# Cisco IOS XE和GuestShell CA Trust eMudra不信任指南

## 目錄

## 目的

本檔案將就Cisco IOS® XE提供指南，以應對緊急情況下對Mudhra根和中間證書頒發機構的不信任。

使用此指南審計和管理其配置允許受影響的層次結構的服務的CA信任。產品適用性和所需的補救在思科資訊性中定義。在變更信任之前，請檢查Cisco IOS XE版本的命令支援和服務影響。

Cisco informational:cisco-sa-emudhra-info-ScS22A1r

### 受影響的eMudra CA憑證：原始和交叉簽名

庫存於2026年10月29日核實。八個eMudra頒發CA金鑰受到影響：6個用於TLS，2個用於代碼簽名。每個金鑰顯示在原始的emSign頒發的CA證書和Sectigo交叉簽名的CA證書中。因此，該清單包含16個證書：12個TLS和4個代碼簽名證書。

每個原始/交叉簽名對都具有相同的主題和公共金鑰，但頒發者、序列號和SHA-256證書指紋不同。這兩種表單提供備用認證路徑，並且必須都包括在稽核中。

#### A.發行商和受影響的證書庫存

頒發者A — 原始TLS證書：CN=emSign Root TLS CA - G3,O=eMudhra Technologies Limited，C=IN。

頒發者B — 原始代碼簽名證書：CN=emSign Root CS CA - G3,O=eMudhra Technologies Limited，C=IN。

頒發者C — 所有交叉簽名的證書：CN=AAA Certificate Services， O=Comodo CA Limited，L=Salford， ST=Greater Manchester， C=GB(Sectigo)。

G3B主題：O=Mudhra BV，C=NL。G3C主題：O=Mudhra Inc，C=US。每個變體單元列出其發行

者引用、十六進位制序列和SHA-256指紋（兩行）。 前導零填充不會更改序列值。

| 影響頒發CA(CN) | 原始證書<br>簽發方/串列（十六進位制）/SHA-256 | Sectigo交叉簽名證書<br>簽發方/串列（十六進位制）/SHA-256 |
|---|---|---|
| 1. EM DV TLS CA - G3B<br>TLS | 發行商A<br>A4AEE678F23362B4C0E460B772F214<br>42C4ACCD12C4F59597925E1A08A7A901<br>02608543809308D50EC427E118BA1493 | 發行商C<br>A024FDF4BA665C785CE4A020483858B7<br>45A883F349AEDFD5F3A649B5498FFB12<br>1712BA8B448F3F2A91DBC5A766FCDBE |
| 2. EM OVER TLS CA - G3B<br>TLS | 發行商A<br>6CADA367FB1C100088120EA202D568<br>98B896625C0C230ADEC3EB2CF6AAD50<br>01ECF9156A68644E82374CE5833BC25B | 發行商C<br>E94223BDE92F914E5AB9ACABFDAC3710<br>5F1DED4DD590AF74631290CF073B122A<br>2AAC6A1FA479778A0BD43579BD832699 |
| 3. EM EV TLS CA - G3B<br>TLS | 發行商A<br>C7C41EFE92D825F05EAE841A4A82C1<br>E7568FE6E12331F4FD7DE61DA4C7559D<br>0F8EB192A218D4741A3BA75184333838 | 發行商C<br>D8F8685E4F2BD9D82402A85A1C1EB731<br>579480AEA166290BD3C643589E795FC0<br>D0E54E86505D180F1DFF99EFD3199512 |
| 4. EM DV TLS CA - G3C<br>TLS | 發行商A<br>588B2E3C2BB8CDA13E1A1209254321<br>0164D7CEAE5BB909C272AF151FF44B11<br>77AE9B47D9424B94F1D9558C30934D19 | 發行商C<br>91F347F1A5B7D39962B95E0EE4E299D1<br>62B7F9868263F72F6911FC78CEAF72C1<br>979158B7368BF648683BB2AA39B02E72 |
| 5. EM OVER TLS CA - G3C<br>TLS | 發行商A<br>296926C227A3A1526392B19482A504<br>CB6E15165AC802E9B3F993F16C25D41F<br>4E81C21EBDE71AE1B012AC00BF9C7C3F | 發行商C<br>8D5A4811939EF447D77111CDD9849AE9<br>7485B51C0ED192878FA1D2F948FB529A<br>E1842CC5086C4B67F7BE5B2039DE9489 |

| 影響頒發CA(CN) | 原始證書<br>簽發方/串列（十六進位制）/SHA-256 | Sectigo交叉簽名證書<br>簽發方/串列（十六進位制）/SHA-256 |
|---|---|---|
| 6. EM EV TLS CA - G3C<br>TLS | 發行商A<br>8009928A64107601AF05FA2F19F109<br>432EC25F0D28DE9006D97BF752F17BBB<br>2CD41F669933FCB072D9A1148D0261F3 | 發行商C<br>05F078752DECE7A1BB8595D303167171<br>FD9D5C2DBBD4995AB69B8D50C439D952<br>7B00529199C2FD01B2174EB58F07021F |
| 7. EM OVER CS CA - G3B<br>代碼簽名 | 發行商B<br>7818933F8F85B4619A2B35FBA83D0A<br>9E39DE2881273ACC225A149C72BA3E0F<br>51424963669AB633EE1DC7DF5DB067B4 | 發行商C<br>41E32B73AC185D6CE0D7480BACF84E69<br>A496E23AC0CAB8155FC9B117B97EAE36<br>8EFCBB9041AEC8804D5A308D2D01C2D8 |
| 8. EM OVER CS CA - G3C<br>代碼簽名 | 發行商B<br>544B7F922C31AE220A4A922916F6E6<br>4B2460A466F95FD40113BCDCCA2CEB29<br>B3B093921DE45474DA7DF48874C630B1 | 發行商C<br>D6A5EF613B390F32EF9CDF349F772841<br>84112972B8E59D14560AE7E711965447<br>4AAD119990CF3722BFC1E3B91615E1FD |

## B.區分的認證途徑

原始TLS路徑

```
emSign ECC Root CA - G3
  +-- emSign Root TLS CA - G3 (issued by emSign ECC Root CA - G3)
       +-- Original EM DV/OV/EV TLS CA - G3B or G3C
            +-- TLS identity certificate
```

原始代碼簽名路徑（Root CS直接受信任）

```
emSign Root CS CA - G3
  +-- Original EM OV CS CA - G3B or G3C
       +-- Code-signing identity certificate
```

Sectigo交叉簽名路徑（TLS和代碼簽名）

```
AAA Certificate Services
  +-- One of the eight cross-signed CAs listed above
       +-- TLS or code-signing identity certificate
```

當一個TLS路徑直接受信任時，該TLS路徑還可以在emSign Root TLS CA - G3終止。圖表顯示了相關的發行人關係；接受的路徑取決於消費服務的信任錨點和驗證策略。

示例中顯示的父/根CA提供鏈上下文，不會計入八個受損的發佈金鑰中。刪除或不信任父項/根的決策與識別被破壞的中間金鑰是分開的。

若要識別，請將證書頒發機構和序列號與SHA-256指紋一起使用。僅使用者名稱是不夠的。證書指紋可識別一個證書變體；spki SHA-256雜湊標識其原始表單和交叉簽名表單共用的公鑰。僅刪除快取的中間路徑不會阻止對等體通過剩餘的受信任路徑呈現該中間路徑。

## 來源和驗證日期

2026年10月29日，對公共事件附件進行了證書識別符號驗證。每個原始/交叉符號對包含相同的公鑰。使用即時思科資訊瞭解產品適用性和補救狀態。

Cisco informational:cisco-sa-emudhra-info-ScS22A1r

Mozilla事件記錄：Mudhra中間金鑰洩漏(2083449)

原始CA憑證附件(9664066)

AAA交叉簽名CA憑證附件(9664067)

蘋果：原始和交叉簽名TLS證書路徑和指紋

截至2026年10月31日，在本指南列出的受攻擊CA中，未識別emSign根CA - G1。其持續信任仍取決於貴組織的政策以及隨後的諮詢更新。

## Cisco IOS XE如何管理證書信任

配置的PKI信任點儲存CA/身份證書和驗證策略。PKI信任池包含用於使用該信任池的服務的內建和下載的CA證書。確定每個相關服務使用的信任源和策略；更改信任池不會替換單獨配置的信任點。

## 1.審計和準備

檢查軟體版本、裝置時間和安裝的證書：

<#root>

**show version show clock show crypto pki trustpoints show running-config | section crypto pki trustpoint**

將完整證書頒發者和十六進位制序列號與清單進行比較，使用主題作為支援上下文。如果Cisco IOS XE僅顯示MD5和SHA1指紋，則無法在該輸出中直接比較清單SHA-256指紋；它用於驗證裝置外部的證書檔案。序列號中的前00填充可以不同。供應商名稱搜尋僅識別候選者。記錄依賴於每個信任點的服務，並檢查原始路徑和交叉簽名路徑，包括直接受信任的中間體。

### 範例：根CA和受影響的子CA

顯示詳細證書的簡短示例；其他欄位將被省略。比較主題、頒發者和序列號。

根CA示例：emSign ECC根CA - G3

```
CA Certificate
  Certificate Serial Number (hex): 3CF607A968700EDA8B84
  Issuer:
    cn=emSign ECC Root CA - G3
  Subject:
    cn=emSign ECC Root CA - G3
  Associated Trustpoints:
```

受影響的SubCA示例：原始的emSign頒發的證書

```
CA Certificate
  Certificate Serial Number (hex): 00A4AEE678F23362B4C0E460B772F214
  Issuer:
    cn=emSign Root TLS CA - G3
  Subject:
    cn=EM DV TLS CA - G3B
```

```
  Associated Trustpoints:
```

受影響的SubCA示例：Sectigo交叉簽名證書

```
CA Certificate
  Certificate Serial Number (hex): 00A024FDF4BA665C785CE4A020483858B7
  Issuer:
    cn=AAA Certificate Services
  Subject:
    cn=EM DV TLS CA - G3B
  Associated Trustpoints:
```

兩個SubCA表單具有相同的Subject，但不同的發佈者和序列。將完整發行商和序列與庫存相匹配；前導00填充可以不同。記錄關聯的信任點，以定位擁有的信任點或池。顯示的根是鏈上下文；它不是八個受損的發行金鑰之一。

保持恢復訪問方法和批准的更換捆綁包可用。必要時使用批准的證書/金鑰備份過程。備份組態；僅此副本不是私鑰備份：

<#root>

**copy running-config**

使用經認可的特定於裝置的值替換尖括弧佔位符。使用show file systems顯示的檔案系統，例如flash:或bootflash:。

## 2.檢查信任路徑

### 刪除直接受信任的受影響SubCA

從信任點和下載的信任池捆綁包中刪除直接受信任影響的子CA。不要依賴吊銷設定來覆蓋受危害的CA中的直接信任。

### 可選根CA刪除

刪除根CA是提供額外保護的可選建議。當實際服務CRL/OCSP檢查獲得當前狀態、評估受信任的父級下受影響的SubCA、拒絕受影響的原始、交叉簽名和適用的較長鏈時，所需的根可以保持受信任，並且如果配置的方法均未提供可用狀態，則驗證失敗。在這些驗證條件下，撤銷檢查可以保護被識別的受損發行者而不刪除根。

考慮刪除不必要的根/信任錨點，以減少對撤銷服務的依賴。首先評估服務依賴性：刪除AAA證書服務可能會中斷不相關的合法鏈。覆蓋eMudra和AAA路徑。僅刪除快取的SubCA不會阻止對等體提供的副本通過剩餘的受信任父級。

### 刪除所選信任點

對於選擇刪除的管理員配置的信任點：

<#root>

```
configure terminal no crypto pki trustpoint
```

```
      end
```

接受之前請複查確認。信任點刪除會銷毀其關聯的證書。如果裝置標識需要替換，請獲取與裝置金鑰匹配的替換證書，並使用服務註冊過程更新其服務繫結。僅安裝新的CA證書不會替換裝置標識。

對於下載的trustpool條目，請使用bundle-replacement過程。內建或功能管理的錨點需要受支援的產品更新或Cisco TAC指導。

## 3.如有需要，更新下載的Trustpool

當下載的套件組合需要更換時，請使用以下步驟。在步驟2中的已驗證撤銷條件下，所需的父/根可以保持受信任狀態。

### 3.1檢查下載的套件組合是否已安裝並使用

<#root>

```
show running-config | section crypto pki certificate pool show crypto pki trustpool verbose show crypto
```

在crypto pki certificate pool和CA記錄下查詢標籤為Trustpool的纜線條目：已下載。套件組合檔案名稱可以與ios.p7b或ios_core.p7b不同。單獨儲存的檔案或配置的刷新URL並不能證明其證書是服務安裝或使用的。確認服務使用信任池，並將其CA記錄與受影響的庫存進行比較。如果未安裝下載的CA，請跳過清理和替換；仍評估其他信任來源。

## 3.2清理下載的信任池

在清理之前保留恢復訪問和已批准的恢復捆綁包可用。如果傳輸依賴於正在刪除的信任，則以後下載可能會失敗。制定相關服務中斷的計畫。

<#root>

```
configure terminal crypto pki trustpool clean end
```

```
show crypto pki trustpool verbose
```

確認下載的CA記錄已丟失。清除操作將刪除所有下載的信任池證書及其管理的捆綁包檔案；內建CA和獨立信任點仍然存在。在替換和服務檢查成功之前不要儲存。

## 3.3獲取並安裝批准的更換捆綁包

獲得經核准的思科簽名的捆綁包。為所需服務選擇ios.p7b或ios_core.p7b，並確認其不包括上面標識的受影響證書和不需要的信任金鑰。2026年10月31日選中的舊捆綁包在ios.p7b中包含emSign根CA - G1，但在ios_core.p7b中既不包含eMudhra也不包含AAA證書服務CA。Core具有更小的信任集：交換之前先檢查服務依賴項，然後驗證您安裝的套件組合的內容。使用已批准的HTTPS或SCP傳輸將其暫存到託管信任池儲存之外。

思科完整CA捆綁包：ios.p7b

思科核心CA捆綁包：ios_core.p7b

<#root>

```
show file systems copy
```

```
configure terminal crypto pki trustpool import url

end show crypto pki trustpool verbose
```

例如，分級URL可以是flash:approved-ios.p7b。如果匯入失敗，請在儲存之前還原已批准的捆綁包。驗證所需的CA和所需的連線。清理不是證書拒絕清單：通過強制撤銷或信任路徑刪除，確認其餘信任點、內建CA和備用路徑拒絕受影響的鏈。

## 4.配置驗證和刷新策略

進行更改之前，請記錄現有的信任池策略、受影響的信任點策略、證書對映繫結和刷新URL，以便在需要時恢復它們。

對於相關配置的信任點：

<#root>

```
configure terminal crypto pki trustpoint

revocation-check crl ocsp exit end
```

對於使用trustpool策略的服務：

<#root>

```
configure terminal crypto pki trustpool policy chain-validation revocation-check crl ocsp exit end show
```

檢查顯示的信任池策略是否繼續對根進行驗證並列出crl ocsp。當CRL檢索不可用時，裝置首先嘗試CRL並嘗試OCSP。當評估受影響的證書時，撤消的結果未通過驗證。當需要成功的撤銷檢查時，不要新增無。

驗證正確的時間、可訪問CA發佈的狀態終結點、接受的響應格式以及不存在適用的撤銷跳過異常。受影響的SubCA狀態必須在可信的父級下評估。在檢查子CA父級之前，可以停止對子CA直接信任。驗證實際服務是否獲得可用、當前狀態並拒絕受影響的鏈。如果無法驗證狀態 — 伺服器訪問和拒絕行為，請不要單獨將配置視為已確認的保護；根據緩解計畫的需要，刪除相關信任路徑。不要新增無，以繞過不可用狀態。

## 在驗證保護之前刷新快取的CRL

即使在CA發佈較新的CRL之後，本地快取/資料庫中已經存在的可用CRL仍可重複使用。檢查狀態伺服器可達性，然後在驗證保護之前清除舊的CRL:

<#root>

```
show crypto pki crls clear crypto pki crl show crypto pki crls
```

clear命令刪除所有信任點的本地CRL;它本身不會下載替代品。確認舊條目已丟失，然後在受影響的服務中啟動新的連線或證書驗證。再次運行show crypto pki crls，並根據CA的當前發佈檢查每個相關的頒發者、LastUpdate、NextUpdate和分發點。包括覆蓋受影響子CA的父頒發者CRL，而不僅包括ID證書頒發者CRL。確認已拒絕受影響的鏈。清除可能會在讀取狀態資料時暫時影響新連線；保留失效關閉驗證。

## 檢視捆綁包刷新源

對於連線的裝置，可選擇配置已批准的到期驅動套件組合刷新源：

<#root>

```
configure terminal crypto pki trustpool policy cabundle url
```

```
exit end show crypto pki trustpool policy
```

檢視所有已配置的捆綁包源。到期驅動的刷新不會替換立即安全更新，而且不能還原不需要的信任路徑。

可選的證書對映篩選器：覆蓋與限制

Cisco IOS XE證書對映(cert-map)匹配證書屬性，如頒發者名稱。此外，此過濾器還可以幫助拒絕由列出的八個CA直接頒發的ID（枝葉）證書。在應用信任點現有的匹配證書策略之前，請對其進行檢查。

2026年10月29日，在實驗實驗室裝置上使用EM DV TLS CA - G3B下的實驗室身份測試行為。在PKI對等證書驗證中，過濾器拒絕直接頒發的身份，但是沒有阻止通過其他子SubCA頒發的身份；一個未上市的合法發行商獲得通過。行為覆蓋使用一個受影響的頒發者，僅在臨時實驗室信任點禁用撤銷功能以隔離過濾器。應用握手和其他版本未通過此過濾器驗證；在依賴實際服務之前先對其進行測試。

<#root>

```
configure terminal crypto pki certificate map EMSIGN-ISSUER-FILTER 10 issuer-name nc cn=EM DV TLS CA - G
```

```
match certificate EMSIGN-ISSUER-FILTER exit end
```

在此， nc的意思是「不包含」。 將所有8個負發行人名稱條件都儲存在同一個條目中，序列10:所有內容必須匹配，證書才能通過此篩選器。與任何列出的名稱匹配的直接頒發者未通過篩選。

Cisco IOS XE可以顯示規範化的條目，例如issuer-name nc cn = em dv tls ca - g3b。行為測試中存

在此小寫和間隔格式。確認對映及其與服務實際使用的驗證信任點的繫結：

<#root>

**show running-config | section crypto pki certificate map show running-config | section crypto pki trustp**

此過濾器未提供全鏈的CA拒絕清單。舉例來說：

```
Trusted root CA
  +-- Affected SubCA
       +-- New child SubCA
            +-- ID (leaf) certificate
```

ID證書頒發者是新的子SubCA，因此其issuer-name篩選器不會識別鏈中更高層的受影響CA。其他檢查（包括CA約束和撤銷）仍然適用。僅將此過濾器用作與本指南中的撤銷驗證和可選根刪除過程一起提供的附加保護。直接簽發的測試、子SubCA以及具有實際服務的合法證書。

第4步的回滾

恢復記錄的吊銷方法、鏈驗證設定和證書對映繫結。刪除由此過程新增的刷新URL，並還原任何以前更改的URL。此示例僅刪除新增的刷新URL和篩選器繫結；它不會還原其他策略設定：

<#root>

**configure terminal crypto pki trustpool policy no cabundle url**

**exit**

**crypto pki trustpoint**

**no match certificate EMSIGN-ISSUER-FILTER exit end**

僅當通過此過程新增URL和繫結時，才運行這些刪除操作。如果替換了以前的證書對映繫結，請恢復該繫結。只有在確認沒有任何其他配置引用新建立的對映後，才將其刪除。

僅當重置為預設值是預期的、已批准的結果時，才使用no crypto pki trustpool policy。此寬重置將清除配置的刷新URL並將吊銷檢查重置為無；它不會還原以前的自定義策略。策略回滾不會還原已刪除的證書、還原已安裝的捆綁包或還原已清除的CRL。在儲存之前重新檢查所需的服務和受影響的鏈拒絕。

## 5.驗證保護和儲存

- 確認已拒絕受影響的原始鏈和交叉符號鏈，包括對等體提供的中間鏈。如果相關鏈較長，則當鏈中受影響的CA較高時檢驗拒絕情況。
- 確認所需的合法連線仍然有效，並且任何替換身份都繫結到目標服務。
- 當吊銷資料不可用時檢查行為。現有的TLS/IPsec會話不會自動通過策略更改進行驗證；如果需要，請使用服務支援的重新連線過程。

檢查成功後：

<#root>

```
show crypto pki certificates verbose show crypto pki trustpool policy write memory
```

在下次計畫重新載入後，並在備用裝置（如果適用）上驗證永續性。如果結果與預期的信任策略不同，請保留日誌並在考慮已驗證的信任更改之前聯絡Cisco TAC。

## 進一步閱讀

Cisco IOS XE PKI Trustpool Management

Cisco:使用Cisco IOS XE PKI配置CA簽名證書

Cisco:CRL快取和吊銷檢查

# Cisco IOS XE GuestShell CA信任指南

**步驟 1:稽核裝置GuestShell部署狀態**

僅對安裝了GuestShell且處於RUNNING或DEPLOYED狀態的Cisco IOS XE系統要求補救。如果GuestShell處於DEPLOYED狀態，必須先使用「guestshell enable」命令啟用它，然後才能執行補救命令。如果show app-hosting list指示「未找到應用」（GuestShell未部署或未啟用），則不需要對GuestShell執行任何操作。

A.處於DEPLOYED狀態的GuestShell(需要操作：必須首先啟用)

當show app-hosting list報告GuestShell處於DEPLOYED狀態時，GuestShell容器儲存存在，但容器已停止。在輸入bash之前，必須運行「guestshell enable」（如果返回停止狀態，則在完成補救之後必須運行「guestshell disable」）：

<#root>

```
Router#

show app-hosting list

App id                                   State
------------------------------------------------------------
guestshell                               DEPLOYED
```

B.處於RUNNING狀態的GuestShell(需要操作：直接繼續)

當show app-hosting list報告GuestShell處於RUNNING狀態時，GuestShell正在運行並且您可以直接進入bash:

<#root>

```
Router#

show app-hosting list

App id                                   State
------------------------------------------------------------
guestshell                               RUNNING
```

B.未啟用/未部署GuestShell（無需執行任何操作）

如果show app-hosting list指示No App found，則系統上未安裝或啟用GuestShell，並且不需要進一步的操作：

<#root>

```
Router#

show app-hosting list

No App found
```

步驟 2:訪問GuestShell並應用CA不信任

從Cisco IOS XE特權EXEC('enable')提示符處執行這些命令。如果GuestShell處於DEPLOYED狀態，請先啟用它。然後輸入bash shell，升級到根目錄，並使用動態資料夾選擇配置CA阻止清單以確保所有Cisco IOS XE版本的相容性：

<#root>

```
! 1. If GuestShell is in DEPLOYED state, enable it first:
Router#

guestshell enable


! 2. Enter GuestShell bash shell:
Router#

guestshell run bash


! 3. Escalate to root user inside GuestShell:
[guestshell@guestshell ~]$

sudo -s


! 4. Prepare the ca-trust blocklist directory (compatible with 17.15.x and 17.18.x):
d=/etc/pki/ca-trust/source/blocklist
[ -d "$d" ] || d=/etc/pki/ca-trust/source/blacklist
mkdir -p "$d"
```

不信任受危害的eMudra憑證

執行trust extract命令將每個受損的eMudhra證書直接提取到ca-trust blocklist目錄中，然後重建系統信任儲存：

```
trust extract --overwrite --format=pem-bundle \
  --filter='pkcs11:object=emSign%20ECC%20Root%20CA%20-%20G3;type=cert' \
  "$d/emSign_ECC_Root_CA_-_G3.pem"

trust extract --overwrite --format=pem-bundle \
  --filter='pkcs11:object=Comodo%20AAA%20Services%20root;type=cert' \
  "$d/Comodo_AAA_Services_root.pem"

trust extract --overwrite --format=pem-bundle \
  --filter='pkcs11:object=emSign%20ECC%20Root%20CA%20-%20C3;type=cert' \
  "$d/emSign_ECC_Root_CA_-_C3.pem"

trust extract --overwrite --format=pem-bundle \
  --filter='pkcs11:object=emSign%20Root%20CA%20-%20C1;type=cert' \
  "$d/emSign_Root_CA_-_C1.pem"

update-ca-trust extract
```

步驟 3:在GuestShell中驗證不受信任的證書

使用下面的驗證命令，驗證提取的四個證書是否出現在系統不信任/阻止清單策略中，是否從活動信任錨點中排除。該命令確認證書已在阻止清單策略中註冊。

```
###Verify with below command
[guestshell@guestshell ~]$ trust list --filter=trust-policy --purpose=server-auth | grep -E -A3 'emSign
    label: AAA Certificate Services
    trust: distrusted
    category: authority

--
    label: emSign ECC Root CA - C3
    trust: distrusted
    category: authority

--
    label: emSign ECC Root CA - G3
    trust: distrusted
    category: authority

--
    label: emSign Root CA - C1
    trust: distrusted
    category: authority

--
    label: emSign Root CA - G1
    trust: anchor
    category: authority

Output will vary based on CentOS Stream version
```

```
###Verify CentOS Stream Version
[guestshell@guestshell ~]$ cat /etc/redhat-release
CentOS Stream release 8

OS                          CentOS Stream 8       CentOS Stream 9
Directory                   blacklist only        blocklist
Result shown                 trust: blacklisted    trust: distrusted
```

步驟 4:狀態永續性和容器生命週期

有關容器永續性的附註：由於/etc/pki/ca-trust駐留在永久容器儲存上，因此這些證書不信任修改在「guestshell enable」和「guestshell disable」操作期間會一直存在，並且裝置會重新啟動。

返回到DEPLOYED狀態（如果適用）：如果GuestShell最初處於DEPLOYED狀態並僅被啟用以執行此不信任過程，請通過從IOS特權EXEC提示符退出bash並運行「guestshell disable」來將GuestShell返回到其先前的停止狀態：

<#root>

```
[root@guestshell ~]#

exit

[guestshell@guestshell ~]$

exit

Router#

guestshell disable
```

生命週期的重要注意事項：如果用「guestshell destroy」完全銷毀GuestShell，則會刪除容器檔案系統。如果隨後重新啟用GuestShell，則會從基本系統映像重新建立容器，並且必須重新應用這些不信任的修正步驟。

步驟 5:回滾過程（還原CA信任）

要撤銷不信任配置並恢復所有Cisco IOS XE版本中的預設CA信任，請動態選擇活動阻止清單目錄($d)，專門刪除通過此過程新增的四個證書檔案（包括Comodo AAA服務根），然後重建信任儲存：

<#root>

```
! Escalate to root user inside GuestShell:
```

```
[guestshell@guestshell ~]$
```

```
sudo -s
```

```
d=/etc/pki/ca-trust/source/blocklist
[ -d "$d" ] || d=/etc/pki/ca-trust/source/blacklist

! Remove only the four certificate files added during remediation:
rm -f "$d/emSign_ECC_Root_CA_-_G3.pem" "$d/Comodo_AAA_Services_root.pem" \
      "$d/emSign_ECC_Root_CA_-_C3.pem" "$d/emSign_Root_CA_-_C1.pem"

! Rebuild the system CA trust store:
update-ca-trust extract
```

驗證阻止清單目錄是否不再包含刪除的檔案：

<#root>

```
[root@guestshell ~]#
```

```
ls -l "$d"/
```

```
total 0
```

確認CA信任恢復：通過重新運行第3步驗證命令，驗證所有五個證書是否都已返回活動信任金鑰(所有條目都報告信任：錨):

<#root>

```
[root@guestshell ~]#
```

```
trust list --filter=trust-policy --purpose=server-auth | grep -E -A3 'emSign|AAA'
```

```
    trust: anchor
    trust: anchor
    trust: anchor
    trust: anchor
    trust: anchor
```

端到端執行記錄示例

該抄表說明了Cisco IOS XE裝置上的完整、成功的GuestShell稽核、補救和驗證會話：

<#root>

```
Router#

guestshell run bash

[guestshell@guestshell ~]$ sudo -s
bash-4.4#

d=/etc/pki/ca-trust/source/blocklist

bash-4.4#

[ -d "$d" ] || d=/etc/pki/ca-trust/source/blacklist

bash-4.4#

mkdir -p "$d"

bash-4.4#

trust extract --overwrite --format=pem-bundle \ >   --filter='pkcs11:object=emSign%20ECC%20Root%20CA%20-

bash-4.4#

trust extract --overwrite --format=pem-bundle \ >   --filter='pkcs11:object=Comodo%20AAA%20Services%20ro

bash-4.4#

trust extract --overwrite --format=pem-bundle \ >   --filter='pkcs11:object=emSign%20ECC%20Root%20CA%20-

bash-4.4#

trust extract --overwrite --format=pem-bundle \ >   --filter='pkcs11:object=emSign%20Root%20CA%20-%20C1;

bash-4.4#

update-ca-trust extract

bash-4.4#

trust list --filter=trust-policy --purpose=server-auth | grep -E -A3 'emSign|AAA'

    label: emSign ECC Root CA - G3
    trust: blacklisted
    category: authority

--
    label: AAA Certificate Services
    trust: blacklisted
    category: authority

--
    label: emSign ECC Root CA - C3
```

```
    trust: blacklisted
    category: authority

--
    label: emSign Root CA - C1
    trust: blacklisted
    category: authority

--
    label: emSign Root CA - G1
    trust: anchor
    category: authority

bash-4.4#

cat /etc/redhat-release

CentOS Stream release 8
bash-4.4#

d=/etc/pki/ca-trust/source/blocklist

bash-4.4#

[ -d "$d" ] || d=/etc/pki/ca-trust/source/blacklist

bash-4.4#

rm -f "$d/emSign_ECC_Root_CA_-_G3.pem" "$d/Comodo_AAA_Services_root.pem" \ >       "$d/emSign_ECC_Root_C

bash-4.4#
bash-4.4#

update-ca-trust extract

bash-4.4#

ls -l "$d"/

total 0
```

命令摘要矩陣

| 操作任務 | |
|---|---|
| 稽核 GuestShell狀態 | show app-hosting list |

| | |
|---|---|
| 啟用GuestShell（如果已部署） | `guestshell enable` |
| 輸入GuestShell Bash | `guestshell run bash` |
| 切換到根使用者 | `sudo -s` |
| 準備阻止清單目錄 | `d=/etc/pki/ca-trust/source/blocklist; [ -d "$d" ] \|\| d=/etc/pki/ca-trust/source/blacklis` |
| 將CA提取到阻止清單 | `trust extract --overwrite --format=pem-bundle ... (x4 CAs)` |
| 重建CA信任儲存 | `update-ca-trust extract` |
| 驗證不信任策略 | `trust list --filter=trust-policy --purpose=server-auth` |
| 恢復已部署狀態（可選） | `guestshell disable` |
| 回滾/恢復信任 | `rm -f "$d/emSign_ECC_Root_CA_-_G3.pem" "$d/Comodo_AAA_Services_root.pem" "$d/emSign_ECC_` |

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）。