

# Domino 服务器 SSL 证书安装文档



沃通电子认证服务有限公司

WoTrus CA Limited

©2004-2022 沃通电子认证服务有限公司 WoTrus CA Limited All Rights Reserved

---

## 目录

一、 获取 SSL 证书.....	3
二、 安装 SSL 证书.....	6
三、 测试 SSL 访问.....	10
四、 备份 SSL 证书.....	10

### 技术支持联系方式

技术支持邮箱: [support@wosign.com](mailto:support@wosign.com)

技术支持热线电话: 0755-26027828 / 0755-26027859 / 0755-26027827

技术支持论坛: <https://bbs.wosign.com>

公司官网地址: <https://www.wosign.com>

## 一、 获取 SSL 证书

### 1.1、创建密钥环文件

Domino 服务器部署不支持导入外部或第三方生成的私钥文件，需要在 Domino 服务器上创建私钥文件。

1) 打开 Lotus Domino 管理客户端，选择“文件”-“应用程序”-“打开”，然后选择“服务器证书管理”应用程序(certsrv.nsf)，点击“Create Key Ring”：



2) 填写服务器密钥环信息：

Key Ring File Name	指定密钥环 kyr 文件的名称和保存位置
Key Ring Password	设置密钥环 kyr 文件的密码
Confirm Password	确认密码
Key Size	算法位数，选择 2048
Common Name	证书绑定主域名，如 test.wosign.com

Organization	申请证书企业、单位名称
State or Province	所在地，如 Shenzhen
Country	国家编码，如 CN

Key Ring Information	Quick Help
Key Ring File: <input type="text" value="test.wosign.com.kyr"/> Name: Key Ring: <input type="password" value="*****"/> Password: Confirm Password: <input type="password" value="*****"/>	Specify the name and password for the key ring file.  <b>Note:</b> You'll be referring to the key ring information you enter here in subsequent steps as you create and install certificates into the key ring.
Key Size	
Key Size: <input type="text" value="2048"/>	Key Size is the size of the public/private key pair in bits. The larger the key size, the greater the encryption strength.  <b>Note:</b> This Edition of Domino provides the ability to generate RSA keys at both 1024 bits and 512 bits, in accordance with export regulations worldwide.
Distinguished Name	
Common Name: <input type="text" value="test.wosign.com"/> Organization: <input type="text" value="WoTrus CA Limited"/> Organizational: <input type="text" value=""/> (optional) Unit: City or Locality: <input type="text" value=""/> (optional) State or Province: <input type="text" value="ShenZhen"/> (no abbreviations) Country: <input type="text" value="CN"/> (two character country code)	The Distinguished Name is the information about your site that will appear in any certificates you create.  <b>Note:</b> Make sure the Common Name matches the URL of your site. Some browsers check the Common Name and the site URL, and do not allow a connection if they don't match.

填写完成以上信息后，点击页面最下方的“Create Key Ring”按钮，在随后弹出的窗口，点“确定”，服务器密钥环文件就创建好了。

## 1.2、创建 CSR 文件

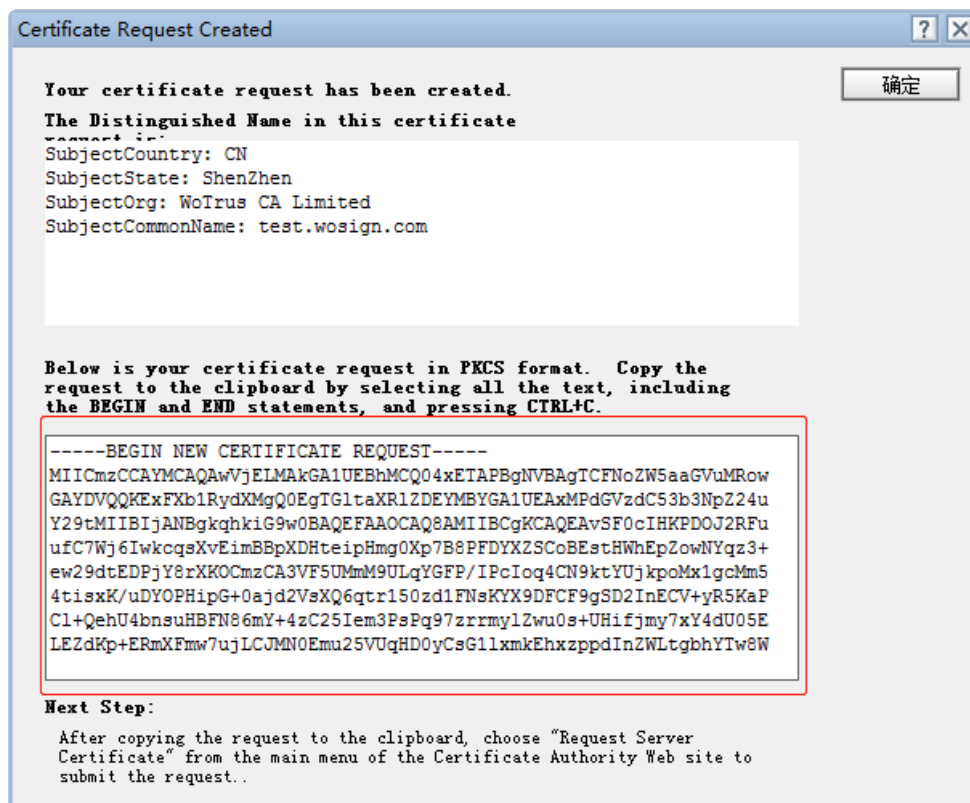
- 1) 点击“Create Certificate Request”，生成 CSR。



2) 选择之前创建密钥环文件，方式 Method 选择“Paste into from on CA’s site”，点击“Create Certificate Request”，输入密钥环密码。

Key Ring Information		Quick Help
Key Ring File Name	<input type="text" value="keyfile.kyr"/>	Specify the key ring file.
		<b>Note:</b> The key ring contains the Distinguished Name information that will be included in the certificate request.
Certificate Request Information		
Log Certificate Request	<input checked="" type="checkbox"/>	Log certificate requests for future reference.
		<b>Note:</b> Choose “View Certificate Request Log” in the main menu page to see a listing of all logged requests.
Method	<input checked="" type="radio"/> Paste into form on CA’s site <input type="radio"/> Send to CA by e-mail	Choose how to submit the certificate request to the Certificate Authority.  <b>Note:</b> The “Paste” method is recommended if it is supported by the Certificate Authority you are using.
<input type="button" value="Create Certificate Request"/>		

3) 复制 CSR 内容，提交到沃通申请证书 CSR 提交界面。



## 二、 安装 SSL 证书

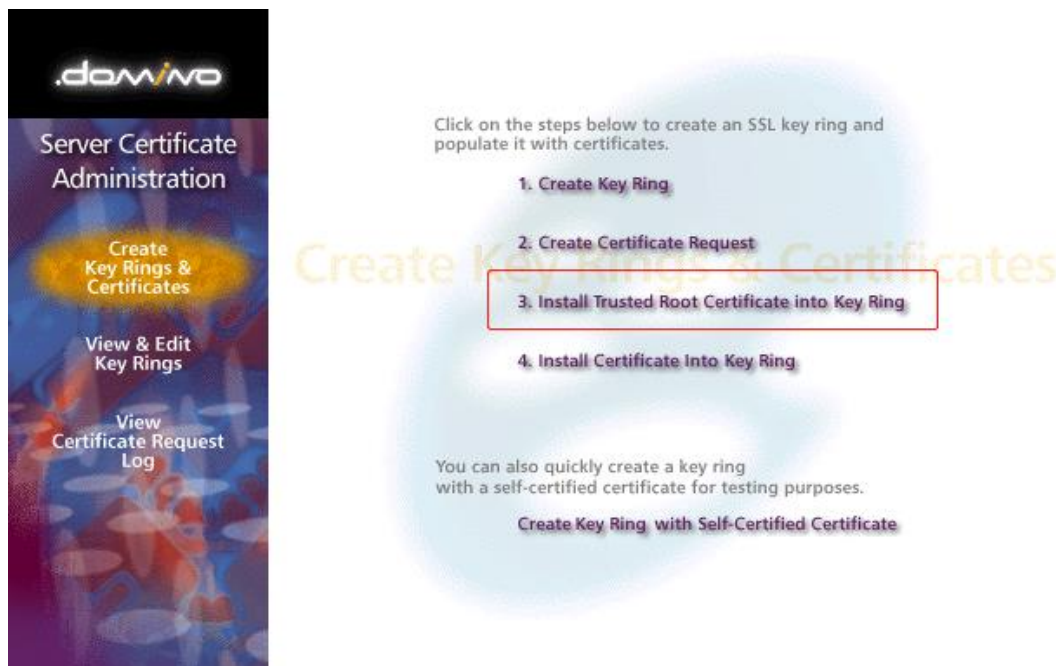
### 2.1、获取 SSL 证书

证书下载后，解压 domain.com\_sha256.zip 压缩包，将会得到 for Nginx.zip、for Apache.zip、for Other Server.zip 三个压缩包，Domino 服务器需要用到 for Other Server 中的证书，解压 for Other Server.zip，得到以下文件：

名称	修改日期	类型	大小
 cross.crt	2019/9/23 星期...	安全证书	2 KB
 issuer.crt	2019/9/23 星期...	安全证书	3 KB
 root.crt	2019/9/23 星期...	安全证书	2 KB
 test.wosign.com.crt	2019/9/23 星期...	安全证书	3 KB


## 2.2、导入 SSL 证书

### 1) 点击“Install Trusted Root Certificate Into Key Ring”

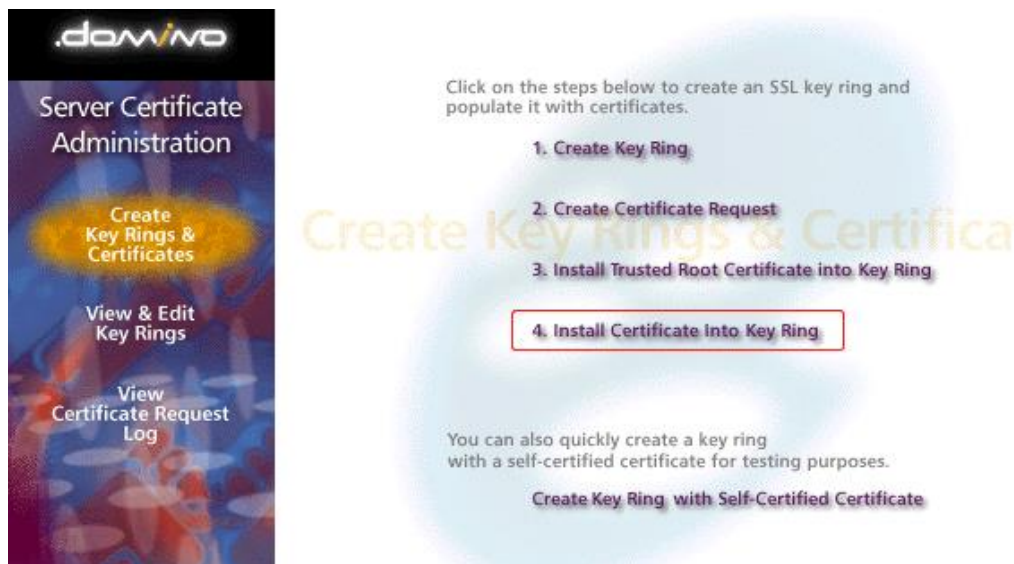


2) 将证书按照 **root.crt-->cross.crt-->issuer.crt** 的顺序，依次导入密钥环文件中，导入时支持选择文件和粘贴内容两种方式，导入过程中需输入密钥环密码。



Certificate Information	
Certificate Label 	The identifier you'll see for this certificate when you choose "View & Edit Key Ring" from the main menu.
Certificate Source	<input type="radio"/> File <input checked="" type="radio"/> Clipboard
Certificate from Clipboard: <pre>-----BEGIN CERTIFICATE----- MIEMjCCAxqgAwIBAgIBATANBgkqhkiG9w0BAQUFADB7MQswCQYDVQQGEwJHQQjEb MBkGA1UECAwSR3JlYXRlc1BNYW5jaGVzdGVyMR4wDgYDVQHDAdTYWxmb3JkMR0w GAYDVQQDBFdb21vZG8gQ0EgTG1taXR1ZDEhMB8GA1UEAwYQFBIEN1cnRpZm1l YXR1IFN1cnZpY2VzMB4XDTAOMDEwMTAwMDAwMFAwXDTI1MTIzNTk1OVVowezEL MAkGA1UEBhMCR01xGzA2BgNVBAgMEkdyZWFOZDI1IHRlZDhlc3R1c2EQA4GA1UE BwwHU2FzZm9yZDEaMBGGA1UECgwRQ29tb2RvIENBIExpbW10ZWQxITAfBgNVBAMM GEFBSBZKXJ0aWZpY2F0ZSBTZXJ2aWN1czCCASIwDQYJKoZIhvcNAQEBBQADggEP ADCCAQoCggEBAL5AnfRu4ep2hxxNRUSOvkbIgwadwSr+GB+05AL686tdUIoWMQQua BtDFcCLNSS1UY8y2bmhGCLPqy0wkwLxyTurxF70VJoSCaN6ajNg4tqJVFMIWPPe 3M/vg4aijJRPn2jymJBGhCfHDr/jzDUsi14HZGWCwEiwqJH5Y92IFCokodmet4 YgNW8IoaE+oxox6gmf049vYnMlhvB/VruPsUK6+3qszWY19zjNoFmag4qMsXeD2R r0me9Hg6jc8P2ULimAyrL580Ad7vn51J8S3frHRNG5i1R8X1KdH5kBJHYpy+g8cm ez6KJcfA3Z3mNWgQIJ2F2N7Sw4ScDV7oL8kCAwEAaOBwDCBvTAdBgNVHQ4EFgQU oBEKIz6W8Qfs4q8p74K1f9AwpLQwDgYDVROPAQH/BAQDAgEGMA8GA1UdEwEB/wQF MAMBAf8weWYDVROfBHQwcjA4oDagMIYyaHR0cDovL2NyYyC5jb21vZG8gY5S5jb20v QUFBQ2VydG1maWNhdGVtZXJ2aWN1cy5jcmwWNgA0oDKGMGh0dHA6Ly9jcmwWY29t b2RvLm5ldC9BQUFDBZKXJ0aWZpY2F0ZVN1cnZpY2VzLmNybDANBgkqhkiG9w0BAQUF AAOACAEACFb8AvCb6P+k+ztZ7xkSAzk/ExfYANMytzwUSWgEdujm713sAg9g1o1Q GE8mIqHj5rC17r+8dFRBv/38ErjHT1r0iWAFf2C3BUrz9vHCv8S5dIa2LX1rzNLz Rt0vXuBqw8M0Ayx91t1awg6nCpnBBYurDC/zXDrPbDdVCYfeU0BSWO/8tqt1bgT2 G9w84FoVxp7Z8VlIMCF1A2zs6SFz7JsDoeA3raAVGI/6uGL0pyypEBMs10UIJqs1 12D4kF501KKAU73yqWjgom7C12yxow+ev+to51byrvLjKzg6CYG1a4XXvi3tPqx3 smP19W1sgtRqAEFQ8TmDn5XpNpaYbg== -----END CERTIFICATE-----</pre>	The source of the certificate can be from a file or from the clipboard.  Paste clipboard contents into this field.  <b>Note:</b> The pasted certificate must include the "Begin Certificate" and "End Certificate" lines.
Merge Trusted Root Certificate into Key Ring	

3) 点击“Install Certificate Into Key Ring”,将用户证书公钥 **domain.com.crt** 文件导入密钥环文件中，导入过程中需输入密钥环密码。





Certificate Information

Certificate Source

File

Clipboard

The source of the certificate can be from a file or from the clipboard.

Paste the clipboard contents into this field.

Note: The pasted certificate must include the "Begin Certificate" and "End Certificate" lines.

Certificate from Clipboard:

```



-----BEGIN CERTIFICATE-----
MIIF4DCCBMigAwIBAgIQXykHgMEV/85e1M3xwhSrHjANBgkqhkiG9w0BAQsFADBC
MQswCQYDVQQGEwJDTjEaMBGGA1UEChMRV29UcnVzIENBIEExpbW10ZWQxMTAvBgNV
BAMKfKdVHJ1cyBPFVBTZXJ2ZXIgc0EgIFtSdW4gYnkgdGhlIElzc3Vlc10wHhcN
MjEwMzI1MDAwMDAwWhcNMjEwMzI1MjM1OTU5WjBiMQswCQYDVQQGEwJDTjEaMBG
A1UEBwwJ5rex5Zyz5biCMSowKAYDVQQKDCHmt7HlnLPluILnmb3mspnnianmtYHm
nInpmZDlhaz1j7gxARBgNVBAMTCm9hLmJzNTYuY24wggeiMA0GCSqGSIb3DQEB
AQUAA4IBDwAwggEKAoIBAQCnLvLsC/2e7syB2GeDYFZndo2eeA1rDNu2CxcyclVS
2jieBOVc+5jGATdwtiLfsBfGZGQMYf+5quYdcUYB9WjOvS9Bmw/9gPr3dklijEq
HjG/K8onn1P39GyIFmW3oLJfPknoIJtBbAgxlnGQYDx1LYhWRm7PjAUjk39KZQb6
b0d7elp8cywNeXLRGu3xmDrh+15LKOBJVpEOacvlmsyy0K6ajd3o/1VjBcfJGfWL
GHiGP7I6CrhIWQKmJNmpJzT/ABqTjI/cTPUH4ttCRpOU+dBgYVWvL+vRxpJUIo+4
7h3nPg7YKaJp5JjMiYrGto11HqDTzFUpMHZP44nH1Ao3AgMBAAGjggKMMIICkjAf
BgNVHSMEGDAwBgNVSY8VM3vAT7b7OjgJ/DQV2mDdFDAdBgNVHQ4EFggQUURxcY14N
kWTAX/2vwPTNz90VjTowDgYDVROPAQH/BAQDAgWgMAwGA1UdEwEB/wQCMAAwHQYD
VR01BBYwFAyIKwYBBQUHAWEGCCsGAQUFBwMCMekGA1UdIARCEAAwNAYLKwYBBAGy
MQECAhYwJTAjBggrBgEFBQcCARYXaHR0cHM6Ly9zZWNoaWdvLmNvbS9DUFMwCAYG
Z4EMAQICMDGA1UdHwQ2MDQwMgAwC6GLGh0dHA6Ly9jcmwuY3Jsb2NzcC5jb3bi9X
blRydXNPFV1Nclncl2lckNBXzIuY3J5MGwGCCsGAQUFBwEBBGAwXjA4BggrBgEFBQc
wAoYsaHR0cDovL2FpYS5jcmxvY3NwLmN1L1dvVHJlc09WU2VydMvYQ0FfMi5jcnQw
IgyIKwYBBQUHMAAGFmh0dHA6Ly9vY3NwLmN1bG9jY3AuY24wggeCBgorBgEEADZ5
AgQCB1HzBIHwA04AdQBGPVXrdfqRIDC1oolp9FN9ESxBdL79SbiFq/L8cP5tRwAA
AXhnBYpAAAAEAwBGMEQCIGKOVfd1G1l1VN1RH9hCaumP12/mM9TXQMBz2kkYsD3j
A1B/JydDpgSS0+NnPyGkkENSd7t1zif5I+MzV17J1A9kewB1AN+1Xqtogk8fbK3u
uF90PlrqzaISpGpejjsSwCBEXCpZAAABeGcFidkAAQDAEYwRAIgEuzxNJYB6yM9
w0sEbfFniyMJ2KttK9kboaxETo4ZBNcCIBVXQAJgLVZKqNa1Q/idKvhTHG2PKcYi
bcfl12jSkCJBTMBUGA1UdEQQOMAYCCm9hLmJzNTYuY24wDQYJKoZIhvcNAQELBQAD
ggEBABQ1fa6ndOeH38KARYBMpSNW/WF+wduy/3C5vcP7ehyEnISrDx5b/YgjcFY
a1DAMtcgaE9tE/191rx4IMtuCRWQOWClm4F4Qh5FUxQyXwAFfHESudTJ1vV4i3tJ
ppZ5dI2mWvIzvFuUv5ce+W1o9JrXzPU6jP2q6tCJ9s7Erqlp6b8AmubU1e2a9ad1
mYl+VyzulmSgnzMCIC2fn8LpHXZG1gtRYqWD783AnPgQVmo0fEeHXZUsFgmlsXvTB
n+QggeJfT/muY05pxg51EFj8+XGRPHFAZJELvvYAEb22hcA1vohSnUECGyiZcz9G
/13grno55pQoTHGmC42yvi9Mvs=
-----END CERTIFICATE-----

```

Merge Certificate into Key Ring

### 2.3、配置 SSL 证书

1) 将导入证书后的密钥环文件到服务器数据目录下(IBM/[Lotus]/Notes/Data)，密钥环文件包含 keyfile.kyr 和 keyfile.sth。

 test.wosign.com.kyr	2021/6/11 10:32	KYR 文件
 test.wosign.com.sth	2021/6/11 10:13	STH 文件

2) 打开服务器配置文档，选择“端口”-“Internet 端口”选项卡，选择密钥环文件进行配置。

地址：中国深圳市南山区南海大道 1057 号科技大厦二期 A 座 502

第 9 页

电话：0755-86008688 网站：www.wosign.com | www.wotrus.com

基本	安全性	端口...	服务器任务...	Internet 协议...	MTA...	杂项	事务记录	共享邮件	DAOS	Lotus Traveler	管理
Notes 网络端口   Internet 端口...   代理											
SSL 设置											
SSL 密钥文件名:			keyfile.kyr								
SSL 协议版本 (用于除 HTTP 以外的所有协议):			可协商的								
接受 SSL 站点验证字:			<input checked="" type="radio"/> 是 <input type="radio"/> 否								
接受到期的 SSL 验证字:			<input type="radio"/> 是 <input checked="" type="radio"/> 否								
SSL 加密法:			RC4 加密 (128 位密钥和 MD5 MAC) RC4 加密 (128 位密钥和 SHA-1 MAC) 三重 DES 加密 (168 位密钥和 SHA-1 MAC) DES 加密 (56 位密钥和 SHA-1 MAC) RC4 加密使用 40 位密钥和 MD5 MAC								
<input type="button" value="修改"/>											
启用 SSL V2: (始终启用 SSL V3)			<input type="checkbox"/> 是								

### 三、 测试 SSL 访问

打开浏览器，输入 <https://yourdomain.com>（证书绑定的实际域名），如浏览器地址栏显示加密小锁，则表示证书配置成功。若显示无法连接，请确保防火墙或安全组等策略有放行 443 端口（SSL 配置端口）。

### 四、 备份 SSL 证书

请将下载的.zip 压缩包和自主生成的私钥.key 文件备份，以防丢失，影响后续使用！