

# 使用當前證書中的資訊生成新的Expressway證書

。

## 目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[設定](#)

[步驟1.查詢當前證書資訊。](#)

[步驟2.使用上述資訊建立新的CSR。](#)

[步驟3.驗證並下載新的CSR。](#)

[步驟4.驗證新證書中包含的資訊。](#)

[步驟5.將新CA證書上傳到Servers Trusted Store \( 如果適用 \) 。](#)

[步驟6.將新證書上傳到Expressway伺服器。](#)

[驗證](#)

[疑難排解](#)

## 簡介

本文說明如何使用現有Expressway憑證中的資訊產生新的憑證簽署請求(CSR)。

## 必要條件

### 需求

思科建議您瞭解以下主題：

- 證書屬性
- Expressway或影片通訊伺服器(VCS)

### 採用元件

本文件所述內容不限於特定軟體和硬體版本。

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。

## 設定

**步驟1.查詢當前證書資訊。**

若要獲取當前證書中包含的資訊，請在Expressway圖形使用者介面(GUI)上導航到**維護>安全>伺服器證書**。

找到**Server certificate data**部分，然後選擇**Show(decoded)**。

在**Common Name(CN)**和**Subject Alternative Name(SAN)**中查詢資訊，如下圖所示：

```
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number:
      35:00:00:00:a1:4b:f0:c2:00:f6:dd:70:05:00:00:00:00:00:a1
    Signature Algorithm: sha256WithRSAEncryption
    Issuer: DC=local, DC=anmiron, CN=anmiron-SRV-AD-CA
    Validity
      Not Before: Dec  2 04:39:57 2019 GMT
      Not After : Nov 28 00:32:43 2020 GMT
    Subject: C=MX, ST=CDMX, L=CDMX, O=TAC, OU=TAC, CN=expe.domain.com
    Subject Public Key Info:
      Public Key Algorithm: rsaEncryption
      Public-Key: (4096 bit)
      Modulus:
        -----
X509v3 extensions:
  X509v3 Key Usage: critical
    Digital Signature, Key Encipherment
  X509v3 Extended Key Usage:
    TLS Web Client Authentication, TLS Web Server Authentication
  X509v3 Subject Alternative Name:
    DNS:expe.domain.com, DNS:domain.com
  X509v3 Subject Key Identifier:
    92:D0:D7:24:4A:BC:E3:C0:02:E5:7E:09:5D:78:FF:56:7A:6E:37:5B
  X509v3 Authority Key Identifier:
    keyid:6C:71:80:4C:9A:21:79:DB:C2:7E:23:7A:DB:9B:73:11:E4:35:61:32
```

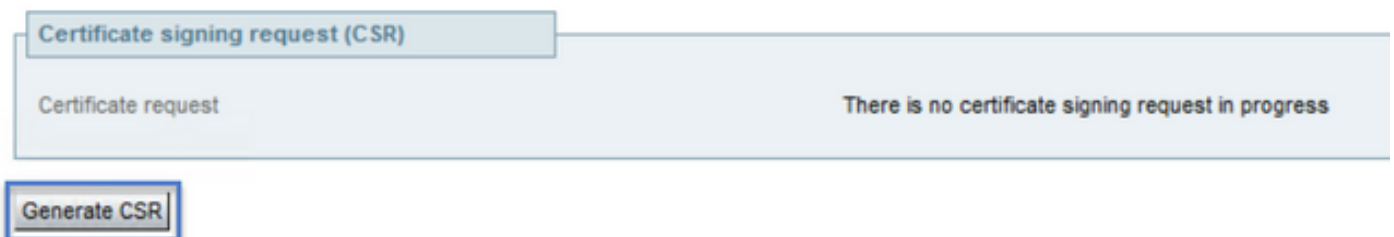
現在您已知道CN和SAN的複製它們以便可以將其新增到新的CSR。

或者，您可以複製證書的其他資訊，如國家(C)、州(ST)、地點(L)、組織(O)、組織單位(OU)。此資訊在CN旁邊。

## 步驟2.使用上述資訊建立新的CSR。

若要建立CSR，請導覽至**Maintenance > Security > Server Certificate**。

找到**憑證簽署請求(CSR)**一節，然後選擇**產生CSR**，如下圖所示：



輸入從當前證書收集的值。

除非該CN是群集，否則無法對其進行修改。對於群集，可以選擇CN作為Expressway完全限定域名(FQDN)或群集FQDN。本檔案使用單一伺服器，因此CN與從目前憑證中獲得的內容相符，如下圖所示：

**Generate CSR**

Common name

Common name

FQDN of Expressway

Common name as it will appear

expe.domain.com

對於SAN，您必須手動輸入值，以防這些值未自動填充，為此，您可以在**其他替代名稱**中輸入值，如果您有多個SAN，這些值必須以逗號分隔，例如：example1.domain.com、example2.domain.com、example3.domain.com。新增後，SAN將列在「Alternative name as it will appear(備用名稱，如圖所示)」部分，如下所示：

Alternative name

Additional alternative names (comma separated)

domain.com

Unified CM registrations domains

Format

DNS

Alternative name as it will appear

DNS:domain.com

**Additional information**是必填資訊，如果沒有自動填充或必須對其進行更改，則必須手動輸入，如下圖所示：

**Additional information**

Key length (in bits)

4096

Digest algorithm

SHA-256

Country

MX

State or province

CDMX

Locality (town name)

CDMX

Organization (company name)

TAC

Organizational unit

TAC

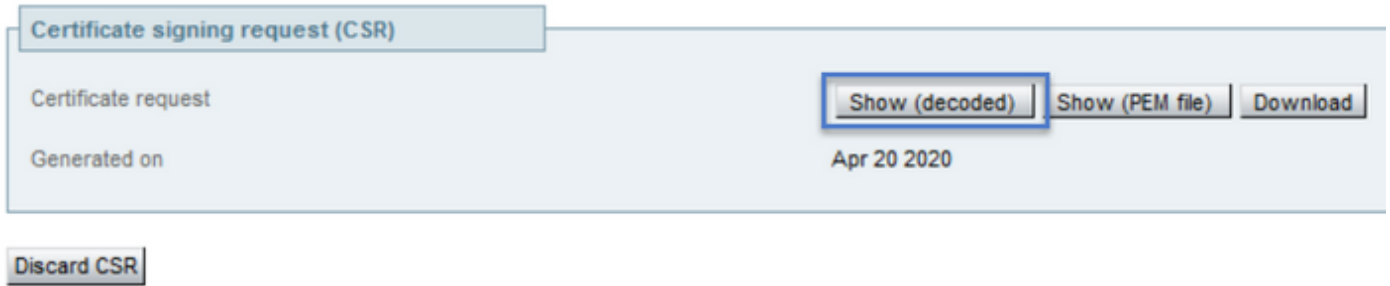
Email address

**Generate CSR**

完成後，選擇**Generate CSR**。

### 步驟3.驗證並下載新的CSR。

產生CSR後，您可以在「**Certificate signing request(CSR)**」一節中選擇**Show(decoded)**，以驗證所有SAN是否存在，如下圖所示：



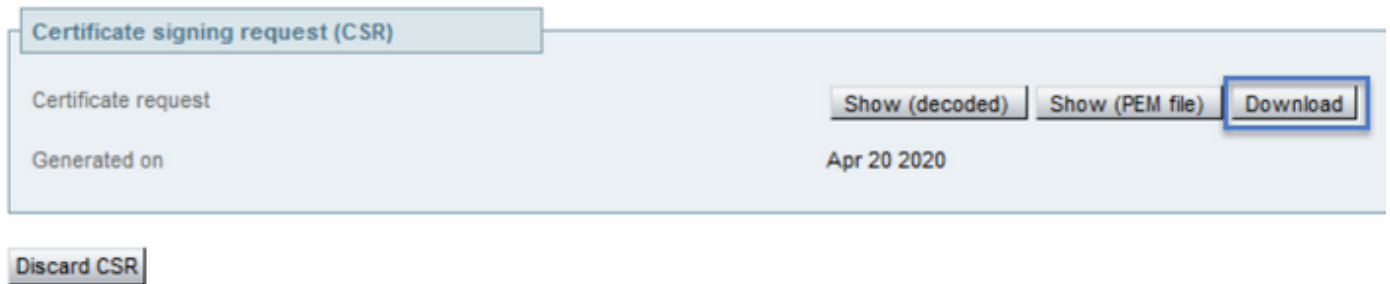
在新視窗中查詢CN和Subject Alternative Name，如下圖所示：

```
Certificate Request:
Data:
  Version: 0 (0x0)
  Subject: OU=TAC, O=TAC, CN=expe.domain.com, ST=CDMX, C=MX, L=CDMX
  Subject Public Key Info:
    Public Key Algorithm: rsaEncryption
    Public-Key: (4096 bit)
    Modulus:
```

CN始終自動新增為SAN:

```
X509v3 Extended Key Usage:
  TLS Web Server Authentication, TLS Web Client Authentication
X509v3 Subject Alternative Name:
  DNS:expe.domain.com, DNS:domain.com
Signature Algorithm: sha256WithRSAEncryption
```

現在，CSR已經過驗證，您可以關閉新視窗，然後在「憑證簽署請求(CSR)」區段上選擇Download(decoded)，如下圖所示：

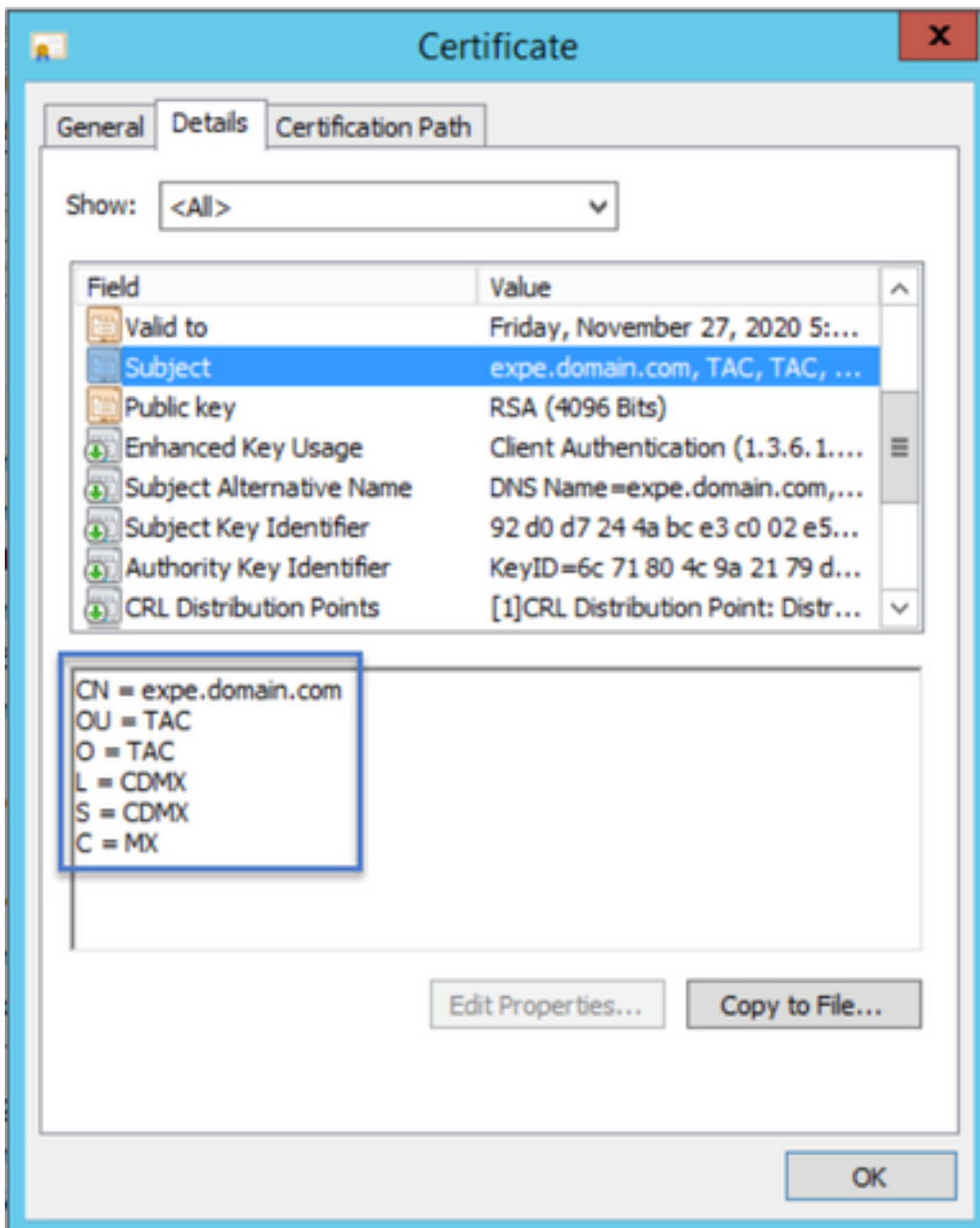


下載後，您可以將新CSR傳送到您的憑證授權單位(CA)以簽署。

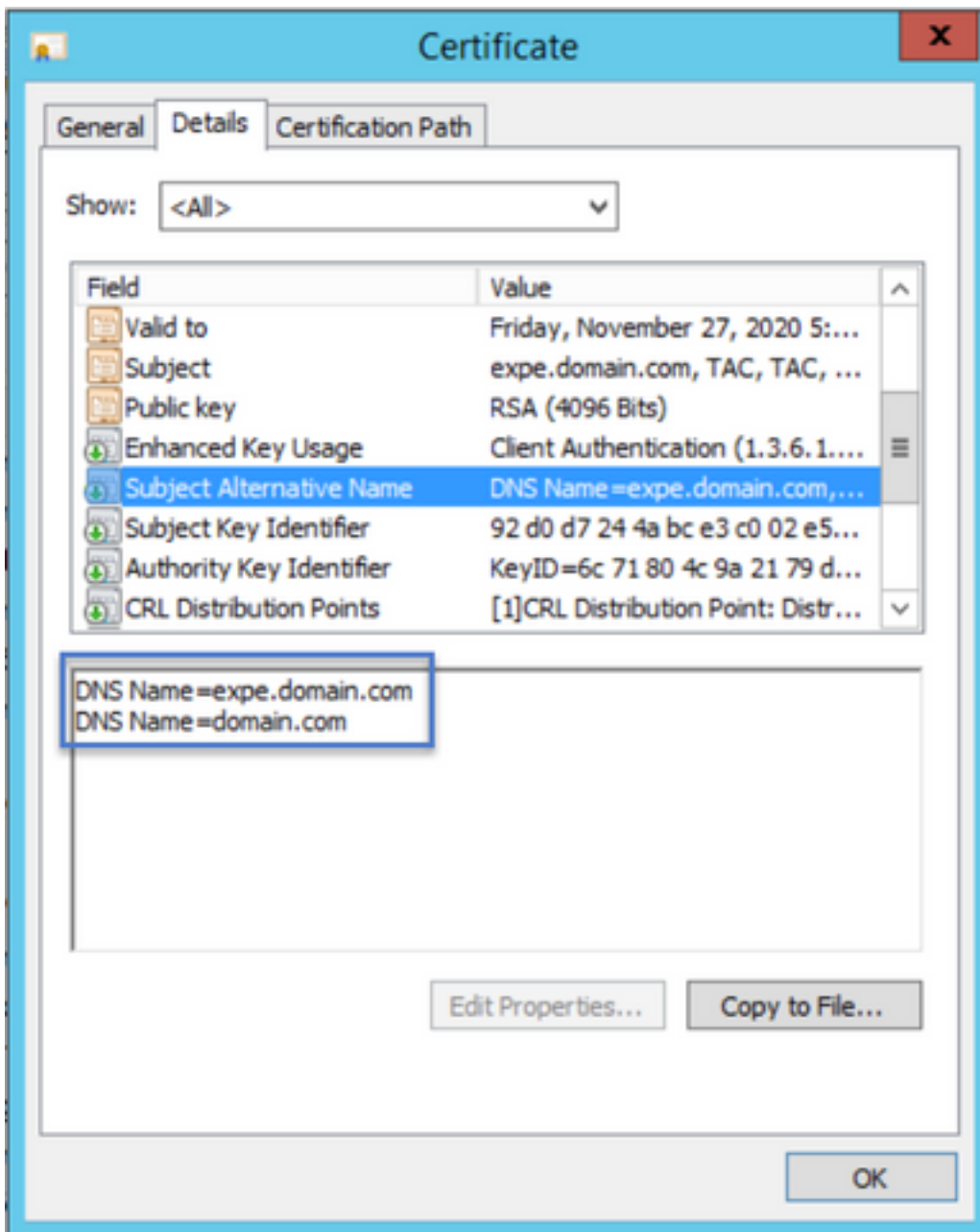
#### 步驟4. 驗證新證書中包含的資訊。

從CA傳回新憑證後，您可以驗證憑證中是否存在所有SAN。為此，您可以開啟證書並查詢SAN屬性。在本文檔中，Windows PC用於檢視屬性，只要您可以開啟或解碼證書來檢視屬性，這不是唯一的方法。

開啟憑證並導覽至Details索引標籤，然後尋找Subject，它應包含CN和其他資訊，如下圖所示：



另請檢視**使用者替代名稱**一節，它必須包含您在CSR中輸入的SAN，如下圖所示：



如果您在CSR中輸入的所有SAN在新憑證中都不存在，請與CA連線，檢視您的憑證是否允許額外的SAN。

### 步驟5.將新CA證書上傳到Servers Trusted Store ( 如果適用 )。

如果CA與簽署舊Expressway證書的CA相同，則可以放棄此步驟。如果它是不同的CA，則必須將新的CA證書上傳到每個Expressway伺服器中的受信任CA清單。如果在Expressway之間（例如Expressway-C和Expressway-E之間）有傳輸層安全(TLS)區域，則必須將新CA上傳到兩台伺服器上，以便它們可以相互信任。

為此，您可以逐一上傳CA憑證。在Expressway上導航到**Maintenance > Security > Trusted CA certificates**。

1. 選擇**瀏覽**。
2. 在新頁面上，選擇CA證書。
3. 選擇**附加CA證書**。

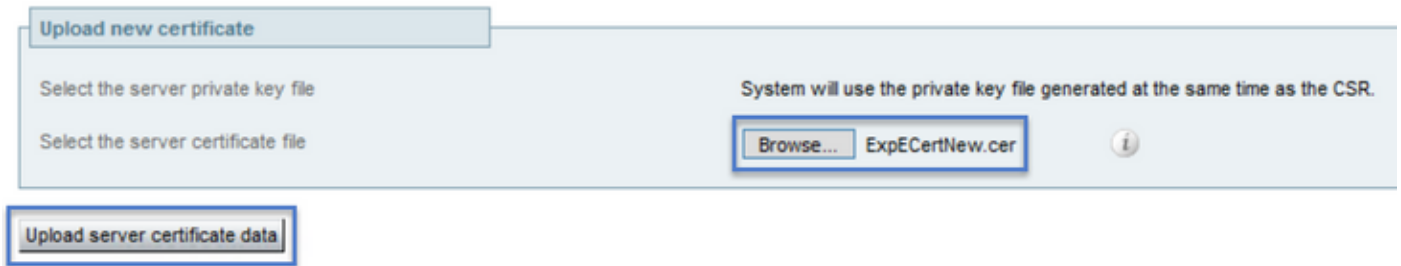
此過程必須針對證書鏈中的每個CA證書（根證書和中間證書）完成，而且必須針對所有Expressway伺服器完成，即使這些伺服器已群集。

## 步驟6.將新證書上傳到Expressway伺服器。

如果新憑證中的所有資訊都正確，若要上傳新憑證，請導覽至：**Maintenance > Security > Server Certificate**。

找到**Upload new certificate**一節，如下圖所示：

1. 在「**Select the server certificate file**」部分中選擇**Browse**。
2. 選擇新證書。
3. 選擇上傳伺服器證書資料。



Upload new certificate

Select the server private key file

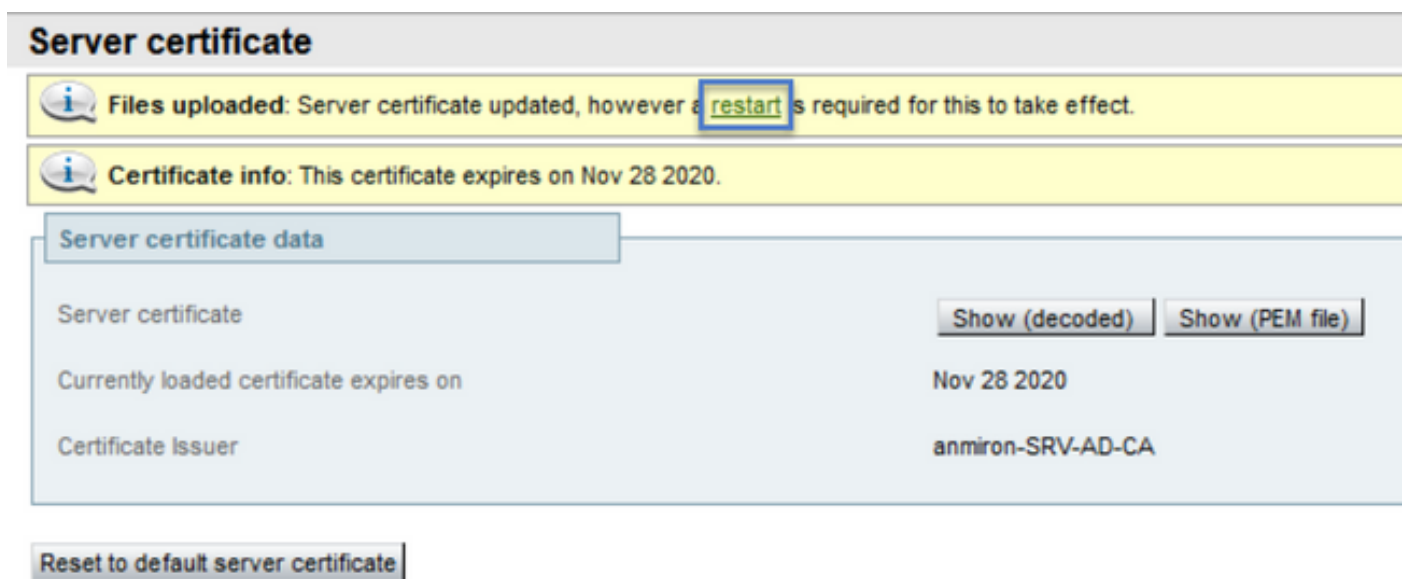
Select the server certificate file

System will use the private key file generated at the same time as the CSR.

Browse... ExpECertNew.cer

Upload server certificate data

如果Expressway接受新證書，則Expressway會提示重新啟動以應用更改，並且消息顯示證書的新到期日期，如下圖所示：



Server certificate

Files uploaded: Server certificate updated, however a restart is required for this to take effect.

Certificate info: This certificate expires on Nov 28 2020.

Server certificate data

Server certificate	Show (decoded)	Show (PEM file)
Currently loaded certificate expires on	Nov 28 2020	
Certificate Issuer	anmiron-SRV-AD-CA	

Reset to default server certificate

要重新啟動Expressway，請選擇**restat**。

## 驗證

伺服器恢復後，新證書必須已安裝，您可以導航到：**Maintenance > Security > Server Certificate**以進行確認。

找到**Server certificate data**並查詢**Currently loaded certificate expires on**部分，其中顯示證書的新到期日期，如下圖所示：

## Server certificate

### Server certificate data

Server certificate

Show (decoded)

Show (PEM file)

Currently loaded certificate expires on

Nov 28 2020

Certificate Issuer

anmiron-SRV-AD-CA

Reset to default server certificate

## 疑難排解

目前尚無適用於此組態的具體疑難排解資訊。