

# VPN 3000 Concentrator and VPN Client Verisign Certificates Installation Procedure

Document ID: 28142

---

**Introduction**

**Prerequisites**

Requirements

Components Used

Conventions

**Configure the Verisign CA Server and VPN 3000 Concentrator**

Troubleshoot

**NetPro Discussion Forums – Featured Conversations**

**Related Information**

---

## Introduction

This document outlines the procedure used to install Verisign Certificates on the Cisco VPN Client and VPN 3000 Concentrator.

## Prerequisites

### Requirements

There are no specific requirements for this document.

### Components Used

The information in this document is based on these software and hardware versions:

- Verisign Certification Authority (CA) Server
- Cisco VPN 3000 Concentrator 4.x

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

### Conventions

For more information on document conventions, refer to the Cisco Technical Tips Conventions.

## Configure the Verisign CA Server and VPN 3000 Concentrator

Complete these steps to configure the Verisign CA Server.

1. Browse to the Verisign CA server control panel page (admin page).
2. Select **Configuration > Install CA**.

Text similar to this appears:

```
Because your organization is using the Private certificate service, your
IPSec certificates are issued under a private Certification Authority (CA)
set up specifically for your organization (as opposed to VeriSign's
public CA). For your network devices to use the IPSec certificates issued by
your CA, your private CA's certificate must reside in the network applications.
```

```
!--- Output suppressed.
```

```
-----BEGIN CERTIFICATE-----
```

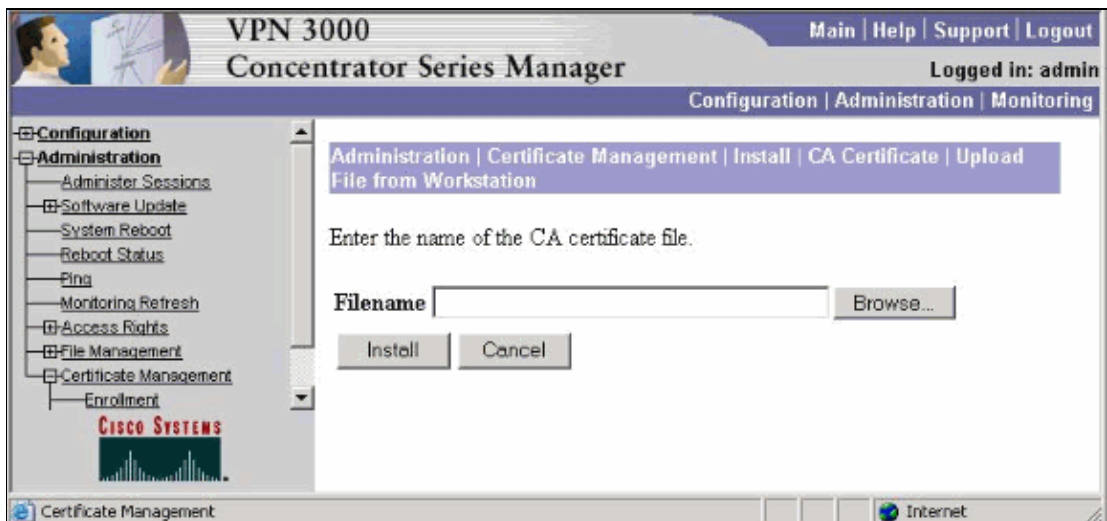
```
!--- Output suppressed.
```

```
-----END CERTIFICATE-----
```

Alternatively, you can download a .tar format zipped file that can be decompressed with WinZip. The .tar file contains these four files:

- ◆ ca.509
- ◆ ca.info
- ◆ ca.nx509 – This file is the actual certificate that you cut and paste. Save this file on your PC.
- ◆ Long string of characters.509

3. Select **Administration > Certificate Management > Install > CA Certificate > Upload File from Workstation**.



4. Click **Browse** and direct the file to the location of your CA ROOT certificate previously saved on your PC.

5. Click **Install**.

6. Select **Administration > Certificate Management** to view CA Root Certificate.

Administration | Certificate Management Wednesday, 09 June 2004 08:28:23  
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: 3, maximum: 6)

Subject	Issuer	Expiration	SCEP Issuer	Actions
RTP_VPN_2003_CA	RTP_VPN_2003_CA	03/18/2009	Yes	<a href="#">View</a>   <a href="#">Configure</a>   <a href="#">Delete</a>   <a href="#">SCEP</a>   <a href="#">Show RAs</a>

7. Choose **Click here to enroll with a Certificate Authority**.

Administration | Certificate Management Wednesday, 09 June 2004 08:32:23  
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: 3, maximum: 6)

Subject	Issuer	Expiration	SCEP Issuer	Actions
RTP_VPN_2003_CA	RTP_VPN_2003_CA	03/18/2009	Yes	<a href="#">View</a>   <a href="#">Configure</a>   <a href="#">Delete</a>   <a href="#">SCEP</a>   <a href="#">Show RAs</a>

**Identity Certificates** (current: 1, maximum: 2)

Subject	Issuer	Expiration	Actions
con_cert at cisco	RTP_VPN_2003_CA	03/18/2005	<a href="#">View</a>   <a href="#">Renew</a>   <a href="#">Delete</a>

8. Select **Administration > Certificate Management > Enrollment > Identity Certificate**.

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 RTP\\_VPN\\_2003\\_CA](#)

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

9. Click **Enroll via PKCS10 Request (Manual)**.

Administration | Certificate Management | Enroll | Identity Certificate | PKCS10

Enter the information to be included in the certificate request. *The CA's certificate **must** be installed as a Certificate Authority before installing the certificate you requested. 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.

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

10. Fill out the form as needed.
11. Click **Enroll**.

A separate window opens with "Begin new certificate request". Copy this certificate request to Notepad.

12. Select **Administration** > **Certificate Management** and ensure that the status of the ID certificate states "in progress".

Administration | Certificate Management Wednesday, 09 June 2004 08:46:31  
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](#)

**Enrollment Status** [ Remove All: [Errored](#) | [Timed-Out](#) | [Rejected](#) | [Cancelled](#) | [In-Progress](#) ] (current: 0 available: 2)

Subject	Issuer	Date	Use	Reason	Method	Status	Actions
No Enrollment Requests							

**Note:** The above graphic has no enrollment request. However, if there was one, the full line is populated with the required information.

13. Browse to the Versign CA enrollment page.
14. Choose the **generate your certificate signing request** option. The options provided are to upload from file or text.
15. Use the text format.
16. Enter this authentication information:

- ◆ Full Name
- ◆ Email Address
- ◆ Title
- ◆ Domain name and IP address (leave this blank)

17. Choose a challenge phrase.

**Note:** You can choose to leave this blank because it is not required.

18. Enter comments.

**Note:** You can choose to leave this blank because it is not required.

19. Click **Submit**.

20. After Verisign states that "your certificate request has been submitted successfully", browse to the Verisign CA control page and click on **Certificate Management**.

21. Click on **Process request**.

22. Click **Approve** to send the first email back to the end user that states the certificate has been approved and the second email with the actual ID certificate.

23. On the VPN 3000 Concentrator, select **Administration > Certificate Management**.

24. Under the ID Certificates Action section, look for < **INSTALL** >.

25. Click **Install**.

Two options appear:

◆ upload

◆ cut and paste

26. Click **Install**.

At this point, you are brought back to the Certificate Management page and you can see the CA certificate and the ID certificate. The certificates are successfully installed.

## Troubleshoot

**Problem:** The "Error installing SSL certificate: Incomplete chain" displays within SSL certificate installation on the VPN 3000 Series Concentrator.

**Cause:** This parse error displays if the VPN concentrator does not have a root Certificate Authority (CA) certificate installed.

**Resolution:** Regardless of whether Simple Certificate Enrollment Protocol (SCEP) or manual enrollment is used, the VPN concentrator must have a root CA installed if third-party certificates are used. In order to obtain and install the Secure Socket Layer (SSL) certificates, perform this procedure:

1. Obtain and install the **root CA certificate**.
2. Create an **enrollment request** for one or more identity certificates.
3. Request an **identity certificate** from the same CA that issued the root CA certificate.
4. Install the **identity certificate** on the VPN concentrator.
5. Enable **Certificate Revocation List (CRL) checking and caching**.
6. Enable **Certificates**.

## NetPro Discussion Forums – Featured Conversations

Networking Professionals Connection is a forum for networking professionals to share questions, suggestions, and information about networking solutions, products, and technologies. The featured links are some of the most recent conversations available in this technology.

NetPro Discussion Forums – Featured Conversations for VPN
Service Providers: VPN Service Architectures
Service Providers: Network Management
Virtual Private Networks: General

---

---

## Related Information

- [Cisco VPN 3000 Series Concentrator Support Page](#)
  - [Cisco VPN 3000 Series Client Support Page](#)
  - [IPSec Support Page](#)
  - [Technical Support – Cisco Systems](#)
- 

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2008 – 2009 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

---

Updated: Jan 14, 2008

Document ID: 28142

---