

# Generating and Installing Certificates on the Cisco VPN 5000 Series Concentrator

## Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Conventions](#)

[VPN 5000 Concentrator Certificates for VPN Clients](#)

[Related Information](#)

## Introduction

This document includes step-by-step instructions on how to generate certificates on the Cisco VPN 5000 Series Concentrators and on how to install certificates on the VPN 5000 Clients.

## 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:

- Cisco VPN 5000 Concentrator software version 5.2.16US
- Cisco VPN Client 5.0.12

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](#).

## VPN 5000 Concentrator Certificates for VPN Clients

Complete these steps.

1. If you do not have a time server, you must set the date and time using the **sys clock** command.

```
RTP-5008# sys clock 12/14/00 12:15
```

To verify that the date and time have been set properly, run the **sys date** command.

2. Enable the certificate generator feature of the VPN Concentrator.

```
RTP-5008# configure certificates
```

```
[ Certificates ]# certificategenerator=on
```

```
*[ Certificates ]# validityperiod=365
```

3. Create the root certificate.

```
*RTP-5008# certificate generate root 512 locality rtp state nc  
country us organization "cisco" commonname "cisco" days 365
```

4. Create the server certificate.

```
*RTP-5008# certificate generate server 512 locality rtp state nc  
country us organization "cisco" commonname "cisco" days 365
```

5. Verify the certificate.

```
*RTP-5008# certificate verify
```

6. Display the certificate in Privacy Enhanced Mail (PEM) format, and then copy the certificate to a text editor for exportation to the client. Make sure to include the begin line, the end line, and the carriage return after the end line.

```
*RTP-5008# show certificate pem root
```

```
-----BEGIN PKCS7-----
```

```
MIAGCSqGSIb3DQEHAqCAMIIBmAIbATEAMIAGAQAANKCCAYYwggGCMIIbLKADAgEC  
AgRAP0AJMA0GCSqGSIb3DQEBBAUAMEgxDdAKBgNVBAcTA3J0cDELMAkGA1UECBMC  
bmMxCzAJBgNVBAYTANVzMQ4wDAYDVQQKEWVjaXNjbzEOMAwGA1UEAxMFY21zY28o  
HhcNMDEwMDYzOTIzWhcNMDEwMDYzOTIzWjBIMQwwCgYDVQQHEWVjaXNjbzEOMAwGA1UEChMFY21zY28xDjAMBGNV  
BAMTBWNpc2NvMFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBAML/buEqz3PnWQ5M6Seq  
gE9uf7sZNUbHKZCp+GP9EpRkFuaYCD9vYZ3+MRTphiY55tDRmxTEglvK618sYIKd  
XDcCAwEAATANBgkqhkiG9w0BAQQFAANBAbuRHckNTXEAXSwyj7c5bEnAMCvI4Whd  
ZRzVST5/QVRPjcaLXb0QJP47CzNecONfmM0bZ3n2nxBnbNDimJQbCgwxAAAAAAA=
```

```
-----END PKCS7-----
```

7. Open the VPN Client to configure it for certificate authentication.
8. On the VPN Client's Configuration tab, select **Add**.
9. Select **Certificate** for the Login Method, and then enter the login name and the primary VPN server address (or fully qualified domain name). Add a secondary VPN server entry if necessary.
10. Select **OK** to close the Login Properties window.
11. Go to **Certificates > Import**, browse to the location where the certificate is located, and select the certificate file.
12. With the certificate listed in the Root Certificates field, click the Configuration tab of the VPN Client.

13. Select the **Connect** button to initiate a VPN connection.

## Related Information

- [Cisco VPN 5000 Series Concentrators End-of-Sales Announcement](#)
- [Cisco VPN 5000 Client](#)
- [IPSec \(IP Security Protocol\)](#)
- [Technical Support - Cisco Systems](#)