

Configurazione e registrazione di un concentratore Cisco VPN 3000 su un router Cisco IOS come server CA

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Esempio di rete](#)

[Convenzioni](#)

[Generazione ed esportazione della coppia di chiavi RSA per il server di certificazione](#)

[Esporta coppia di chiavi generata](#)

[Verifica coppia di chiavi generata](#)

[Abilitare il server HTTP sul router](#)

[Abilitare e configurare il server CA sul router](#)

[Configurazione e registrazione di Cisco VPN 3000 Concentrator](#)

[Verifica](#)

[Risoluzione dei problemi](#)

[Informazioni correlate](#)

[Introduzione](#)

In questo documento viene descritto come configurare un router Cisco IOS® come server Autorità di certificazione (CA). Inoltre, illustra come registrare un Cisco VPN 3000 Concentrator sul router Cisco IOS per ottenere un certificato radice e ID per l'autenticazione IPsec.

[Prerequisiti](#)

[Requisiti](#)

Nessun requisito specifico previsto per questo documento.

[Componenti usati](#)

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco serie 2600 Router con software Cisco IOS versione 12.3(4)T3

- Cisco VPN 3030 Concentrator versione 4.1.2

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Esempio di rete

Nel documento viene usata questa impostazione di rete:



Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento [Cisco sulle convenzioni nei suggerimenti tecnici](#).

Generazione ed esportazione della coppia di chiavi RSA per il server di certificazione

Il primo passaggio consiste nella generazione della coppia di chiavi RSA utilizzata dal server CA Cisco IOS. Sul router (R1), generare le chiavi RSA come mostrato di seguito:

```
R1(config)#crypto key generate rsa general-keys label cisco1 exportable
The name for the keys will be: cisco1
Choose the size of the key modulus in the range of 360 to 2048 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.
```

```
How many bits in the modulus [512]:
% Generating 512 bit RSA keys ...[OK]
```

```
R1(config)#
*Jan 22 09:51:46.116: %SSH-5-ENABLED: SSH 1.99 has been enabled
```

Nota: è necessario utilizzare lo stesso nome per la coppia di chiavi (*key-label*) che si intende utilizzare per il server dei certificati (tramite il comando **crypto pki server *cs-label*** descritto in seguito).

Esporta coppia di chiavi generata

Le chiavi devono quindi essere esportate nella memoria RAM non volatile (NVRAM) o nel

protocollo TFTP (in base alla configurazione in uso). Nell'esempio viene usata la NVRAM. In base all'implementazione, è possibile utilizzare un server TFTP separato per archiviare le informazioni sul certificato.

```
R1(config)#crypto key export rsa cisco1 pem url nvram: 3des cisco123
```

```
% Key name: cisco1
  Usage: General Purpose Key
Exporting public key...
Destination filename [cisco1.pub]?
Writing file to nvram:cisco1.pub
Exporting private key...
Destination filename [cisco1.prv]?
Writing file to nvram:cisco1.prv
R1(config)#
```

Se si utilizza un server TFTP, è possibile reimportare la coppia di chiavi generata come illustrato di seguito:

```
crypto key import rsa key-label pem [usage-keys] {terminal | url url} [exportable] passphrase
```

Nota: se non si desidera esportare la chiave dal server di certificati, importarla nuovamente nel server di certificati dopo averla esportata come coppia di chiavi non esportabile. Pertanto, non è possibile estrarre nuovamente la chiave.

[Verifica coppia di chiavi generata](#)

È possibile verificare la coppia di chiavi generata richiamando il comando **show crypto key mypubkey rsa**:

Alcuni comandi **show** sono supportati dallo [strumento Output Interpreter \(solo utenti registrati\)](#); lo strumento permette di visualizzare un'analisi dell'output del comando **show**.

```
R1#show crypto key mypubkey rsa
% Key pair was generated at: 09:51:45 UTC Jan 22 2004
Key name: cisco1
  Usage: General Purpose Key
  Key is exportable.
Key Data:
  305C300D 06092A86 4886F70D 01010105 00034B00 30480241 00CC2DC8 ED26163A
  B3642376 FAA91C2F 93A3825B 3ABE6A55 C9DD3E83 F7B2BD56 126E0F11 50552843
  7F7CA4DA 3EC3E2CE 0F42BD6F 4C585385 3C43FF1E 04330AE3 37020301 0001
% Key pair was generated at: 09:51:54 UTC Jan 22 2004
Key name: cisco1.server
  Usage: Encryption Key
  Key is exportable.
Key Data:
  307C300D 06092A86 4886F70D 01010105 00036B00 30680261 00EC5578 025D3066
  72149A35 32224BC4 3E41DD68 38B08D39 93A1AA43 B353F112 1E56DA42 49741698
  EBD02905 FE4EC392 7174EEBF D82B4475 2A2D7DEC 83E277F8 AEC590BE 124E00E1
  C1607433 5C7BC549 D532D18C DD0B7AE3 AECDD9C 07AD84DD 89020301 0001
```

[Abilitare il server HTTP sul router](#)

Il server CA Cisco IOS supporta solo registrazioni effettuate tramite SCEP (Simple Certificate Enrollment Protocol). Di conseguenza, per rendere possibile questa operazione, il router deve eseguire il server HTTP Cisco IOS incorporato. Per attivarlo, utilizzare il comando `ip http server`:

```
R1(config)#ip http server
```

Abilitare e configurare il server CA sul router

Attenersi alla procedura seguente.

1. È molto importante ricordare che il server di certificazione deve utilizzare lo stesso nome della coppia di chiavi appena generata manualmente. L'etichetta corrisponde all'etichetta della coppia di chiavi generata:

```
R1(config)#crypto pki server cisco1
```

Dopo aver abilitato un server certificati, è possibile utilizzare i valori predefiniti preconfigurati o specificare i valori tramite CLI per la funzionalità del server certificati.

2. Il comando **database url** specifica la posizione in cui vengono scritte tutte le voci di database per il server CA. Se questo comando non viene specificato, tutte le voci del database vengono scritte in Flash.

```
R1(cs-server)#database url nvram:
```

Nota: se si utilizza un server TFTP, l'URL deve essere `tftp://<indirizzo_ip>/directory`.

3. Configurare il livello del database:

```
R1(cs-server)#database level minimum
```

Questo comando controlla il tipo di dati archiviati nel database di registrazione dei certificati. **Minimo:** vengono archiviate informazioni sufficienti solo per continuare a rilasciare nuovi certificati senza conflitti. valore predefinito. **Nomi:** oltre alle informazioni fornite nel livello minimo, il numero di serie e il nome del soggetto di ciascun certificato. **Completo:** oltre alle informazioni fornite nei livelli minimo e nomi, ogni certificato rilasciato viene scritto nel database. **Nota:** la parola chiave **complete** produce una grande quantità di informazioni. Se viene emesso, è necessario specificare anche un server TFTP esterno in cui memorizzare i dati tramite il comando **database url**.

4. Configurare il nome dell'autorità emittente della CA sulla stringa DN specificata. Nell'esempio viene utilizzato il CN (nome comune) `cisco1.cisco.com`, L (località) della RTP e C (paese) degli USA:

```
R1(cs-server)#issuer-name CN=cisco1.cisco.com L=RTP C=US
```

5. Specificare la durata, in giorni, di un certificato CA o di un certificato. I valori validi sono compresi tra *1 e 1825 giorni*. La durata predefinita del certificato CA è di **3 anni** e la durata predefinita del certificato è di **1 anno**. La durata massima del certificato è *inferiore di un mese alla durata del certificato CA*. Ad esempio:

```
R1(cs-server)#lifetime ca-certificate 365
```

```
R1(cs-server)#lifetime certificate 200
```

6. Definire la durata, in ore, del CRL utilizzato dal server dei certificati. Il valore massimo della durata è **336 ore** (2 settimane). Il valore predefinito è **168 ore** (1 settimana).

```
R1(cs-server)#lifetime crl 24
```

7. Definire un CDP (Certificate-Revocation-List Distribution Point) da utilizzare nei certificati rilasciati dal server dei certificati. L'URL deve essere un URL HTTP. Ad esempio, l'indirizzo IP del nostro server è 172.18.108.26.

```
R1(cs-server)#cdp-url http://172.18.108.26/cisco1cdp.cisco1.crl
```

8. Abilitare il server CA usando il comando **no shutdown**.

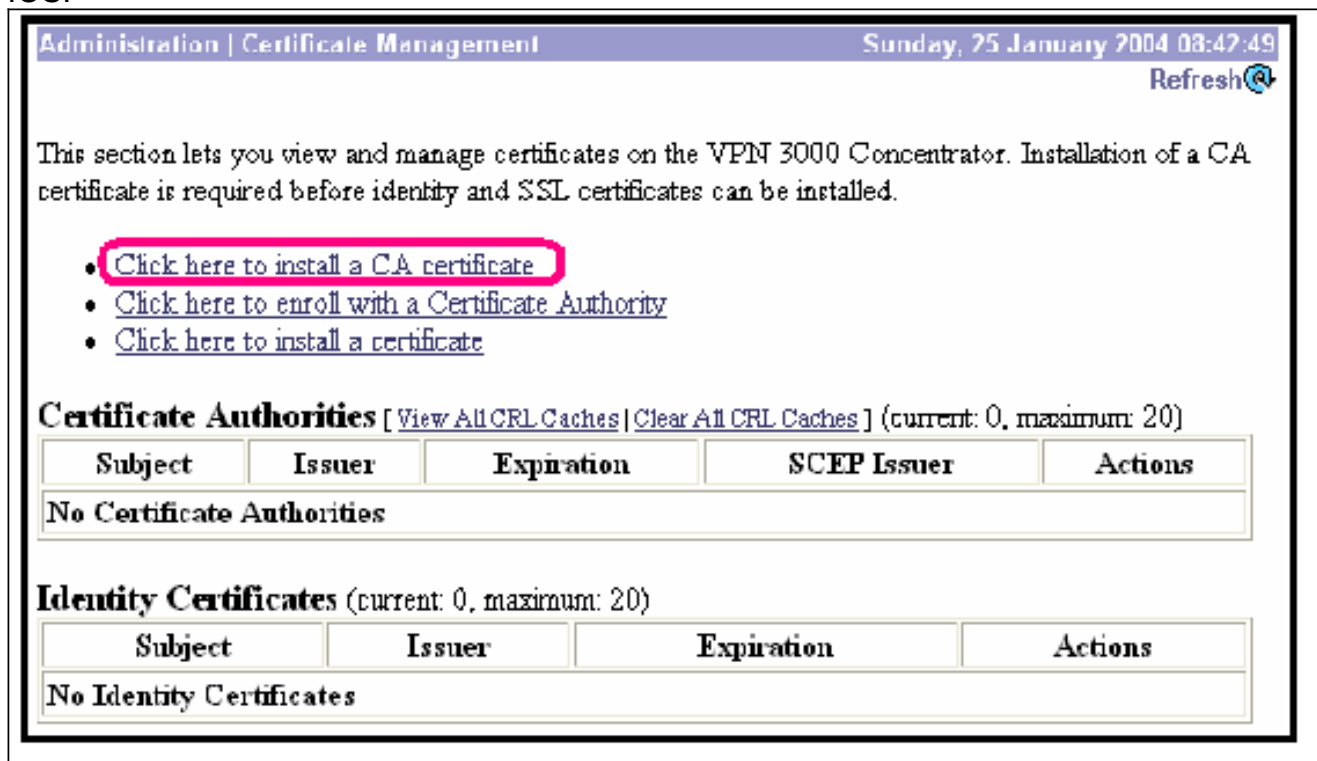
```
R1(cs-server)#no shutdown
```

Nota: eseguire questo comando solo dopo aver completato la configurazione del server di certificati.

Configurazione e registrazione di Cisco VPN 3000 Concentrator

Attenersi alla procedura seguente.

1. Selezionare **Amministrazione > Gestione certificati** e scegliere **Fare clic qui per installare un certificato CA** per recuperare il certificato radice dal server CA Cisco IOS.



Administration | Certificate Management Sunday, 25 January 2004 08:47:49 Refresh

This section lets you view and manage certificates on the VPN 3000 Concentrator. Installation of a CA certificate is required before identity and SSL certificates can be installed.

- [Click here to install a CA certificate](#)
- [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: 0, maximum: 20)

Subject	Issuer	Expiration	SCEP Issuer	Actions
No Certificate Authorities				

Identity Certificates (current: 0, maximum: 20)

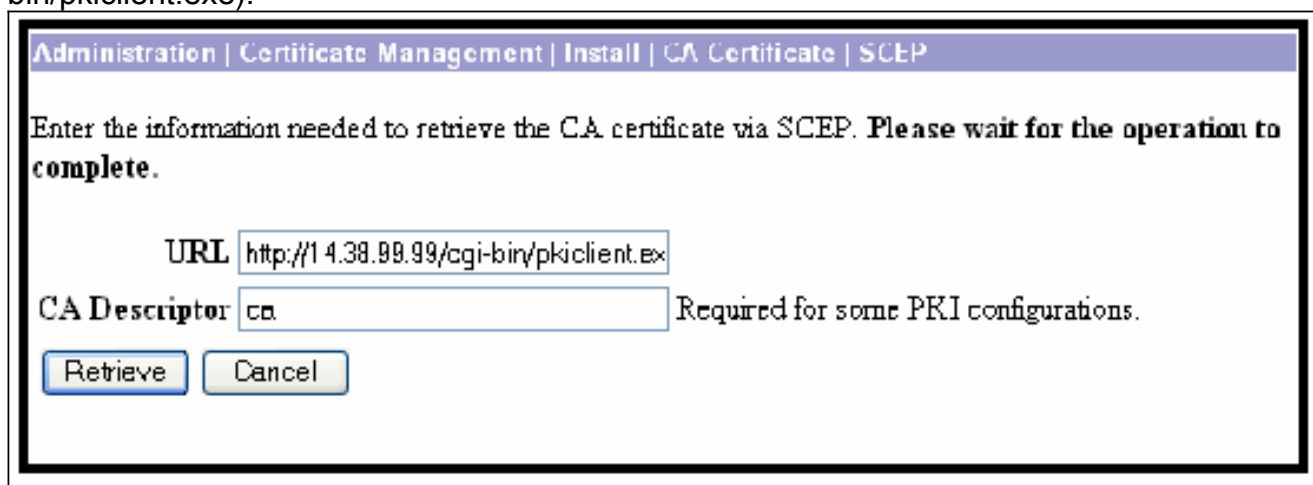
Subject	Issuer	Expiration	Actions
No Identity Certificates			

2. Selezionare **SCEP** come metodo di

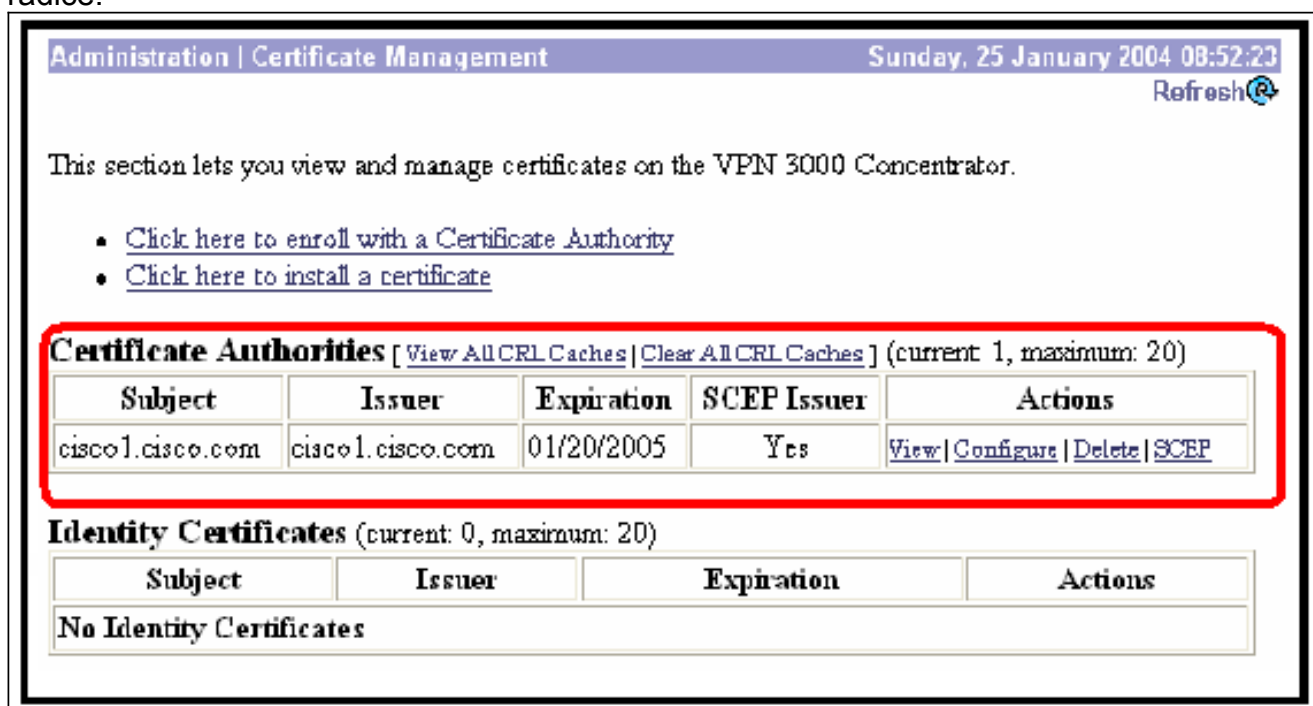


installazione.

- Immettere l'URL del server CA Cisco IOS, un descrittore CA, e fare clic su **Recupera**. **Nota:** l'URL corretto in questo esempio è `http://14.38.99.99/cgi-bin/pkiclient.exe` (è necessario includere il percorso completo di `/cgi-bin/pkiclient.exe`).



Selezionare **Amministrazione > Gestione certificati** per verificare che il certificato radice sia stato installato. Nella figura vengono illustrati i dettagli del certificato radice.



- Selezionare **Fare clic qui per effettuare la registrazione a un'Autorità di certificazione** per

ottenere il certificato ID dal server CA Cisco IOS.

Administration | Certificate Management Sunday, 25 January 2004 08:52:23 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: 1, maximum: 20)

Subject	Issuer	Expiration	SCEP Issuer	Actions
cisco1.cisco.com	cisco1.cisco.com	01/20/2005	Yes	View Configure Delete SCEP

Identity Certificates (current: 0, maximum: 20)

Subject	Issuer	Expiration	Actions
No Identity Certificates			

5. Selezionare **Enroll via SCEP su cisco1.cisco.com** (cisco1.cisco.com è il CN del server CA Cisco IOS).

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 cisco1.cisco.com](#)

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

6. Completare il modulo di registrazione immettendo tutte le informazioni da includere nella richiesta di certificato. Dopo aver completato il modulo, fare clic su **Enrollment** (Registra) per avviare la richiesta di registrazione sul server CA.

Administration Certificate Management Enroll | Identity Certificate | SSCP

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

Common Name (CN)	<input type="text" value="rtp-vpn3000"/>	Enter the common name for the VPN 3000 Concentrator to be used in this PKI.
Organizational Unit (OU)	<input type="text" value="TAC"/>	Enter the department.
Organization (O)	<input type="text" value="Cisco"/>	Enter the Organization or company.
Locality (L)	<input type="text" value="RTP"/>	Enter the city or town.
State/Province (SP)	<input type="text" value="NC"/>	Enter the State or Province.
Country (C)	<input type="text" value="US"/>	Enter the two-letter country abbreviation (e.g. United States = US).
Subject AlternativeName (FQDN)	<input type="text"/>	Enter the Fully Qualified Domain Name for the VPN 3000 Concentrator to be used in this PKI.
Subject AlternativeName (E-Mail Address)	<input type="text"/>	Enter the E-Mail Address for the VPN 3000 Concentrator to be used in this PKI.
Challenge Password	<input type="text"/>	Enter and verify the challenge password for this certificate request.
Verify Challenge Password	<input type="text"/>	
Key Size	<input type="text" value="RSA 512 bits"/>	Select the key size for the generated RSA key pair.

Dopo aver fatto clic su Registra, in VPN 3000 Concentrator viene visualizzato "È stata generata una richiesta di certificato".

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](#)

Nota:

il server CA Cisco IOS può essere configurato in modo da concedere automaticamente i certificati con il sottocomando Cisco IOS CA Server **grant automatic**. Questo comando è utilizzato per questo esempio. Per visualizzare i dettagli del certificato ID, selezionare **Amministrazione > Gestione certificati**. Il certificato visualizzato è simile a questo.

Administration | Certificate Management Sunday, 25 January 2004

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: 1, maximum: 20)

Subject	Issuer	Expiration	SCEP Issuer	Actions
cisco1.cisco.com	cisco1.cisco.com	01/20/2005	Yes	View Configure Delete SCEP

Identity Certificates (current: 1, maximum: 20)

Subject	Issuer	Expiration	Actions
rtp-vpn3000 at Cisco	cisco1.cisco.com	08/12/2004	View Renew Delete

[Verifica](#)

Per informazioni sulla verifica, vedere la sezione [Verifica della coppia di chiavi generata](#).

[Risoluzione dei problemi](#)

Per informazioni sulla risoluzione dei problemi, consultare il documento sulla [risoluzione dei problemi di connessione su VPN 3000 Concentrator](#) o sulla [risoluzione dei problemi di sicurezza IP - descrizione e uso dei comandi di debug](#).

[Informazioni correlate](#)

- [Cisco VPN serie 3000 Concentrator Support Page](#)
- [Cisco VPN serie 3000 Client Support Page](#)
- [Pagina di supporto per IPsec](#)
- [Supporto tecnico – Cisco Systems](#)