrypted Alert
 4715 2022-07-11 16:55:25.956170  10.48.36.46     35622 10.48.36.215     8443 TCP      CS0          54 35622 → 8443 [RST] Seq=3153 Win=0 Len=0
 4716 2022-07-11 16:55:25.956232  10.48.36.215     8443 10.48.36.46     35622 TCP      CS0          66 8443 → 35622 [FIN, ACK] Seq=5765 Ack=3153 Win=35072 Len=0 TSval=343633269 TSecr=878570474
 4717 2022-07-11 16:55:25.956252  10.48.36.46     35622 10.48.36.215     8443 TCP      CS0          54 35622 → 8443 [RST] Seq=3153 Win=0 Len=0
```

```
    ˅ Certificates (2423 bytes)
        Certificate Length: 1507
      ˅ Certificate: 308205df308204c7a003020102021345000001220560 58d3... (id-at-commonName=cucm-ms.steven.lab,id-at-organizationalUnitName=TAC,id-at-organizationName=Cisco,id-at-localityName=Diegem,id-at-stateOrProvinceName=Belgium,id-at-countryNa
        ˅ signedCertificate
            version: v3 (2)
            serialNumber: 0x450000012205605 8d34860844200020000 0122
          › signature (sha1WithRSAEncryption)
          › issuer: rdnSequence (0)
          › validity
          › subject: rdnSequence (0)
          › subjectPublicKeyInfo
          ˅ extensions: 9 items
            › Extension (id-ce-extKeyUsage)
            › Extension (id-ce-keyUsage)
            ˅ Extension (id-ce-subjectAltName)
                Extension Id: 2.5.29.17 (id-ce-subjectAltName)
                critical: True
              ˅ GeneralNames: 3 items
                ˅ GeneralName: dNSName (2)
                    dNSName: cups.steven.lab
                ˅ GeneralName: dNSName (2)
                    dNSName: steven.lab
                ˅ GeneralName: dNSName (2)
                    dNSName: cucm.steven.lab
            › Extension (id-ce-subjectKeyIdentifier)
            › Extension (id-ce-authorityKeyIdentifier)
            › Extension (id-ce-cRLDistributionPoints)
            › Extension (id-pe-authorityInfoAccessSyntax)
            › Extension (id-ms-certificate-template)
            › Extension (id-ms-application-certificate-policies)
        › algorithmIdentifier (sha1WithRSAEncryption)
          Padding: 0
          encrypted: 9fba7f8741637a2a92071efb68f227b9cecc7ec4a470c82b...
        Certificate Length: 910
      › Certificate: 3082038a30820272a003020102021062176f3fc2939a8044... (id-at-commonName=steven-DC-CA,dc=steven,dc=lab)
› Secure Sockets Layer
```

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。



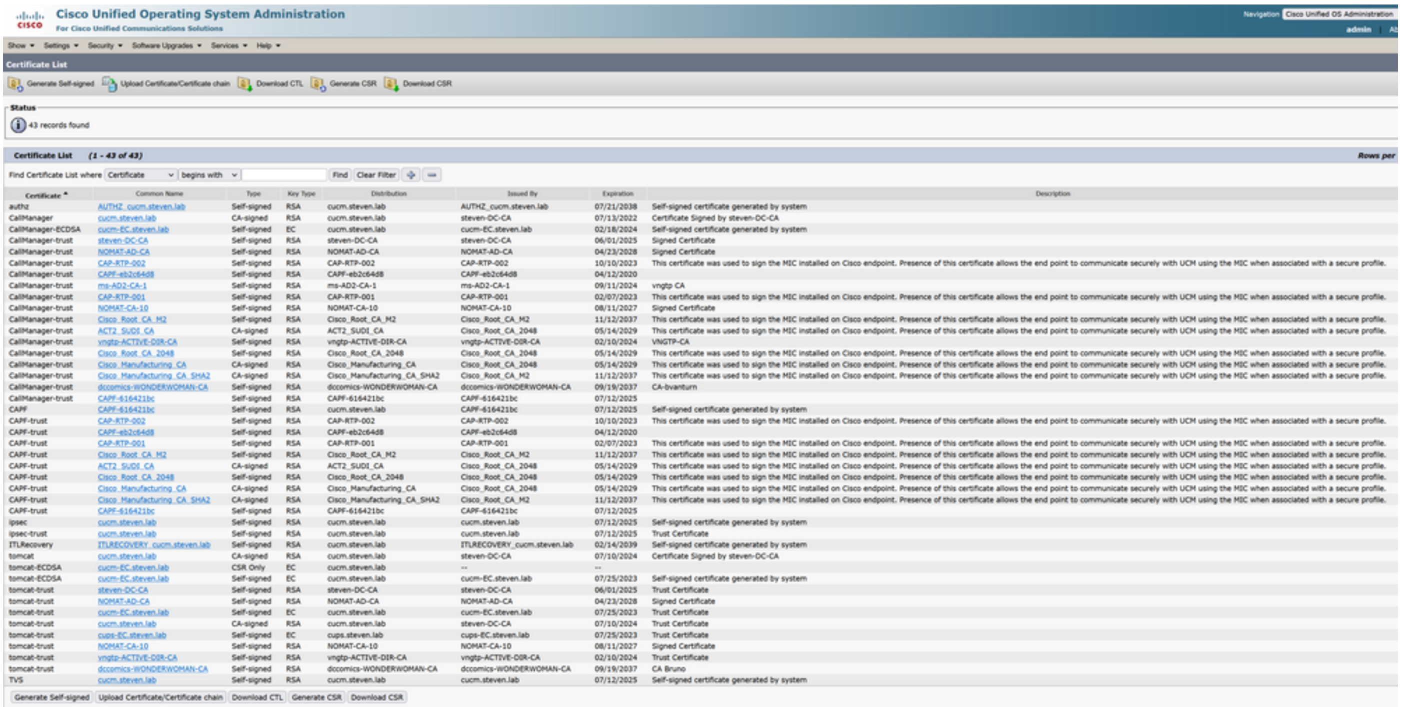
```
tcp.port==6972
```

```
No.   Time                        Source        Src port Destination  Dest port Protocol DSCP VLAN Length Info
 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      CS0          66 31576 → 6972 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=878570525 TSecr=343633320
 4733 2022-07-11 16:55:26.007100  10.48.36.46     31576 10.48.36.215     6972 TLSv1.2  CS0         583 Client Hello
 4734 2022-07-11 16:55:26.016350  10.48.36.215     6972 10.48.36.46     31576 TLSv1.2  CS0        1514 Server Hello, Certificate, Server Key Exchange
 4735 2022-07-11 16:55:26.016391  10.48.36.46     31576 10.48.36.215     6972 TCP      CS0          66 31576 → 6972 [ACK] Seq=518 Ack=1449 Win=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  CS0         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      CS0          66 31576 → 6972 [ACK] Seq=518 Ack=1882 Win=63744 Len=0 TSval=878570535 TSecr=343633329
 4738 2022-07-11 16:55:26.016703  10.48.36.46     31576 10.48.36.215     6972 TLSv1.2  CS0          73 Alert (Level: Fatal, Description: Unknown CA)
 4739 2022-07-11 16:55:26.016821  10.48.36.46     31578 10.48.36.215     6972 TCP      CS0          74 31578 → 6972 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=878570535 TSecr=0 WS=128
 4740 2022-07-11 16:55:26.016965  10.48.36.46     31576 10.48.36.215     6972 TCP      CS0          66 31576 → 6972 [RST, ACK] Seq=525 Ack=1882 Win=64128 Len=0 TSval=878570535 TSecr=343633329
 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 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=343633330 TSecr=878570535 WS=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      CS0          66 6972 → 31576 [FIN, ACK] Seq=1882 Ack=525 Win=30080 Len=0 TSval=343633330 TSecr=878570535
 4744 2022-07-11 16:55:26.017121  10.48.36.46     31576 10.48.36.215     6972 TCP      CS0          54 31576 → 6972 [RST] Seq=525 Win=0 Len=0
 4745 2022-07-11 16:55:26.017218  10.48.36.46     31578 10.48.36.215     6972 TLSv1.2  CS0         583 Client Hello
 4746 2022-07-11 16:55:26.024226  10.48.36.215     6972 10.48.36.46     31578 TLSv1.2  CS0        1514 Server Hello, Certificate, Server Key Exchange
 4747 2022-07-11 16:55:26.024265  10.48.36.46     31578 10.48.36.215     6972 TCP      CS0          66 31578 → 6972 [ACK] Seq=518 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      CS0          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  CS0          73 Alert (Level: Fatal, Description: Unknown CA)
 4751 2022-07-11 16:55:26.024647  10.48.36.46     31578 10.48.36.215     6972 TCP      CS0          66 31578 → 6972 [RST, ACK] Seq=525 Ack=1883 Win=64128 Len=0 TSval=878570543 TSecr=343633337
 4767 2022-07-11 16:55:26.083159  10.48.36.46     31580 10.48.36.215     6972 TCP      CS0          74 31580 → 6972 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=878570601 TSecr=0 WS=128
```

```
˅ Secure Sockets Layer
  › TLSv1.2 Record Layer: Handshake Protocol: Server Hello
  ˅ TLSv1.2 Record Layer: Handshake Protocol: Certificate
      Content Type: Handshake (22)
      Version: TLS 1.2 (0x0303)
      Length: 667
    ˅ Handshake Protocol: Certificate
        Handshake Type: Certificate (11)
        Length: 663
        Certificates Length: 660
      ˅ Certificates (660 bytes)
          Certificate Length: 657
        ˅ Certificate: 3082028d30820214a00302010202107470ee62271e3d1346... (id-at-localityName=Diegem,id-at-stateOrProvinceName=Belgium,id-at-commonName=cucm-EC.steven.lab,id-at-organizationalUnitName=TAC,id-at-organizationName=Cisco,id-at-countryNa
          ˅ signedCertificate
              version: v3 (2)
              serialNumber: 0x7470ee62271e3d13461b9946f0a3bf1d
            › signature (ecdsa-with-SHA384)
            ˅ issuer: rdnSequence (0)
              › rdnSequence: 6 items (id-at-localityName=Diegem,id-at-stateOrProvinceName=Belgium,id-at-commonName=cucm-EC.steven.lab,id-at-organizationalUnitName=TAC,id-at-organizationName=Cisco,id-at-countryName=BE)
            › validity
            › subject: rdnSequence (0)
            › subjectPublicKeyInfo
            ˅ extensions: 5 items
              › Extension (id-ce-keyUsage)
              › Extension (id-ce-extKeyUsage)
              › Extension (id-ce-subjectKeyIdentifier)
              › Extension (id-ce-basicConstraints)
              ˅ Extension (id-ce-subjectAltName)
                  Extension Id: 2.5.29.17 (id-ce-subjectAltName)
                ˅ GeneralNames: 1 item
                  ˅ GeneralName: dNSName (2)
                      dNSName: cucm.steven.lab
          › algorithmIdentifier (ecdsa-with-SHA384)
            Padding: 0
            encrypted: 3064023012543bd5ebe74570b1171eb489ff03b060cd80d8...
  › TLSv1.2 Record Layer: Handshake Protocol: Server 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 Unified Operating System Administration
For Cisco Unified Communications Solutions
Navigation Cisco Unified OS Administration
admin | Ab
Show ▾ Settings ▾ Security ▾ Software Upgrades ▾ Services ▾ Help ▾
Certificate List
Generate Self-signed
Upload Certificate/Certificate chain
Download CTL
Generate CSR
Download CSR
Status

43 records found

Certificate List (1 - 43 of 43)

Rows per
Find Certificate List where Certificate begins with
Find
Clear Filter

Certificate ▲	Common Name	Type	Key Type	Distribution	Issued By	Expiration	Description
authz	AUTHZ_cucm.steven.lab	Self-signed	RSA	cucm.steven.lab	AUTHZ_cucm.steven.lab	07/21/2038	Self-signed certificate generated by system
CallManager	cucm.steven.lab	CA-signed	RSA	cucm.steven.lab	steven-DC-CA	07/13/2022	Certificate Signed by steven-DC-CA
CallManager-ECDSA	cucm-EC.steven.lab	Self-signed	EC	cucm.steven.lab	cucm-EC.steven.lab	02/18/2024	Self-signed certificate generated by system
CallManager-trust	steven-DC-CA	Self-signed	RSA	steven-DC-CA	steven-DC-CA	06/01/2025	Signed Certificate
CallManager-trust	NOMAT-AD-CA	Self-signed	RSA	NOMAT-AD-CA	NOMAT-AD-CA	04/23/2028	Signed Certificate
CallManager-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.
CallManager-trust	CAPF-eb2c64d8	Self-signed	RSA	CAPF-eb2c64d8	CAPF-eb2c64d8	04/12/2020	
CallManager-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 UCM 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 UCM using the MIC when associated with a secure profile.
CallManager-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 UCM using the MIC when associated with a secure profile.
CallManager-trust	vngtp-ACTIVE-DIR-CA	Self-signed	RSA	vngtp-ACTIVE-DIR-CA	vngtp-ACTIVE-DIR-CA	02/10/2024	VNGTP-CA
CallManager-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 UCM using the MIC when associated with a secure profile.
CallManager-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 UCM using the MIC when associated with a secure profile.
CallManager-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.
CallManager-trust	dccomics-WONDERWOMAN-CA	Self-signed	RSA	dccomics-WONDERWOMAN-CA	dccomics-WONDERWOMAN-CA	09/19/2037	CA-bvanturn
CallManager-trust	CAPF-616421bc	Self-signed	RSA	CAPF-616421bc	CAPF-616421bc	07/12/2025	
CAPF	CAPF-616421bc	Self-signed	RSA	cucm.steven.lab	CAPF-616421bc	07/12/2025	Self-signed certificate generated by system
CAPF-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.
CAPF-trust	CAPF-eb2c64d8	Self-signed	RSA	CAPF-eb2c64d8	CAPF-eb2c64d8	04/12/2020	
CAPF-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 UCM using the MIC when associated with a secure profile.
CAPF-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 UCM using the MIC when associated with a secure profile.
CAPF-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 UCM using the MIC when associated with a secure profile.
CAPF-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 UCM 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 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	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	cucm.steven.lab	07/12/2025	Self-signed certificate generated by system
ipsec-trust	cucm.steven.lab	Self-signed	RSA	cucm.steven.lab	cucm.steven.lab	07/12/2025	Trust Certificate
ITLRecovery	ITLRECOVERY_cucm.steven.lab	Self-signed	RSA	cucm.steven.lab	ITLRECOVERY_cucm.steven.lab	02/14/2039	Self-signed certificate generated by system
tomcat	cucm.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	EC	cups.steven.lab	cups-EC.steven.lab	07/25/2023	Trust Certificate
tomcat-trust	NOMAT-CA-10	Self-signed	RSA	NOMAT-CA-10	NOMAT-CA-10	08/11/2027	Signed Certificate
tomcat-trust	vngtp-ACTIVE-DIR-CA	Self-signed	RSA	vngtp-ACTIVE-DIR-CA	vngtp-ACTIVE-DIR-CA	02/10/2024	Trust Certificate
tomcat-trust	dccomics-WONDERWOMAN-CA	Self-signed	RSA	dccomics-WONDERWOMAN-CA	dccomics-WONDERWOMAN-CA	09/19/2037	CA Bruno
TVS	cucm.steven.lab	Self-signed	RSA	cucm.steven.lab	cucm.steven.lab	07/12/2025	Self-signed certificate generated by system

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="netwo
HTTPMSG:
|GET http://vcs_control.steven.lab:8443/c3RldmVuLmxhYi9odHRwcy8xMC40OC4zNi4yMTUvODQ0Mw/cucm-uds/user/emu
...

2022-07-11T19:49:01.478+02:00 vcsc traffic_server[3916]: UTCTime="2022-07-11 17:49:01,478" Module="netwo
2022-07-11T19:49:01.478+02:00 vcsc traffic_server[3916]: UTCTime="2022-07-11 17:49:01,478" Module="netwo
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：

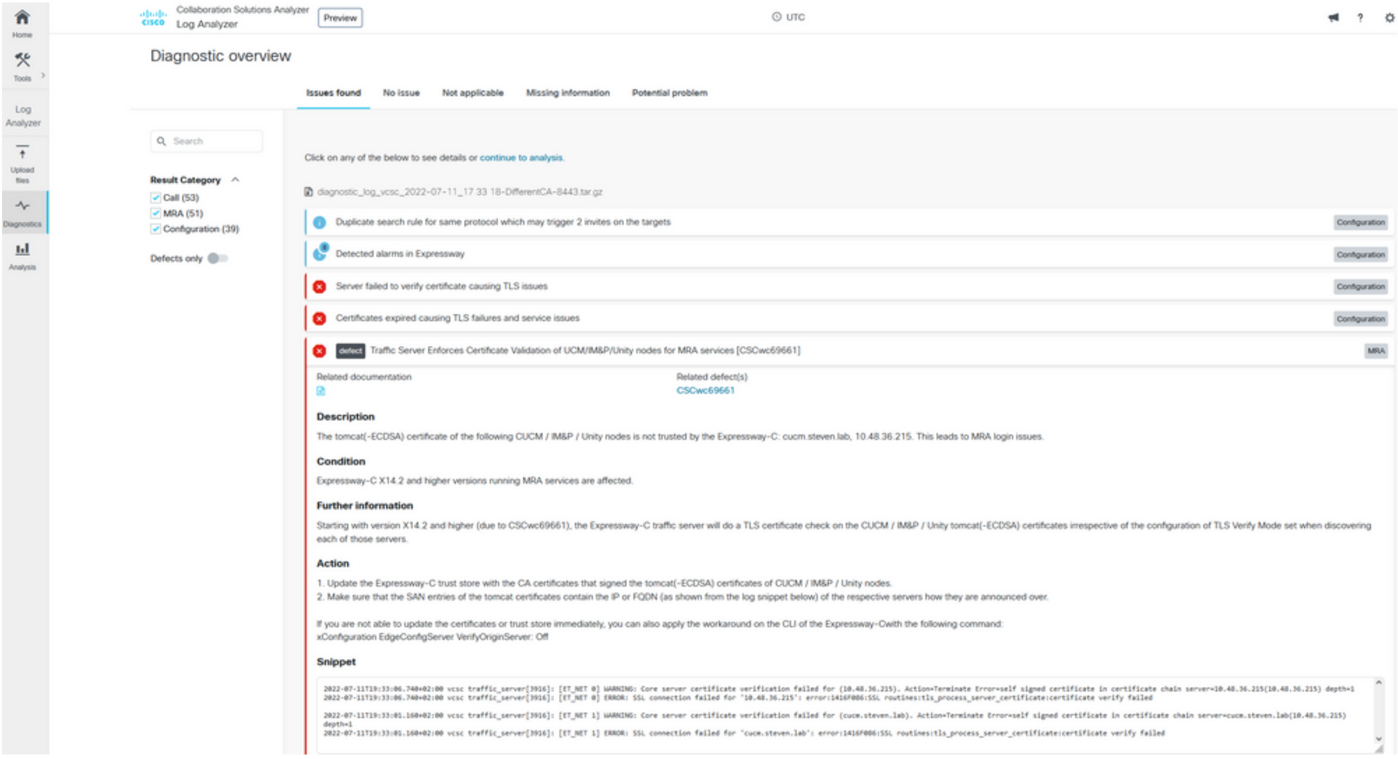
1. 在Expressway E和Expressway C伺服器上啟動診斷日誌記錄（最好啟用TCPDumps），方法是透過維護>診斷>診斷日誌記錄（如果是集群，則僅從主節點啟動即可）

2. 在升級後嘗試MRA登入或測試中斷的功能

3. 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. 上傳和分析合作解決方案分析器工具上的日誌

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



Diagnostic overview

Click on any of the below to see details or continue to analysis.

diagnostic_log_vcsc_2022-07-11_17 33 18-DifferentCA-8443.tar.gz

Duplicate search rule for same protocol which may trigger 2 invites on the targets

Detected alarms in Expressway

Server failed to verify certificate causing TLS issues

Certificates expired causing TLS failures and service issues

Traffic Server Enforces Certificate Validation of UCM/IM&P/Unity nodes for MRA services [CSCwc69661]

Related documentation

Related defect(s)
CSCwc69661

Description

The tomcat(-ECDSA) certificate of the following CUCM / IM&P / Unity nodes is not trusted by the Expressway-C: cucm.steven.lab, 10.48.36.215. This leads to MRA login issues.

Condition

Expressway-C X14.2 and higher versions running MRA services are affected.

Further information

Starting with version X14.2 and higher (due to CSCwc69661), the Expressway-C traffic server will do a TLS certificate check on the CUCM / IM&P / Unity tomcat(-ECDSA) certificates irrespective of the configuration of TLS Verify Mode set when discovering each of those servers.

Action

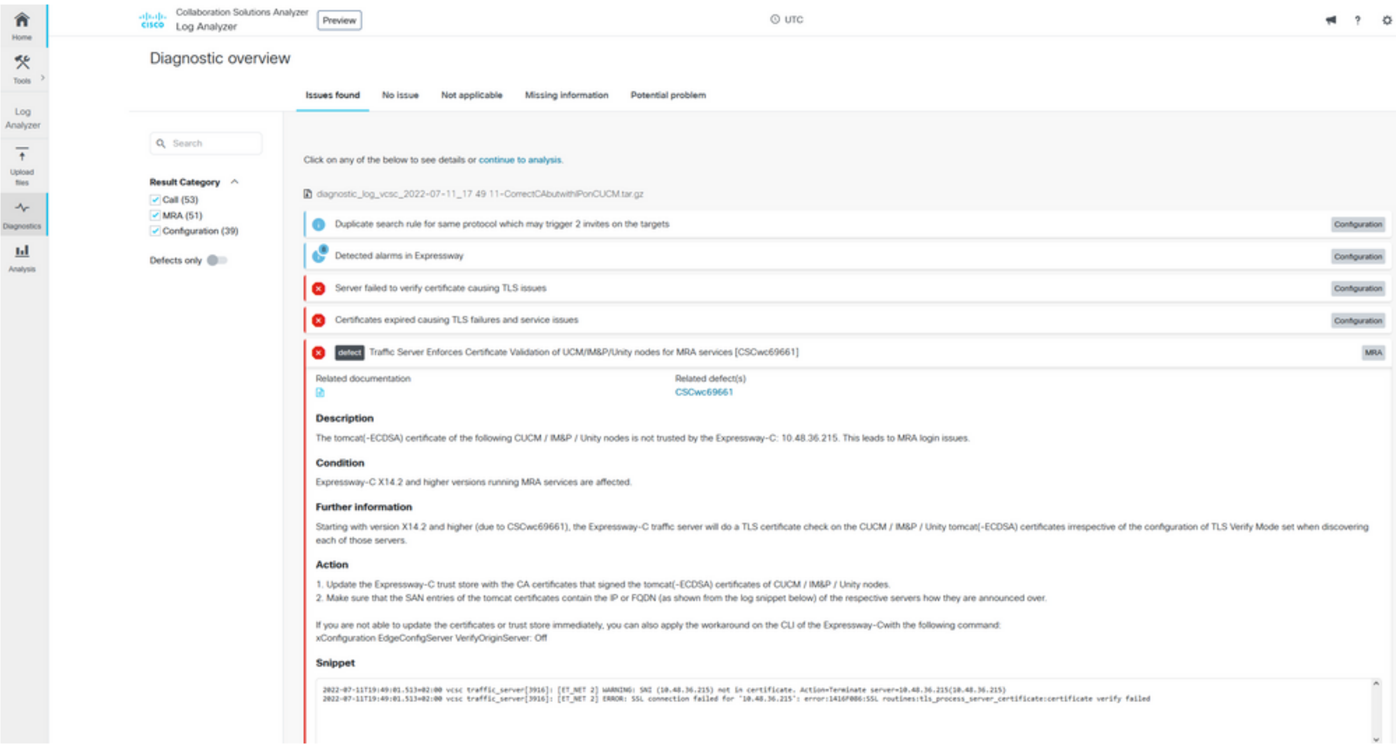
1. Update the Expressway-C trust store with the CA certificates that signed the tomcat(-ECDSA) certificates of CUCM / IM&P / Unity nodes.
2. Make sure that the SAN entries of the tomcat certificates contain the IP or FQDN (as shown from the log snippet below) of the respective servers how they are announced over.

If you are not able to update the certificates or trust store immediately, you can also apply the workaround on the CLI of the Expressway-Cwith the following command:
xConfiguration EdgeConfigServer VerifyOriginServer: Off

Snippet

```
2022-07-11T19:33:06.740+02:00 vcsc traffic_server[3916]: [ET_NET 0] WARNING: Core server certificate verification failed for (10.48.36.215). Action=Terminate Error=self signed certificate in certificate chain server=10.48.36.215(10.48.36.215) depth=1
2022-07-11T19:33:06.740+02:00 vcsc traffic_server[3916]: [ET_NET 0] ERROR: SSL connection failed for '10.48.36.215': error:1416F086:SSL routines:tls_process_server_certificate:certificate verify failed

2022-07-11T19:33:01.160+02:00 vcsc traffic_server[3916]: [ET_NET 1] WARNING: Core server certificate verification failed for (cucm.steven.lab). Action=Terminate Error=self signed certificate in certificate chain server=cucm.steven.lab(10.48.36.215)
depth=1
2022-07-11T19:33:01.160+02:00 vcsc traffic_server[3916]: [ET_NET 1] ERROR: SSL connection failed for 'cucm.steven.lab': error:1416F086:SSL routines:tls_process_server_certificate:certificate verify failed
```

CA診斷簽名



Diagnostic overview

Result Category

☑ Call (53)
☑ MRA (51)
☑ Configuration (39)

Defects only

Click on any of the below to see details or continue to analysis.

diagnostic_log_vcsc_2022-07-11_17 49 11-CorrectCAbutwithIPonCUCM.tar.gz

- Duplicate search rule for same protocol which may trigger 2 invites on the targets — Configuration
- Detected alarms in Expressway — Configuration
- Server failed to verify certificate causing TLS issues — Configuration
- Certificates expired causing TLS failures and service issues — Configuration
- defect Traffic Server Enforces Certificate Validation of UCM/IM&P/Unity nodes for MRA services [CSCwc69661] — MRA

Related documentation

Related defect(s)
CSCwc69661

Description

The tomcat(-ECDSA) certificate of the following CUCM / IM&P / Unity nodes is not trusted by the Expressway-C: 10.48.36.215. This leads to MRA login issues.

Condition

Expressway-C X14.2 and higher versions running MRA services are affected.

Further information

Starting with version X14.2 and higher (due to CSCwc69661), the Expressway-C traffic server will do a TLS certificate check on the CUCM / IM&P / Unity tomcat(-ECDSA) certificates irrespective of the configuration of TLS Verify Mode set when discovering each of those servers.

Action

1. Update the Expressway-C trust store with the CA certificates that signed the tomcat(-ECDSA) certificates of CUCM / IM&P / Unity nodes.
2. Make sure that the SAN entries of the tomcat certificates contain the IP or FQDN (as shown from the log snippet below) of the respective servers how they are announced over.

If you are not able to update the certificates or trust store immediately, you can also apply the workaround on the CLI of the Expressway-Cwith the following command:
xConfiguration EdgeConfigServer VerifyOriginServer: Off

Snippet

```
2022-07-11T19:49:01.513+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)
2022-07-11T19:49:01.513+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
```

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 CSCwa12905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
```

It

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）。