

# Geração e Instalação de Certificados do Cisco VPN 5000 Series Concentrator

## Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenções](#)

[Certificados do VPN 5000 Concentrator para VPN Clients](#)

[Informações Relacionadas](#)

## [Introdução](#)

Este documento inclui instruções passo a passo em como gerar Certificados no Concentradores Cisco VPN série 5000 e em como instalar Certificados nos clientes VPN5000.

## [Pré-requisitos](#)

### [Requisitos](#)

Não existem requisitos específicos para este documento.

### [Componentes Utilizados](#)

As informações neste documento são baseadas nestas versões de software e hardware:

- Versão de software do concentrador 5.2.16US do Cisco VPN 5000
- Cisco VPN Client 5.0.12

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

### [Convenções](#)

Para obter mais informações sobre convenções de documento, consulte as [Convenções de dicas técnicas Cisco](#).

## [Certificados do VPN 5000 Concentrator para VPN Clients](#)

Termine estas etapas.

1. Se você não tem um Time Server, você deve ajustar a data e hora usando o comando **sys clock**.

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

Para verificar que a data e hora esteve ajustada corretamente, execute o comando **sys date**.

2. Permita a característica do gerador certificado do concentrador VPN.

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

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

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

3. Crie o certificado de raiz.

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

4. Crie o certificado de servidor.

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

5. Verifique o certificado.

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

6. Indique o certificado no formato do Privacy Enhanced Mail (PEM), e copie então o certificado a um editor de texto para a exportação ao cliente. Certifique-se incluir a linha do começo, a linha final, e a tecla semelhante a tecla ENTER após a linha final.

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

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

```
MIAGCSqGSIb3DQEHAqCAMIIBmAIbATEAMIAGAQAQAAKCCAYYwggGCMII BLKADAgEC  
AgRAP0AJMA0GCSqGSIb3DQEBBAUAMEgxDDAKBgNVBAcTA3J0cDELMAkGA1UECBMC  
bmMxCzAJBgNVBAYTAnVzMQ4wDAYDVQQKEwVjaXNjbzEOMAwGA1UEAxMFY21zY28o  
HhcNMDAwNzE0MDYzOTIzWhcNMDAwNzE0MDYzOTIzWjBIMQwwCgYDVQQHEwNydHAX  
CzAJBgNVBAGTAm5jMQswCQYDVQQGEwJ1czEOMAwGA1UEChMFY21zY28xDjAMBGNV  
BAMTBWNpc2NvMFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBAML/buEqz3PnWQ5M6Seq  
gE9uf7sZNUbHKZCp+GP9EpRkFuaYCD9vYZ3+MRTphiY55tDRmxTEglvK618sYIKd  
XDcCAwEAATANBgkqhkiG9w0BAQQFAANBABuRHckNTXEAXSwyj7c5bEnAMCvI4Whd  
ZRzVST5/QVRPjcaLXb0QJP47CzNecONfmM0bZ3n2nxBnbNDimJQbCgwxAAAAAAA=
```

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

7. Abra o cliente VPN para configurar-lo para o certificado de autenticação.
8. No guia de configuração do cliente VPN, seletor **adicionar**.
9. Selecione o **certificado** para o método de login, e dê entrada com então o nome do início de uma sessão e o endereço preliminar do servidor de VPN (ou nome de domínio totalmente qualificado). Adicionar uma entrada secundária do servidor de VPN caso necessário.
10. Selecione **ESTÁ BEM** para fechar a janela de propriedades do início de uma sessão.

11. Vá ao **certificados > importar**, consulte ao lugar onde o certificado é encontrado, e selecione o arquivo certificado.
12. Com o certificado alistado nos certificados de raiz coloque, clique o guia de configuração do cliente VPN.
13. Selecione o **botão connect** para iniciar uma conexão de VPN.

## Informações Relacionadas

- [Anúncio End-of-Life de concentradores do Cisco VPN 5000 Series](#)
- [Cisco VPN 5000 Client](#)
- [IPSEC \(Protocolo de Segurança IP\)](#)
- [Suporte Técnico - Cisco Systems](#)