

# Create a Certificate Signing Request on the SSL Services Module Using Copy and Paste

---

## Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Conventions](#)

[Main Task](#)

[Task](#)

[Step-by-Step Instructions](#)

[Intermediate Certificates](#)

[Verify](#)

[Troubleshoot](#)

[NetPro Discussion Forums - Featured Conversations](#)

[Related Information](#)

---

## Introduction

This document describes how to:

- create a certificate signing request (CSR) on the Secure Socket Layer Module (SSLM)
- import the certificate using cut and paste in privacy-enhanced mail (PEM) format

## Prerequisites

Before you begin, you need to know the domain name that is assigned to the certificate. You also need the Certificates Authorities (CA) root certificate, and possibly the CA intermediate certificate.

## Requirements

Before attempting this configuration, ensure that you meet these requirements:

- CA root certificate; possibly the intermediate root certificate
- domain name for certificate

- information

## Components Used

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

- release 2.1(2)
- Verisign Test Certificate

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](#).

## Main Task

### Task

This section details each step needed to create the CSR, from the creation of the key pair to importing the server certificate.

### Step-by-Step Instructions

Complete the instructions in this section.

1. Create the key pair.

nov10-key is the name of the key pair.

**Note:** Be sure to specify **exportable**; otherwise, you are not able to export the key pair from the SSLM.

```
ssl-proxy(config)#crypto key generate rsa general-keys label nov10-key exp  
The name for the keys will be: nov10-key  
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]: 1024  
% Generating 1024 bit RSA keys ...[OK]
```

2. Create the trustpoint .

The name of the trustpoint is yoursite. You need to enter the subject name in X.509 format and your domain name. This information is used to create the CSR.

```

ssl-proxy(config)#crypto ca trustpoint yoursite
ssl-proxy(ca-trustpoint)#enrollment terminal pem
ssl-proxy(ca-trustpoint)#crl optional
ssl-proxy(ca-trustpoint)#subject-name C=US, ST=Massachusetts, L=Boxborough
OU=Tac, CN=www.yourdomain.com
ssl-proxy(ca-trustpoint)#fqdn www.yourdomain.com
ssl-proxy(ca-trustpoint)#rsakeypair nov10-key
ssl-proxy(ca-trustpoint)#exit

```

### 3. Generate the CSR.

```

ssl-proxy(config)#crypto ca enroll yoursite
% Start certificate enrollment ..
% The subject name in the certificate will be: C=US, ST=Massachusetts, L=B
OU=Tac, CN=www.yourdomain.com
% The fully-qualified domain name in the certificate will be: www.yourdoma
% The subject name in the certificate will be: www.yourdomain.com
% Include the router serial number in the subject name? [yes/no]: no
% Include an IP address in the subject name? [no]: no
Display Certificate Request to terminal? [yes/no]: yes

```

Certificate Request follows:

```

-----BEGIN CERTIFICATE REQUEST-----
MIIB+jCCAAMCAQAwwGZgZAZBgNVBAMTEnd3dy55b3VyZG9tYWluLmNvbTEEMMAoG
A1UECXMdVGFjMQ4wDAYDVQQKEwVDaXNjbzETMBEGA1UEBxMKQm94Ym9yb3VnaDEW
MBQGA1UECBMNTWFzc2FjaHVzZXR0czELMAkGA1UEBhMCVVMxITAfBgkqhkiG9w0B
CQIWEnd3dy55b3VyZG9tYWluLmNvbTCBnzANBgkqhkiG9w0BAQEFAAOBjQAwYkC
gYEAwwCQrKH+RYvhQpZuuVADHah4BoFRefiV+b6UXXI8dOmnkKB/wlw+Hure4N6p
QsBPMEglmkU5AT38JcrWku8JfGVEEap54UX+ZGs4o37ssskL4vr0qenQ0PpkIVE4
4iZLb+KxS5XbGrNRN6Mx4A8npV8xelWew8TqNw2h+oNYEBcCAwEAAAhMB8GCSqG
SIb3DQEJJDjESMBAwDgYDVR0PAQH/BAQDAgWgMA0GCSqGSIb3DQEBAUAA4GBAKjW
SeLVzYdRSIkEL+rrYeuJfpoQTPIgTyjLNeIla/ipoA/cQYPR0RBQ3N1k8G2JhXhW
De4hNDsYPtnPZ65kUSjLLV6BenxKjXzIDhdc2x8MyhMu5t/tAbxelG3daJGHUBD
Of5meQ4JrbfWZHATmoiTEpAbWVNHC2h7oJO5Ldhw
-----END CERTIFICATE REQUEST-----

```

---End - This line not part of the certificate request---

Redisplay enrollment request? [yes/no]: no

### 4. Send the CSR to your CA.

Use copy and paste to send the CSR to your CA. If your CA asks for a server type, select Apache.

### 5. Load the CA root certificate

Before you can load the server certificate, you must load any CA certificates. At a minimum, this is the CA root certificate, and possibly a CA intermediate certificate. Your CA is able to provide you with the necessary certificates.

```

ssl-proxy(config)#crypto ca authenticate yoursite
Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself

```



If you have an intermediate certificate, you need to configure two trustpoints. One trustpoint contains the CA root certificate only. You only need to configure enrollment terminal PEM and Certificate Revocation List (CRL) optional. The second trustpoint contains the intermediate certificate and the server certificate. The second trustpoint is configured similar to the first trustpoint, however, instead of the root certificate, use the intermediate certificate.

## Verify

There is currently no verification procedure available for this configuration.

## Troubleshoot

This section provides troubleshooting information relevant to this configuration.

If you run into problems loading the certificates, enable debugging with the **debug crypto pki transactions** command.

Make sure you have the complete certificate chain. You can determine this by viewing the certificates on a PC. Save the certificates with a .cer extension, then double click to open them.

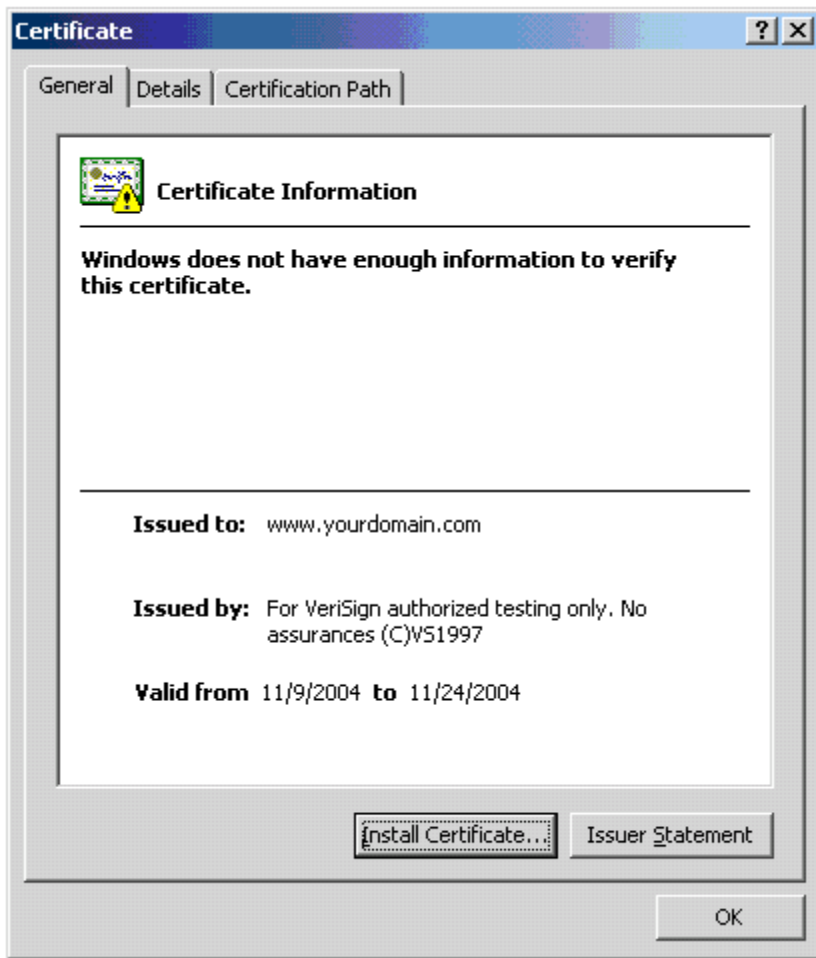
The root certificate is shown in Figure 1. You can determine this by looking at the **Issued to** and **Issued by** sections. Both sections are the same. Also, note that the certificate is showing up as not trusted because it a test certificate.

### Figure 1



The server certificate is shown in Figure 2. You can determine that it matches the root certificate because the **Issued by** section matches the **Issued by** section on the root certificate.

**Figure 2**



## 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 CDN](#)
- [Emerging Technologies: Content Networking](#)