



让互联网更加安全可信

沃通电子认证服务有限公司

WoTrus CA Limited

# 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

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	『test.wosign.com.kyr』	Specify the name and password for the key ring file.
Name:	『*****』	<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 Ring	『*****』	
Password:	『*****』	
Confirm Password:	『*****』	
Key Size		
Key Size:	『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:	『test.wosign.com』	The Distinguished Name is the information about your site that will appear in any certificates you create.
Organization:	『WoTrus CA Limited』	
Organizational Unit:	『』 (optional)	
City or Locality:	『』 (optional)	<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.
State or Province:	『ShenZhen』 (no abbreviations)	
Country:	『CN』 (two character country code)	
<b>Create Key Ring</b>		

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

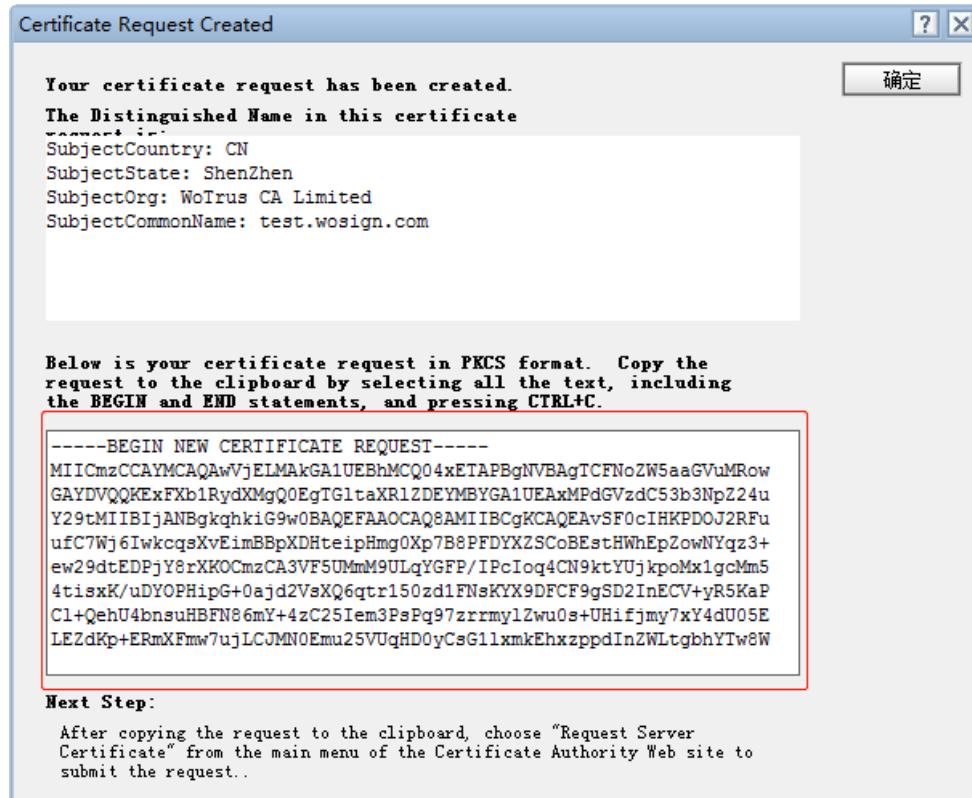
- 1) 点击“Create Certificate Request”,生成 CSR。



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。

<b>Key Ring Information</b>		<b>Quick Help</b>
Key Ring File <input type="text" value="keyfile.kyr"/> Name		Specify the key ring file.  <b>Note:</b> The key ring contains the Distinguished Name information that will be included in the certificate request.
<b>Certificate Request Information</b>		
Log Certificate <input checked="" type="checkbox"/> Request		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

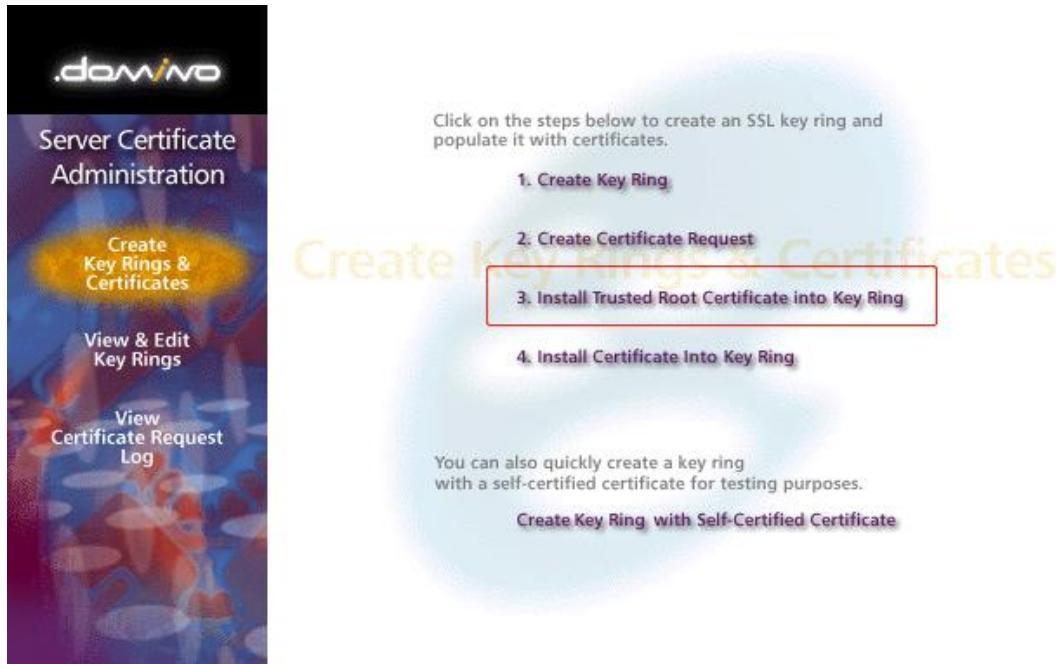
### 2.1、获取 SSL 证书

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 <input type="text"/>		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	The source of the certificate can be from a file or from the clipboard.

Certificate from Clipboard:

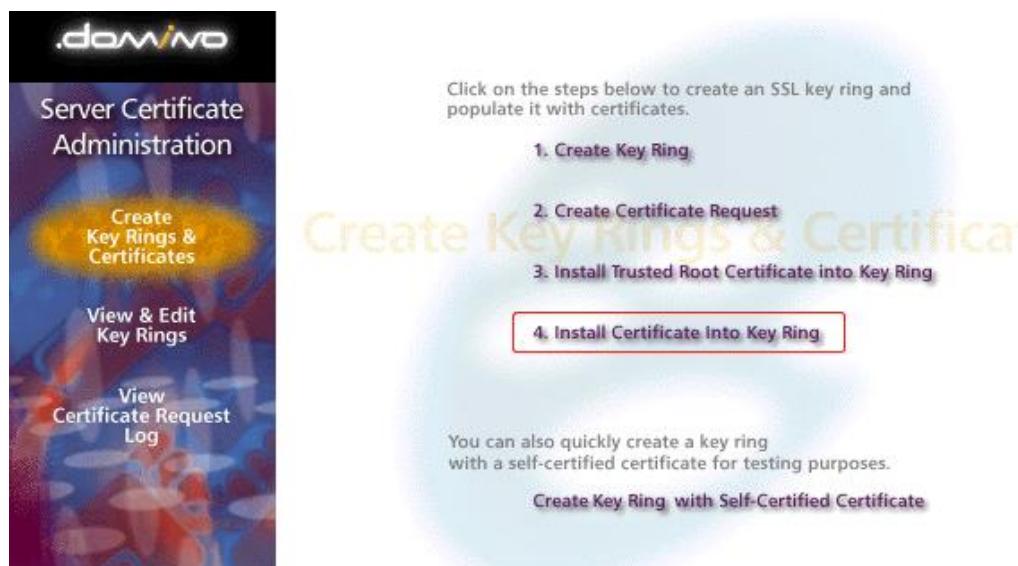
```

-----BEGIN CERTIFICATE-----
MIIEkjCCAxggAwIBAgIBATANBgkqhkiG9w0BAQUFADB7MQswCQYDVQQGEwJHQjEB
MBkGA1UECAwSR3JLYXRLciBNYN5jaGVzdGvYMRAwDgYDVQQHDAadTlWxmb3JkRRow
GAYDVQQKDBFDb21vZG8gQ0EgTGltaxR1ZDEHMB8GA1UEAwYQUBFIE1cnRpZmlj
YXRlIiFN1cnZpY2VtM84XDThAMDEwMTAwdAwMFOxDTI4MTIzMTIzNTk1OVowezEL
MAkGA1UEBMCR0IxGzA2BgNVBAgMEkdyZWNf0ZXIgTlNuY2hlc3RlcjEgMA4GA1UE
BwwHU2FsZm9yZDEaMBgGA1UECgwRQ29tb2RvIENBIExpbWl0ZWQxITAfBgNVBAMM
GEFBQSBDZXJ0aWZpY2F0ZSBTZXJ2aWN1czCCAS1wDQYJKoZIhvcNAQEBBQADgEP
ADCCAQcGgEBAL5AnFRu4ep2hxNRUS0VkbIgwadwSr+GB+OSAL686tdUICNQua
BtDFcCLN81UY8y2bmhGC1Pqy0wkLxyTurxf7a70VJoSCsN6sjNg4tqJVFMiWPPE
3M/vg4aijJRPN2jymoBGFCHdr/jzDUsi14HZGWCWeiwqJH5Y292IFCokcdmtet4
YgNWB1caE+oxox6gmf049vYnMlhvb/VruPsUK6+3qszWY19zjNoFmag4qMsXeDZR
rOme9Hg6jc8P2ULimAyrL580Ad7vnS1J8S3frHRNG5i1R8X1KdH5kBjHYp+g8cm
ez6KUcfA323mWqgQIj2P2N7sw4ScDV7oL8kCawEAoBwDCBvTadBgNVHQ4EFgQU
oBEK1z6W8Qfs4qpP74Klf9AwpLQwDgYDVROPAQH/BQAQDaEGMA8GA1UdEwEB/wQF
MAMBAF8newYDVR0fBHQwcjA4oDagNIYyaHR0cDovL2Nybc5jb21vZG9jYSSjb20v
QUBFQ2Vyd1maWHdGVTZXJ2aWN1cy5cmwWhQAOoDKGMGhdHA6Ly9jcmwuY29t
b2RvLm51dc9BQUDZKJ0aWZpY2F0ZVN1cnZpY2VzLmNyBDANBgkqhkiG9w0BAQUF
AAOCARQERACFb8AvC6P+k+c7xkSAzk/ExFYAWMytrwUSWgEdujm713sAg9glo1Q
GE8mfghj5xCL1r+8dFRBv/38ErjHT1ro1WAFF2C3BUrz9vHCv8S5dia2LX1rzNLz
Rt0vxuBgw8M0ay9lt1awg6nCpnBBYurDC/zXDrPbDdVCYfeU0BsWO/8tgt1bgT2
G9w84FoVxp728v1IMCF1a2zs6Sz7JsDoeA3raAVGI/6ugLOpyypEBMs1OUIJqsi
12D4KF501KKuU73yqWjgom7C12yxow+ev+to51byrvLjKzg6CYG1a4XXvi3tPxq3
smPi9WIsgtRqAEFQ8ImDn5XpNpAyBgg==
-----END CERTIFICATE-----

```

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	<input type="radio"/> File <input checked="" type="radio"/> Clipboard
Certificate from Clipboard: <pre>-----BEGIN CERTIFICATE----- MIIF4DCCBMrAgIBAgIQYykHgMEV/8selM3xwhSrHjANBgkqhkiG9w0BAQsFADbc MQswCQYDVQQGEwJDTjEaMBgGA1UEChMRV29UcnVzIEENBIEpbWl0ZWQzMtAvBgNV BAMMKFdVJ1cyBFViBTZXJ2ZXIgQ0EgIFIftSdW4gYnkgdGh1IE1zc3Vlc10wHhcN MjEwMzI1MDAwMDAwWhcNMjIwMzI1MjM1OTU5WjB1MQswCQYDVQQGEwJDTjESMBAG A1UEBww5rex5Zyz5biCM5owKAYDVQQKDCHmt7HlnLPluILnmk3mspnniamtYHm nInpmZDlhazlj7gxEzARBgNVBAMTCm9hLmzNTYuY24wggEiMA0GCSqGSIb3DQE AQAA4IBDwAwggEKAoIBACnLvLsC/Ce7syB2GeDYFZndo2eeAIrDNu2Cxycy1VS 2jjeBOVc+5jGATdwstilfsBfGZGQMYf+5quYdcUYB9WjOvS9Emw/9gPr3dk1ijEq HjG/K8onn1P39GyIfMW3oLJFpknoIJtBbAqxlnGQYDx1LYhWRm7PjAUjk39KZQb6 b0d7elp8cywNeXLRgU3xmDrh+15LK0bjVpEOacvImssyy0K6ajd3o/1VjBcfJGFNL GHiGP7I6CrhIWQKmJNcqJzT/ABqTjI/cTPUH4ttCRpOU+dBgyVWvL+vRxpJUIo+4 7h3nPg7YKaJp5JjMiYrGto11HqTzFUpMHzP44nH1Ao3AgMBAAGjggKWMIIcKjAf BgNVHSMEGDAwBQNSY8VM3vAT7b70jgJ/DOV2mDdFDAdBgNVHQ4EFgQUURxcY14N kWtAX/2vwPTNz90VjTowDgYDVR0PAQH/BAQDAgWgMawGA1UdEwEB/wQCMAAwHQYD VR01BBYwFAYIKwYBBQUHwEGCCsGAQUFBwMCMEkGA1UdIARCMCAwNAYLkwyBBAGy MQECAhYwJTAjBgrBgfEFBQcCARYXaHROcHM6Ly9zZWN0aWdvLmNb89DUFMwCAYG Z4EMAQICMD0GA1UdHwQ2MDQwMqAwoC6GLGh0dHA6Ly9jcmwuY3Jsb2NzcC5jb9X b1RydXNPV1NlcnZlckNBXzIuY3JsjMGwGCCsGAQUFBwEBBGAwXjA4BggrBgfBQcw AoYsaHR0cDovL2FpYS5jcmxvY3NwLmNuL1dvVHJ1c09WU2VydmlvY0OFFm15jcqnQw IgYIKwYBBQUHMGAGFmh0dHA6Ly9vY3NwLmNybg9jcc3AuY24wggECBgorBgfEEAdZ5 AgQCBIH2BIHwAO4AdQBgpVXrdfsRQfRIDC1oop9PN9ESxBdL79SbiFq/L8cP5tRwAA AXhnBYpAAAAEwBGMEMQCIKGOfd1Gli1VNIRH9hCaumP12/mM9TXQMBz2kkYsD3j AiB/JydDpgs0+NnPyGkkENSD7t1zif5I+MzV17J1A9kewB1AN+1Xqtogk8fbK3u uF90P1rlqzaISpGpejjsSwCEBXCPzAAABeGeFidkIAAQDAEYwRAIgEuuzxNJB6yM9 w0sEbfFniyMJ2KttK9kboaxEt04ZBNcIBVXQAjgLZKqNa1q/ikVhTHG2PKcYi bcf12jskCJBTMBUGA1UdEQQOMAyCc9hLmJzNTYuY24wDQYJKoZIhvcNAQELBQAD ggEBABQ1fa6nd0eH38KAryBMpSNW/WF+wduy/3C5vcP7ehyEnISrDx5b/YgjcFYy a1DAWtcaE9tE/191rx4IMtuCRWQOwClm4F4Qh5FUXQyXwAFFHESudTJ1vvV4i3tJ ppZ5dI2mWvIzvPuuV5ce+W1o9JrXzPU6jP2q6tC9s7Erqlp6b8AmubU1e2a9ad1 mY1+Vyzu1msGnzMCICZfn8LpHXZG1gtRYqWD783AnPqQVm0fEeHXZUsFgmlsXvTB n+QggeJfT/muY05pxg51EFj8+xgRPHFAZJE1vvY AeB22hcAIvohSnUECGy1Zcz9G /13grno55poQoTHGmC42yvi9Mvs= -----END CERTIFICATE-----』</pre>	
<a href="#">Merge Certificate into Key Ring</a>	

### 2.3、配置 SSL 证书

- 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

- 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。

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.key

SSL 协议版本(用于除 HTTP 以外 可协商的所有协议):

接受 SSL 站点验证字:  是  否 是

接受到期的 SSL 验证字:  是  否 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

启用 SSL V2:  
(始终启用 SSL V3)  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！