

Solutions Products Ordering Support Partners Training Corporate

Sample Configurations

# Import Certificates and Private Key with Copy and Paste

[TAC Notice: What's Changing on TAC Web](#)

## Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Conventions](#)

[Main Task](#)

[Task](#)

[Step-by-Step Instructions](#)

[Verify](#)

[Troubleshoot](#)

[NetPro Discussion Forums - Featured Conversations](#)

[Related Information](#)

Help us help you.

Please rate this document.

Excellent

Good

Average

Fair

Poor

This document solved my problem.

Yes

No

Just browsing

Suggestions for improvement:

(256 character limit)

## Introduction

This document describes how to import your certificates and private key in privacy-enhanced mail (PEM) format with copy and paste.

In this document, there are two trustpoints; the first trustpoint contains the certificate authority (CA) root certificate, and the second trustpoint contains the CA intermediate and server certificates and the private key.

## Prerequisites

### Requirements

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

- Your certificates and keys must be in PEM format.
- Your private key must be in PEM format and encrypted.
- You must have the complete certificate chain. This includes, at a minimum, the CA root certificate, and possibly the CA intermediate and server certificates. If you do not have the

complete certificate chain, the import of the server certificate fails.

## Components Used

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

- Secure Socket Layer Module (SSLM) version 2.1(2)
- certificates in PEM format
- encrypted private key in PEM format

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

In this configuration, there are three certificates: the CA root, CA intermediate, and the server certificates. Because there are two CA certificates, you need to create two trustpoints. The first trustpoint is used to hold the CA root certificate, and the second trustpoint contains the CA intermediate and server certificate and the private key.

### Step-by-Step Instructions

Complete the steps in this section.

1. Create a trustpoint for the CA root certificate.

```
ssl-proxy(config)#crypto ca trustpoint root-tank.com
ssl-proxy(ca-trustpoint)#enrollment terminal PEM
ssl-proxy(ca-trustpoint)#crl optional
ssl-proxy(ca-trustpoint)#exit
```

2. Import the CA root certificate with copy and paste.

```
ssl-proxy(config)#crypto ca authenticate root-tank.com
```

Enter the base 64 encoded CA certificate.  
End with a blank line or the word "quit" on a line by itself

```
-----BEGIN CERTIFICATE-----
MIIDujCCAyOgAwIBAgIBADANBgkqhkiG9w0BAQQFADCB0DELMakGA1UEBhMCVVMx
CzAJBgNVBAGTAklBMRMwEQYDVQQHEwpcb3hib3JvdWdoMRgwFgYDVQQKEw9SdXN0
ZWQgUm9vdCBJTkMxEDA0BgNVBAsTB1Jvb3QgQ0ExHjAcBgNVBAMTFXJvb3RDQS5y
```

```

dXN0ZWRYb290LmNvbTEjMCEGCSqGSIB3DQEJARYUYWRtaW4ucnVzdGVkcm9vdC5j
b20wHhcNMDQwODI4MDQwMjA3WHcNMDUwODI4MDQwMjA3WjCBODELMAkGA1UEBhMC
VVMxCzAJBgNVBAGTAK1BMRMwEQYDVQQHEwPb3hib3JvdWdoMRgwFgYDVQQKEw9S
dXN0ZWQgUm9vdCBjTtMxEDAObGVBAsTB1Jvb3QgQ0ExHjAcBgNVBAMTFXJvb3RD
QS5ydXN0ZWRYb290LmNvbTEjMCEGCSqGSIB3DQEJARYUYWRtaW4ucnVzdGVkcm9v
dC5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAK0TJDw6e85ySiYfbWUV
SZCEpMy5oBGNHeqfflwCnBjbHudyn9EmsZR72af7AweCpq71yIFRjaCsE6/2mJTW
1vxJRFb5H5CkH1tLwJL5HVHtZjeGwU+FIz6R8yKpbq2SIBSZ95+GbSz7hIjZ78qY
61+z6qDup50W4OLJUgUL464nAgMBAAGjggEAMIH9MB0GA1UdDgQWBQ5NXpGMxPL
gBF67e/ydXUm4AIPYjCBzQYDVR0jBIHFMIHCgBQ5NXpGMxPLgBF67e/ydXUm4AIP
YqGBpqSBozCBODELMAkGA1UEBhMCVVMxCzAJBgNVBAGTAK1BMRMwEQYDVQQHEwPb3
hib3JvdWdoMRgwFgYDVQQKEw9SdXN0ZWQgUm9vdCBjTtMxEDAObGVBAsTB1Jvb3
QgQ0ExHjAcBgNVBAMTFXJvb3RDQS5ydXN0ZWRYb290LmNvbTEjMCEGCSqGSIB3
DQEJARYUYWRtaW4ucnVzdGVkcm9vdC5jb22CAQAwDAYDVR0TBAAUwAwEB/zANBgkq
hkiG9w0BAQFFAAOBgQAvLLBopgRnr1sYmCP+kmqRkqvBsdXjAG77nWB4TeNEmYJi
+eCxuXXhBsQnWNye0yxakaj4EL2wJiXi6eNKCT0gZqZrB66/p2ki7Mpu/3x8g4qe
Bma/nzCvAaA25o5kh8VlgUHSnFoOmhpLsxrDm90umBWTsALci8v70pjBT+09QA==
-----END CERTIFICATE-----

```

**quit**

```

Certificate has the following attributes:
Fingerprint: 615171D8 C3989EFA 4D45B23F 8ACBCDC3
% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
% Certificate successfully imported

```

### 3. Create a second trustpoint for the CA intermediate and server certificates and the private key

```

ssl-proxy(config)#crypto ca trustpoint server-tank.com
ssl-proxy(ca-trustpoint)#enrollment terminal PEM
ssl-proxy(ca-trustpoint)#crl optional
ssl-proxy(ca-trustpoint)#exit

```

### 4. In this order, import the: CA intermediate certificate, private key, and server certificate with copy and paste. **luckydog** is the password for the private key.

```

ssl-proxy(config)#crypto ca import server-tank.com PEM terminal luckydog

% Enter PEM-formatted CA certificate.
% End with a blank line or "quit" on a line by itself.

```

```

-----BEGIN CERTIFICATE-----
MIIDrTCCAaxagAwIBAgIBATANBgkqhkiG9w0BAQFFADCBODELMAkGA1UEBhMCVVMx
CzAJBgNVBAGTAK1BMRMwEQYDVQQHEwPb3hib3JvdWdoMRgwFgYDVQQKEw9SdXN0
ZWQgUm9vdCBjTtMxEDAObGVBAsTB1Jvb3QgQ0ExHjAcBgNVBAMTFXJvb3RDQS5y
dXN0ZWRYb290LmNvbTEjMCEGCSqGSIB3DQEJARYUYWRtaW4ucnVzdGVkcm9vdC5j
b20wHhcNMDQwODI4MDQyMDM2WHcNMDUwODI4MDQyMDM2WjCBkzELMAkGA1UEBhMC
VVMxCzAJBgNVBAGTAK1BMRMwEQYDVQQHEwPb3hib3JvdWdoMRgwFgYDVQQKEw1U
YW5rIERvZyZyBUb3lzMRQwEgYDVQQLLEwtUYW5rIFN0aWNrczEVM5O8sRMp10BLI
LnRhbmsuY29tMR0wGwYJKoZIhvcNAQkBFg5hZG1pbi50YW5rLmNvbTCBnzANBgkq
hkiG9w0BAQFFAAOBjQAwgYkCgYEA65WjIJCevYynLrWUsPz1H+VM5O8sRMp10BLI
vSTCwSrWD9rn0Hut9R3Cwc2MmjecDk8avDXxv+VqKLkI41KGLz6yniNcJvFsLi8X
InXrRL53INAXkC1xbP0jsnz5iJU9aquvh81ak/f2nvKm9p9y8QLGYouDdzoFBHc4
kE5DN0eCAwEAaAaOCAQAwgf0wHQYDVR0OBByEFD1zYK+rK0zEDJ1hrHev7Q09OQhx
MIHNBgNVHSMGegcUwgcKAFDk1ekYe8uAEXrt7/JldSbgAg9ioYGmpIGjMIGMQsw
CQYDVQQGEwVUzELMAkGA1UECBMCTUEEzARBgNVBAcTckJveGJvc91Z2gxGDAW
BgNVBAoTD1Jlc3RlZCBzSb290IEl0QzEQMA4GA1UECXMHU9vdCBDQTEeMBwGA1UE

```

```
AxMvCm9vdENBLnJ1c3RlZHJvb3QuY29tMSMwIQYJKoZiHvcNAQkBFhRhZGlpb15y
dXN0ZWRYb290LmNvbYIBADAMBgNVHRMEBTADAQH/MA0GCSqGSIb3DQEBAUA4GB
AKC9izT+RkBQ8lUOK2VsLMYSi7a6uAzJwUwfIezYevl9U1AgQKrO++GvKkaTwfCS
NerJajut7JZr+JOH4+Ai16Ccz7yZjzqZ8/lFmB0dDzJGlib5ASE0eiy/+azp6GFG1
acYcDdCtNaa3oR6DknNKDWihRQpIF3P/rFsbPb0+t/OD
```

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

```
quit
```

```
% Enter PEM-formatted encrypted private key.
```

```
% End with "quit" on a line by itself.
```

```
-----BEGIN RSA PRIVATE KEY-----
```

```
Proc-Type: 4, ENCRYPTED
```

```
DEK-Info: DES-EDE3-CBC, C33CAD1289ACFEFA
```

```
J9YQleEprFS2otCWKJJUm9N6mul6bvZCyJNe8B/frxApPVP944SqN1MjF6ZiDhHN
GDSyVSxwSmdkqhWdYW9wWy3nbcJ8On005jfvplmnMtLRJS95doDF0MhdD59RI2O
ZzUir+tyBSdhPGnBYgdNta4z6QaITALEHOpSfQFe5fRc55311esySCCMTTSsioZB
2h8RJ/7dbFbJlHoI7vNX5/Eu0Xa40aVUPa7vWJYcU+NF105xgO4zQt4JHHKg607v
JSEJGN/L+8WG0UC7jLUMdpupL1LQB4wHMzVU3Ir5pLbZje3KT7DZE3J450rCWR+3
JhoQLAM44xWgOzcEue3Fdt7Qn1LEuAXNiRs4oZBXNTP4FtwcOcwIbMF/yJVeQSm
sPgTop+NMj+rrf8IX9PjmFNiu9mnruanGs9hkrDjmoeV1685csDT9mSNhKZbWgUs
M/2RUNXdHSNesSsaMLVG581LY54fvrd6Q3iPGcCOEsWUirXvqkZjJvaPUUsV/V/q
Ljn9/900U5lYrgQCX8Qt4k3qfJuzh9jIK4wW8fqPDGc/iDqH6yh3ykSc4OL1xRGr
0rL6AfViBg4yTCFh4iN3JeGmlfCpn0fQloc0UzBE1N/0nJnAqR6VvFTTmlgtixFz
7EqshltIRPT/nZAwOVpMcEFQZ3CaOL0tO9Z5+j9hstj3IIqFhU8CXgUhH3ofuPAE
gJL600U13TydXtNazR4/jTX5M+6EQrQNNor8RW9zfH/ATA2+Kmr1bfsMn+tQJsop
ln0HAqSgGisEUy0RSaw6tuOpnlz/9wQH4x0K/S/LSYIkRUyVFHwXcA==
```

```
-----END RSA PRIVATE KEY-----
```

```
quit
```

```
% Enter PEM-formatted certificate.
```

```
% End with a blank line or "quit" on a line by itself.
```

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

```
MIICmzCCAgQCAQEwDQYJKoZiHvcNAQEEBQAwgZMxCzAJBgNVBAYTAlVTMQswCQYD
VQQIEwJNQTETETMBEGA1UEBxMKQm94Ym93VnaDEWMBQGA1UEChMNvGFuayBeb2cg
VG95czEUMBIGA1UECXMlVGFuayBTdGlja3MxFTATBgNVBAMTDHd3dy50YW5rLmNv
bTEdMBSGCSqGSIb3DQEJARYOYWRTaW4udGFuay5jb20wHhcNMDQwODI4MDQzNTU2
WhcNMDUwODI4MDQzNTU2WjCB1zELMAkGA1UEBhMCVVMxCzAJBgNVBAGTAk1BMRMw
EQYDVQQHEWpCb3hib3JvdWdoMRYwFAYDVQQKEw1UYW5rIERvZyB1b3lzMrgwFgYD
VQQLEw9UYW5rIENoZXcgU3RyY2sxFTATBgNVBAMTDHd3dy50YW5rLmNvbTEdMBSG
CSqGSIb3DQEJARYOYWRTaW4udGFuay5jb20wgZ8wDQYJKoZiHvcNAQEEBQADgY0A
MIGJAoGBANSFialDM3AuM82o2ypTtyo1F2hGaQHtUx1NVAcS Yeph9qg3Mvxd1Wr
ubCKZPCJFJGLOK9noA1QMdiXKqQPW5EuMXHff+ZeocT41VteTl/eWmPC7x4Eh jxk
ZVwD+yZo03H3c6EnxFVMEW4kwHZfICq2YklHPRoMSozC+M7i6p+NAGMBAAEwDQYJ
KoZiHvcNAQEEBQADgYEAbRuXwfiUggg51i/6PJmY5qyJO8cOnKoc2tZxtE4Ed4jj
/Uoh0v8xBJAbTGwD0h/gJCOgmF3/MTJ1HodL2srx9wP6OQcdKBg3YiwEMcj7dSZK
8awdXCJ/gwmOGc7xJt6cOKDXnhjAvEsHcm8A7GQ2aROvJL3y3ozNeqdxhH3dwh0=
```

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

```
quit
```

```
% PEM files import succeeded.
```

## Verify

Use these commands to view your certificates and trustpoints:

- `ssl-mod#show crypto ca certificates server-tank.com`
- `ssl-mod#show crypto ca trustpoints server-tank.com`
- `ssl-mod#show crypto key mypubkey rsa`

## Troubleshoot

This section provides information you can use to troubleshoot your configuration.

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

If your private key is not encrypted, you can use **openssl rsa -in your-key.PEM -out new-key-des3.PEM -des3** to encrypt it.

## 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
<a href="#">Viewing real server and client IP address in CSS using single arm config</a> - Dec 15, 2004
<a href="#">Graphing VIPs on CSM with SNMP</a> - Dec 14, 2004
<a href="#">Cannot ping VIP on CSS 111500 using sg0730203 (07.30.2.03)</a> - Dec 14, 2004
<a href="#">Some Basic Getting Started Info for CDN</a> - Dec 14, 2004
<a href="#">CPU utilisation on 11503</a> - Dec 14, 2004

## Related Information

- [Catalyst 6500 Series SSL Services Module Product Support](#)
- [Technical Support - Cisco Systems](#)

---

<a href="#">Home</a>	<a href="#">How to Buy</a>	<a href="#">Login</a>	<a href="#">Profile</a>	<a href="#">Feedback</a>	<a href="#">Site Map</a>	<a href="#">Help</a>
----------------------	----------------------------	-----------------------	-------------------------	--------------------------	--------------------------	----------------------

All contents are Copyright © 1992-2004 Cisco Systems, Inc. All rights reserved. [Important Notices](#) and [Privacy Statement](#).