

在Cisco VPN 3000集中器上通過HTTP進行CRL檢查

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[慣例](#)

[網路圖表](#)

[配置VPN 3000 Concentrator](#)

[逐步說明](#)

[監控](#)

[驗證](#)

[來自集中器的日誌](#)

[成功的集中器日誌](#)

[失敗的日誌](#)

[疑難排解](#)

[相關資訊](#)

簡介

本文檔介紹如何使用HTTP模式對安裝在Cisco VPN 3000集中器中的證書頒發機構(CA)證書啟用證書吊銷清單(CRL)檢查。

通常情況下，憑證預期在整個有效期內有效。但是，如果證書由於諸如名稱更改、主體和CA之間的關聯更改以及安全威脅等原因變得無效，CA將撤銷證書。在X.509中，CA通過定期發出已簽名的CRL來撤銷證書，其中每個被撤銷的證書由其序列號標識。啟用CRL檢查意味著每次VPN集中器使用證書進行身份驗證時，都會檢查CRL以確保正在驗證的證書沒有被吊銷。

CA使用輕量型目錄訪問協定(LDAP)/HTTP資料庫來儲存和分發CRL。它們也可能使用其他方法，但VPN集中器依賴於LDAP/HTTP訪問。

HTTP CRL檢查是在VPN集中器3.6版或更高版本中引入的。但是，在早期的3.x版本中引入了基於LDAP的CRL檢查。本文檔僅討論使用HTTP進行CRL檢查。

注意：VPN 3000系列集中器的CRL快取大小取決於平台，無法根據管理員的意願進行配置。

必要條件

需求

嘗試此組態之前，請確保符合以下要求：

- 您已使用用於網際網路金鑰交換(IKE)身份驗證的證書 (未啟用CRL檢查) 從VPN 3.x硬體客戶端成功建立IPsec隧道。
- 您的VPN集中器始終可以連線到CA伺服器。
- 如果您的CA伺服器已連線到公共介面，則您已經在公共 (預設) 過濾器中開啟了必要的規則。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- VPN 3000集中器版本4.0.1 C
- VPN 3.x硬體使用者端
- Microsoft CA伺服器，用於在Windows 2000伺服器上運行證書生成和CRL檢查。

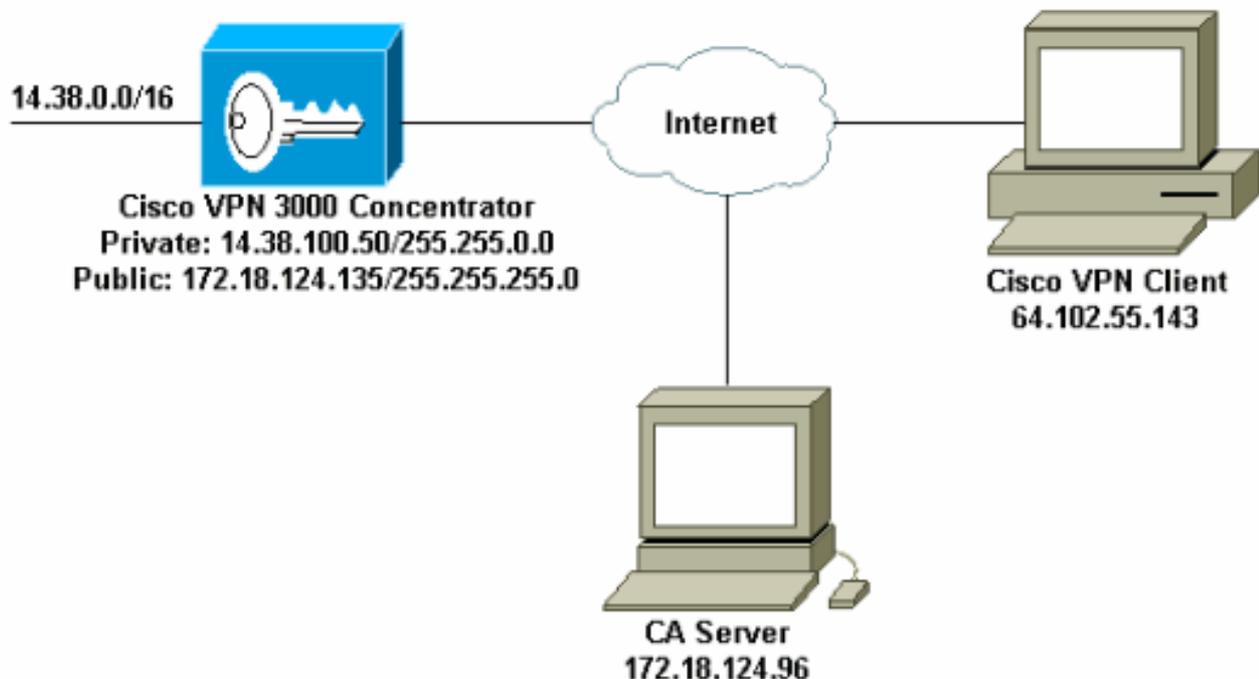
本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除 (預設) 的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

慣例

請參閱[思科技術提示慣例以瞭解更多有關文件慣例的資訊。](#)

網路圖表

本檔案會使用以下網路設定：

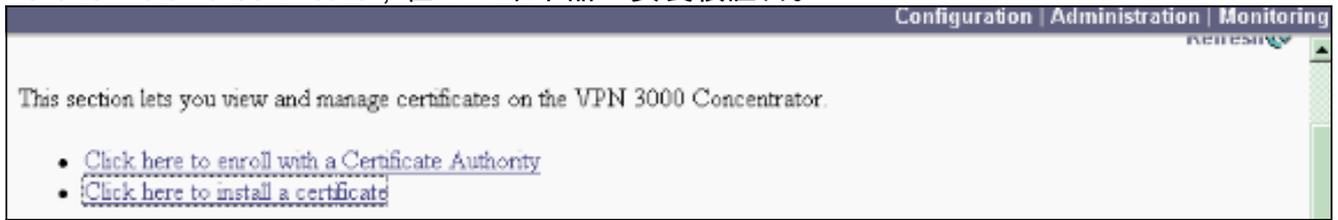


配置VPN 3000 Concentrator

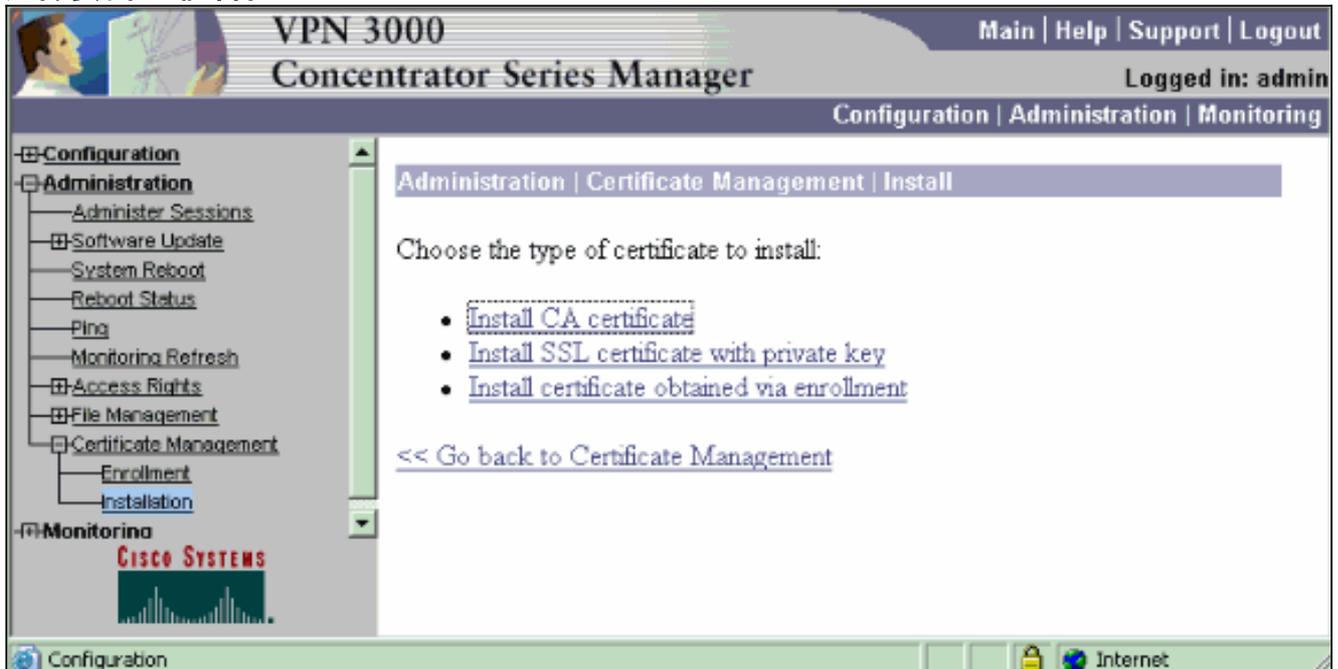
逐步說明

完成以下步驟以配置VPN 3000集中器：

1. 如果您沒有證書，請選擇Administration > Certificate Management以請求證書。選擇Click here to install a certificate，在VPN集中器上安裝根證書。



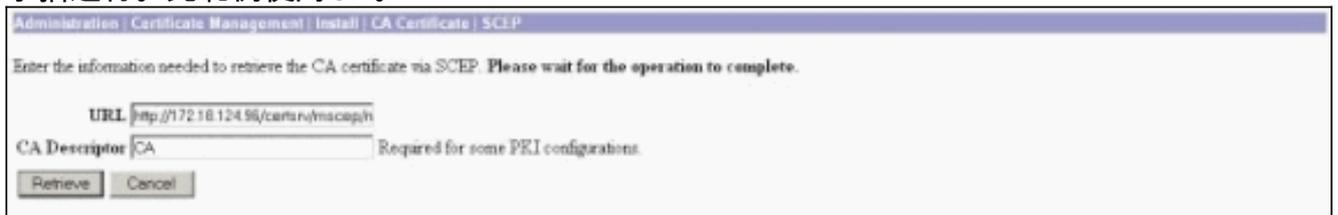
2. 選擇安裝CA證書。



3. 選擇SCEP (簡單證書註冊協定) 以檢索CA證書。



4. 在SCEP視窗中，在URL對話方塊中輸入CA伺服器的完整URL。在本示例中，CA伺服器的IP地址是172.18.124.96。由於本示例使用Microsoft的CA伺服器，因此完整的URL是http://172.18.124.96/certsrv/mscep/mscep.dll。接下來，在「CA描述符」對話方塊中輸入單字描述符。此範例使用CA。



5. 按一下「Retrieve」。您的CA證書應顯示在「管理」>「證書管理」視窗下。如果您沒有看到憑證，請返回步驟1，然後再次執行程式。

Administration | Certificate Management Thursday, 13 August 2003 11:45:41
Refresh

This section lets you view and manage certificates on the VPN 3000 Concentrator.

- [Click here to enroll with a Certificate Authority](#)
- [Click here to install a certificate](#)

Certificate Authorities [[View All CAs](#)] [[Clear All CAs](#)] (current: 3, maximum: 20)

Subject	Issuer	Expiration	SCEP Issuer	Actions
janb-ca-ra at Cisco Systems	janb-ca-ra at Cisco Systems	03/12/2005	Yes	View Configure Delete SCEP Show RA's

Identity Certificates (current: 0, maximum: 20)

Subject	Issuer	Expiration	Actions
No Identity Certificates			

SSL Certificate [[Generate](#)] *Note: The public key in the SSL certificate is also used for the SSH host key.*

Subject	Issuer	Expiration	Actions
14.38.100.50 at Cisco Systems, Inc.	14.38.100.50 at Cisco Systems, Inc.	08/14/2005	View Renew Delete

Enrollment Status [[Remove All Errors](#)] [[Timed Out](#)] [[Rejected](#)] [[Cancelled](#)] [[In Progress](#)] (current: 0 available: 20)

Subject	Issuer	Date	Use	Reason	Method	Status	Actions
No Enrollment Requests							

6. 擁有CA證書後，選擇Administration > Certificate Management > Enroll，然後按一下Identity certificate。

Administration | Certificate Management | Enroll

This section allows you to create an SSL or identity certificate request. The identity certificate request allows the VPN 3000 Concentrator to be enrolled into the PKI. The certificate request can be sent to a CA, which will issue a certificate. The CA's certificate *must* be installed as a Certificate Authority before installing the certificate you requested.

Choose the type of certificate request to create:

- [Identity certificate](#)
- [SSL certificate](#)

[<< Go back to Certificate Management](#)

7. 按一下Enroll via SCEP at ...以申請身份證書。

Administration | Certificate Management | Enroll | Identity Certificate

Select the enrollment method for the identity certificate. To install a certificate with SCEP, the issuing CA's certificate must also be installed with SCEP. [Click here to install a new CA using SCEP before enrolling.](#)

- [Enroll via PKCS10 Request \(Manual\)](#)
- [Enroll via SCEP at janb-ca-ra at Cisco Systems](#)

[<< Go back and choose a different type of certificate](#)

8. 完成以下步驟以填寫登錄檔：在Common Name(CN)欄位中，輸入要用於公鑰基礎設施(PKI)中的VPN集中器的公用名稱。在組織單位(OU)欄位中輸入您的部門。OU應與配置的IPsec組名稱匹配。在「組織(O)」欄位中輸入您的組織或公司。在Locality(L)欄位中輸入您的城市或城鎮。在「省/市/自治區(SP)」欄位中輸入您的省/市/自治區。在「國家/地區(C)」欄位中輸入您的國家/地區。在Fully Qualified Domain Name(FQDN)欄位中輸入要在PKI中使用的VPN集中器的完全限定域名(FQDN)。在Subject Alternative Name(email Address)欄位中，輸入要在PKI中使用的VPN集中器的電子郵件地址。在Challenge Password欄位中輸入證書請求的質詢密碼。在Verify Challenge Password欄位中重新輸入質詢密碼。從Key Size下拉選單中選擇生成的RSA金鑰對的金鑰大小。

Administration | Certificate Management | Enroll | Identity Certificate | SCEP

Enter the information to be included in the certificate request. Please wait for the operation to finish.

Common Name (CN) Enter the common name for the VPN 3000 Concentrator to be used in this PKI.

Organizational Unit (OU) Enter the department.

Organization (O) Enter the Organization or company.

Locality (L) Enter the city or town.

State/Province (SP) Enter the State or Province.

Country (C) Enter the two-letter country abbreviation (e.g. United States = US).

Subject AlternativeName (FQDN) Enter the Fully Qualified Domain Name for the VPN 3000 Concentrator to be used in this PKI.

Subject AlternativeName (E-Mail Address) Enter the E-Mail Address for the VPN 3000 Concentrator to be used in this PKI.

Challenge Password Enter and verify the challenge password for this certificate request.

Verify Challenge Password

Key Size Select the key size for the generated RSA key pair.

9. 選擇**Enroll**並在輪詢狀態下檢視SCEP狀態。

10. 轉到您的CA伺服器以批准身份證書。在CA伺服器上批准後，您的SCEP狀態應為「已安裝」。

Administration | Certificate Management | Enrollment | Request Generated

A certificate request has been generated.

SCEP Status: Installed

- [Go to Certificate Management](#)
- [Go to Certificate Enrollment](#)
- [Go to Certificate Installation](#)

11. 在Certificate Management下，您應該會看到您的身份證書。如果沒有，請檢查CA伺服器上的日誌以瞭解更多疑難解答。

Administration | Certificate Management Thursday, 15 August 2002 11:50:14
Refresh

This section lets you view and manage certificates on the VPN 3000 Concentrator.

- [Click here to enroll with a Certificate Authority](#)
- [Click here to install a certificate](#)

Certificate Authorities [View All CRL Caches | Clear All CRL Caches] (current: 3, maximum: 20)

Subject	Issuer	Expiration	SCEP Issuer	Actions
janzb-ca-ra at Cisco Systems	janzb-ca-ra at Cisco Systems	03/12/2005	Yes	View Configure Delete SCEP Show RA's

Identity Certificates (current: 1, maximum: 20)

Subject	Issuer	Expiration	Actions
Concentrator_cert at Cisco	janzb-ca-ra at Cisco Systems	08/15/2003	View Banner Delete

SSL Certificate [Generate] *Note: The public key in the SSL certificate is also used for the SSH host key.*

Subject	Issuer	Expiration	Actions
14.38.100.50 at Cisco Systems, Inc.	14.38.100.50 at Cisco Systems, Inc.	08/14/2005	View Remove Delete

Enrollment Status [Remove All | Errored | Timed-Out | Rejected | Cancelled | In-Progress] (current: 0 available: 19)

Subject	Issuer	Date	Use	Reason	Method	Status	Actions
No Enrollment Requests							

12. 在收到的證書上選擇**View**，檢視證書是否具有CRL分發點(CDP)。CDP列出來自此證書頒發者的所有CRL分發點。如果您的憑證上具有CDP，且使用DNS名稱向CA伺服器傳送查詢，請確保在VPN集中器中定義了DNS伺服器，以使用IP位址解析主機名稱。在本例中，示例CA伺服器的主機名為janzib-pc，它解析為DNS伺服器上的IP地址172.18.124.96。



13. 按一下CA證書上的**Configure**以對收到的證書啟用CRL檢查。如果對收到的證書具有CDP並且想要使用它，則從正在檢查的證書中選擇「**使用CRL分發點**」。由於系統必須從網路分發點檢索並檢查CRL，啟用CRL檢查可能會降低系統響應時間。此外，如果網路速度慢或擁塞，CRL檢查可能會失敗。啟用CRL快取以緩解這些潛在問題。這會將檢索到的CRL儲存在本地易失性儲存器中，因此允許VPN集中器更快速地驗證證書的吊銷狀態。啟用CRL快取後，VPN集中器首先檢查快取中是否存在所需的CRL，並在需要檢查證書的撤銷狀態時根據CRL中的序列號清單檢查證書的序列號。如果找到此證書的序列號，則該證書被視為已吊銷。VPN集中器從外部伺服器檢索CRL，當它在快取中找不到所需的CRL、當快取的CRL的有效期已過期時，或者當配置的刷新時間已過時。當VPN集中器從外部伺服器收到新的CRL時，它會用新的CRL更新快取。快取最多可包含64個CRL。**註**：CRL快取存在於記憶體中。因此，重新啟動VPN集中器會清除CRL快取。VPN集中器在處理新的對等身份驗證請求時，使用更新的CRL重新填充CRL快取。如果您選擇**使用靜態CRL分發點**，則最多可以使用五個靜態CRL分發點，如本視窗中所指定。如果選擇此選項，您必須至少輸入一個URL。您還可以從要檢查的證書中選擇**使用CRL分發點**，或者選擇**使用靜態CRL分發點**。如果VPN集中器無法在證書中找到五個CRL分發點，則會新增靜態CRL分發點，最多五個。如果選擇此選項，請至少啟用一個CRL分發點協定。您還必須輸入至少一個（且最多五個）靜態CRL分發點。如果要禁用CRL檢查，請選擇**No CRL Checking**。在CRL快取下，選擇**Enabled**框以允許VPN集中器快取檢索到的CRL。預設情況下不啟用CRL快取。禁用CRL快取時（取消選中該框），CRL快取將被清除。如果配置了CRL檢索策略，該策略使用來自所檢查證書的CRL分發點，請選擇用於檢索CRL的分發點協定。在此案例中選擇**HTTP**以檢索CRL。如果CA伺服器指向公共介面，請將HTTP規則分配給公共介面過濾器。

Administration | Certificate Management | Configure CA Certificate

Certificate jazib-ca-ra at Cisco Systems

CRL Retrieval Policy

Use CRL distribution points from the certificate being checked
 Use static CRL distribution points
 Use CRL distribution points from the certificate being checked or else use static CRL distribution points
 No CRL checking

Choose the method to use to retrieve the CRL.

CRL Caching

Enabled
 Disabled

Check to enable CRL caching. Disabling will clear CRL cache.

Refresh Time:

Enter the refresh time in minutes (5 - 1440). Enter 0 to use the Next Update field in the cached CRL.

CRL Distribution Points Protocols

HTTP
 LDAP

Choose a distribution point protocol to use to retrieve the CRL. If you choose HTTP, be sure to assign HTTP rules to the public interface filter. (For more information, click Help.) If you choose LDAP, configure the LDAP distribution point defaults below.

LDAP Distribution Point Defaults

Server:
 Server Port:
 Login DN:
 Password:
 Verify:

Enter the hostname or IP address of the server.
 Enter the port number of the server. The default port is 389.
 Enter the login DN for access to the CRL on the server.
 Enter the password for the login DN.
 Verify the password for the login DN.

Static CRL Distribution Points

LDAP or HTTP URLs:

- Enter up to 5 URLs to use to retrieve the CRL from the server.
- Enter each URL on a new line.

Certificate Acceptance Policy

Accept Subordinate CA Certificates
 Accept Identity Certificates signed by this issuer

Apply Cancel

監控

選擇 **Administration > Certificate Management**，然後按一下 **View All CRL cache**，檢視VPN集中器是否已快取來自CA伺服器的任何CRL。

驗證

本節提供的資訊可用於確認您的組態是否正常運作。

來自集中器的日誌

在VPN集中器上啟用這些事件，以確保CRL檢查正常工作。

1. 選擇 **Configuration > System > Events > Classes** 以設定日誌記錄級別。
2. 在Class Name下，選擇IKE、IKEDBG、IPSEC、IPSECDBG或CERT。
3. 按一下 **Add** 或 **Modify**，然後選擇 **Severity to Log** 選項1-13。
4. 如果要修改，請按一下 **Apply**，如果要新增新條目，請按一下 **Add**。

成功的集中器日誌

如果CRL檢查成功，這些消息將在可過濾事件日誌中看到。

```
1315 08/15/2002 13:11:23.520 SEV=7 CERT/117 RPT=1
The requested CRL was found in cache.
The CRL Distribution point is: http://jazib-pc/CertEnroll/jazib-ca-ra.crl
```

1317 08/15/2002 13:11:23.520 SEV=8 CERT/46 RPT=1
CERT_CheckCrl(62f56e8, 0, 0)

1318 08/15/2002 13:11:23.520 SEV=7 CERT/2 RPT=1
Certificate has not been revoked: session = 2

1319 08/15/2002 13:11:23.530 SEV=8 CERT/50 RPT=1
CERT_Callback(62f56e8, 0, 0)

1320 08/15/2002 13:11:23.530 SEV=5 IKE/79 RPT=2 64.102.60.53
Group [ipseccgroup]
Validation of certificate successful
(CN=client_cert, SN=61521511000000000086)

有關成功的集中器日誌的完整輸出，請參閱[成功的集中器日誌](#)。

[失敗的日誌](#)

如果您的CRL簽入不成功，這些消息將在可過濾事件日誌中看到。

1332 08/15/2002 18:00:36.730 SEV=7 CERT/6 RPT=2
Failed to retrieve revocation list: session = 5

1333 08/15/2002 18:00:36.730 SEV=7 CERT/114 RPT=2
CRL retrieval over HTTP has failed. Please make sure that proper filter rules
have been configured.

1335 08/15/2002 18:00:36.730 SEV=7 CERT/8 RPT=2
Error processing revocation list: session = 5, reason = Failed to retrieve CRL
from the server.

請參閱[撤銷的集中器日誌](#)，瞭解失敗集中器日誌的完整輸出。

有關成功的客戶端日誌的完整輸出，請參閱[成功的客戶端日誌](#)。

請參閱[已撤銷的客戶端日誌](#)以瞭解失敗的客戶端日誌的完整輸出。

[疑難排解](#)

有關故障排除的詳細資訊，請參閱[排除VPN 3000集中器上的連線問題](#)。

[相關資訊](#)

- [Cisco VPN 3000系列集中器支援頁](#)
- [Cisco VPN 3000使用者端支援頁面](#)
- [IPSec 協商/IKE 通訊協定](#)
- [技術支援與文件 - Cisco Systems](#)