

Domino SSL 证书安装文档



沃通电子认证服务有限公司

WoTrus CA Limited

目录

一、 获取 SSL 证书	2
1.1、选择 SSL 证书.....	2
1.2、合成 SSL 证书.....	3
二、 安装 SSL 证书	4
2.1、导入 SSL 证书.....	4
2.2、绑定 SSL 证书.....	6
三、 测试 SSL 访问	7
四、 备份 SSL 证书	7

技术支持联系方式

技术支持邮箱: supp3@wotrus.com

技术支持热线电话: 18822828659 / 0755-26027827

技术支持网页: <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. Note: 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. Note: 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 <input type="text" value="ShenZhen"/> (no abbreviations) Province: 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. Note: 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.
<input type="button" value="Create Key Ring"/>	

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

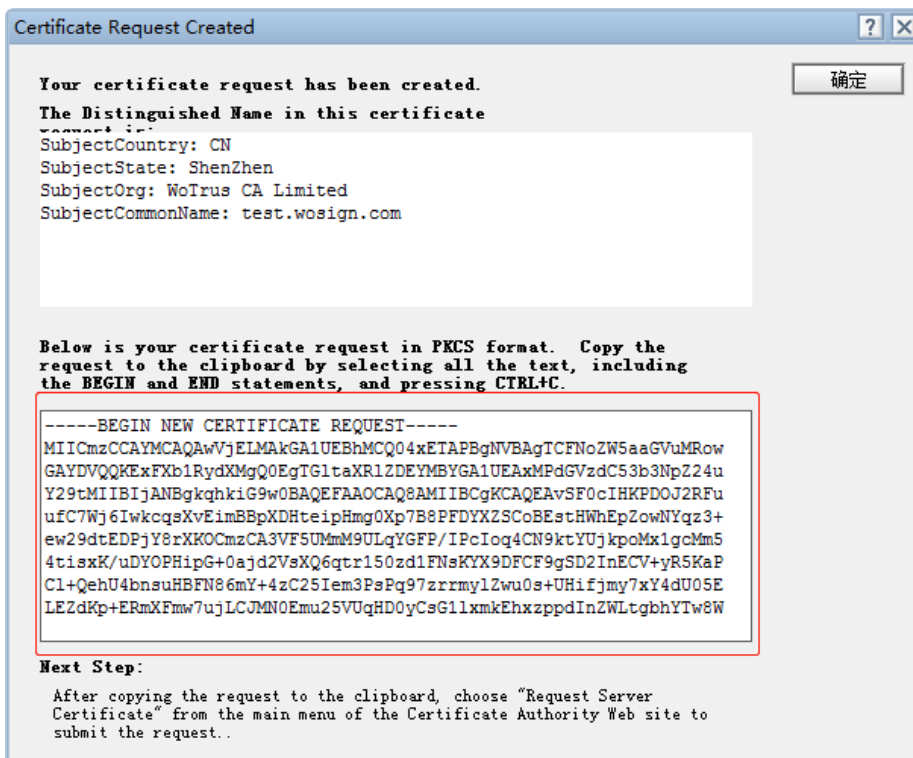
- 1) 点击“Create Certificate Request”，生成 CSR。



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 <input type="text" value="keyfile.kyr"/> Name	Specify the key ring file. Note: The key ring contains the Distinguished Name information that will be included in the certificate request.
Certificate Request Information	
Log Certificate Request <input type="checkbox" value="Yes"/>	Log certificate requests for future reference. Note: 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. Note: 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

成功在沃通申请证书后，会得到一个.zip 压缩包文件，解压后得到四个文件夹(见图 1)，不同服务器或设备要求不同的格式，Domino 服务器需要用到 OtherServer 中的证书，如图 1：

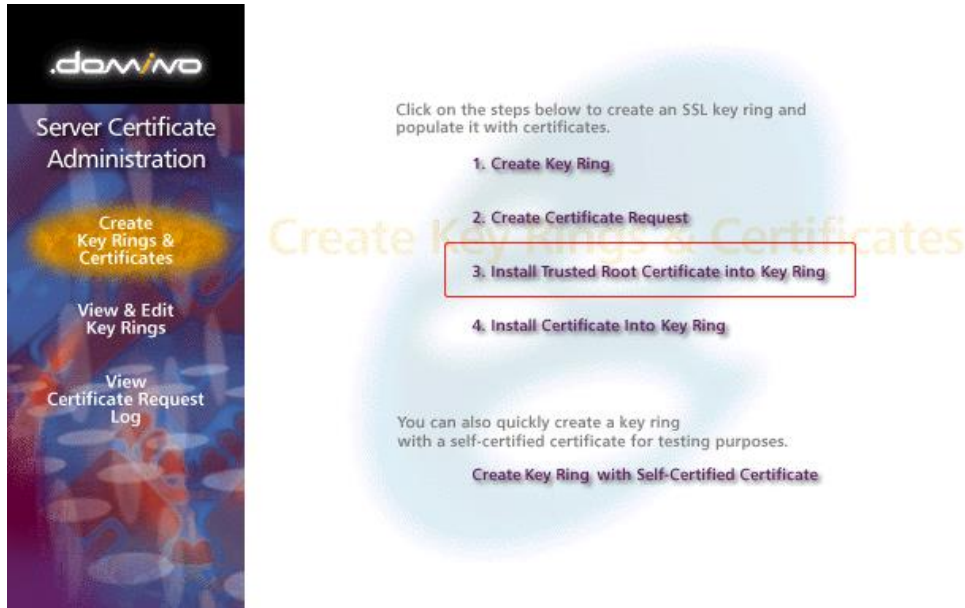
名称	修改日期	类型	大小
ApacheServer	2023/10/23 12:09	文件夹	
NginxServer	2023/10/23 12:09	文件夹	
OtherServer	2023/10/23 12:09	文件夹	
PEM格式文件	2023/10/23 12:09	文件夹	
README.txt	2023/10/23 12:09	TXT 文件	1 KB

图 1

名称	修改日期	类型	大小
cross.crt	2023/3/31 16:34	安全证书	2 KB
intermediate.crt	2023/3/31 16:34	安全证书	3 KB
root.crt	2023/3/31 16:34	安全证书	2 KB
test.wosign.com.crt	2023/3/31 16:34	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-->intermediate.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: <pre>-----BEGIN CERTIFICATE----- MIIEIjCCAxqgAwIBAgIBATANBgkqhkiG9w0BAQUFADB7MQswCQYDVQQGEWJHQQjEb MBkGALUECAwSR3JlYXRlciB5NW5jaGVzdGVyMRAwDgYDVQQHDAdYWxmb3JkMR0w GAYDVQQKQzBDb21vZG8gQ0EgTG1taXR1ZDEhMB8GA1UEAwYQUBFBIEN1cnRpZmlj YXR1IEN1cnRpZ2ZyZ2ZyZ2ZyZ2ZyZ2ZyZ2ZyZ2ZyZ2ZyZ2ZyZ2ZyZ2ZyZ2ZyZ2Zy MAkGALUEBhMCR0IeGzAZBgNVBAGMEkdyZWF0Z0Z0Z0Z0Z0Z0Z0Z0Z0Z0Z0Z0Z0Z0 BwHU2FsZm9yZDEaMBGALUECgWRQ29tb2RvIENBIEkxZWV1Z0Z0Z0Z0Z0Z0Z0Z0Z0 GEFBQSBdZXJ0aWZpY2F0ZSB0Z0Z0Z0Z0Z0Z0Z0Z0Z0Z0Z0Z0Z0Z0Z0Z0Z0Z0Z0 ADCCAQoCggEBAL5AnFRu4ep2hxxNRUSOvkbIgwadwSr+GB+O5AL686tdUIoNMQua BtDFcCLNSS1UY8y2bhmGC1Pqy0wkWxLxyTurxFa70VJcScN6sjNg4tqJVFm1WPPE 3M/vg4aijJRPN2jymJBGhCfHdR/jzDUs14HZGWCwEiwQJH5Y292IFCokodmet4 YgNW8IoaE+oxox6gmf049vYnMlhvB/VruPsUK6+3qszWY19zjNoFmag4qMsXeDZR rOme9Hg6jc8P2ULimAyrLS8OAd7vn51J8S3frHRNG5i1R8X1KdH5kBJHYpy+g8cm ez6KJcfA3Z3mNWgQIJ2P2N7Sw4ScDV7oL8kCAwEAaOBwDCBvTAdBgNVHQ4EFgQU oBEKIz6W8Qfs4q8p74K1f9AwpLQwDgYDVROPAQH/BAQDAgEGMA8GA1UdEwEB/wQF MAMBAAf8ewYDVROfBHQwcjA4oDagNIYyaHR0cDovL2Nybc5jb21vZG8yY5Y5jb2v QVFBQ2VydG1maWNhdGVIZXJ2aWN1cy5jcmwwNqA0oDKGMGH0dHA6Ly9jcmwwY292 b2RvLm5ldC9BQUF0Z0 AAOCAQACFb8AvCb6P+k+tZ7xkSAzk/ExfYAWMyt.rwUSWgEdujm713sAg9g1o1Q GE8mTgHj5rC17r+8dFRBv/38ErjHT1r0iWAFf2C3Buzr29vHCV8S5dIa2L1rzNLz Rt0vxuBqw8M0Ayx91t1awg6nCPnBBYurDC/zXDRPbDdVCYfeU0B8WO/8tqt1bgT2 G9w84FvXp7Z8V1IMCF1A2z86SFz7JsDoeA3raAVGI/6ugLOpyyPEBMs10UIJqsi 12D4kF501KkaU73yqWjgom7Cl2yxow+ev+to51byrvLjKz96CYG1a4XXvi3tPqx3 smPi9WigtRqAEFQ8TmDn5XpNpaYbg== -----END CERTIFICATE-----</pre>	Paste clipboard contents into this field. Note: The pasted certificate must include the "Begin Certificate" and "End Certificate" lines.
<input type="button" value="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。



Click on the steps below to create an SSL key ring and populate it with certificates.

1. Create Key Ring
2. Create Certificate Request
3. Install Trusted Root Certificate into Key Ring
4. Install Certificate into Key Ring

You can also quickly create a key ring with a self-certified certificate for testing purposes.

[Create Key Ring with Self-Certified Certificate](#)

Certificate Information	
Certificate Source	<input type="radio"/> File <input checked="" type="radio"/> Clipboard
Certificate from Clipboard:	<pre>-----BEGIN CERTIFICATE----- MIIF4DCCBmIwIBAgIQXykHgMEV/85e1M3xwhSrHjANBgkqhkiG9w0BAQsFADBc MQswCQYDVQQGEwJDTjEaMBGGA1UEChMRV29UcnVzIENBIEExpbW10ZWQxMTAvBgNV BAMKFDVHJ1cyBPeVlBTXJ2ZXIgc0EgIFtSdW4gYnkqdGh1IE1zc3Vlc10wHhcN MjEwMzI1MDAwMDAwWWhcNMjEwMzI1OTU5WjBiMQswCQYDVQQGEwJDTjEaMBGGA1 UEBwwJ5rex5Zyz5biCMSowKAYDVQQKDCRmt7H1nLPluILnmb3mspnnianmtYHm nInpmZDIhazlj7gxEzARBgNVBAMTCm9hLmJzNTYuY24wggeiMA0GCSqGSIb3DQEB AQUAA4IBDwAwggEKAoIABgQCNLvsC/2e7syB2GeDYFZndo2eeA1rDNu2Cxcyc1V5 2jie80Vc+5jGATdwtiLfsBFGZGQMYf+5quYdcUYB9WjOvS9Bmw/9gPr3dk1ijEq Hjg/K8onn1P39gyIfmW3oLJFpknoIjtBbAqxlnGQYDx1LYhWRm7PjAUjk39K2Qb6 b0d7e1p8cywNeXLRGu3xmDrh+15LKOBJVpEOacvmsyy0K6ajd3o/1VjBcfJGFwL GHiGP7I6CrhIWQKmJNmpJzT/ABqTjI/cTpuH4ttCRpOU+dBgyVWvL+vRxpJUio+4 7h3nPg7YkaJp5JjMiYrGto11HqDTzFUpMHZP44nH1Ao3AgMBAAGjggKwMIICkAf BgNVHSMEGDAwGBQNSY8VM3vAT7b7OjgJ/DQV2mDdFDAdbgNVHQ4EFggQUURxcY14N kWtAX/2vwPTNz90VjTowDgYDVROPAQH/BAQDAgWgMAwGA1UdEwEB/wQCMAAHQYD VR01BBYwFAyIKwYBBQUHAwEGCCsGAQUFBwMCMEkGA1UdIARCAEAwNAYLKwYBBAGy MQECAhYwJTAjBggrBgEFBQcCARYXaHR0cHM6Ly9zZWNoaWwvLmVzS9DUFMwCAYG Z4EMAQICMD0GA1UdHwQ2MDQwMgAwoC6GLGh0dHA6Ly9jcmwvY3Jsb2NzcC5jb3R1 b1RydXNFV1N1cnZlcjNlbnRzIuY3J5MGwGCCsGAQUFBwEBBGAwXjA4BggrBgEFBQcw AoYsaHR0cDovL2FpYSSjcmxvY3NwLmN1L1dvVHJ1c09WU2VydMvY0FfMi5jcnQw IgyIKwYBBQUHMAGGFmh0dHA6Ly9vY3NwLmN1bnYyY24wY24wggeCBgorBgEEAdZ5 AgQCBiHzBIHwAO4AdQBgpVXrdFqRIDC1oolp9PN9ESxBdL79SbiFq/L8cP5tRwAA AXhnBYpAAAAEAWBGMEQCIGKovfd1G1i1Vn1RH9hCaumP12/mM9TXQMBz2kkYsD3j A1B/JydDpgSS0+NnPyGkkENSD7t1zif5I+MzV17J1A9kewB1AN+1Xqtoqk8fbK3u uF90PlrqzaIspGpejjsSwCBEXCpZAAABeGcFidkAAAQDAEYwRAIgeEuznNjYb6yM9 wOsEbfFniyMJ2KtK9kboaxETo4ZBNcIBVXQAJgLVZKqNa1Q/idKvhTHG2PKcYi bcfl2jokCJBTMBUGA1UdEQQOMAYCCm9hLmJzNTYuY24wDQYJKoZIhvcNAQELBQAD ggEABQ1fa6nd0eH38KARYBmpSNW/WF+wduy/3C5vcP7ehyEnISrDx5b/YgjcFYY a1DAWtcgaE9te/191rx4ImtuCRWQOWClm4F4Qh5FUxQyXwAfffHESudTJ1vV4i3tJ ppZ5dI2mWvIzvpUuV5ce+W1o9JrXzPU6jP2q6tCJ9s7Erq1p6b8AmubU1e2a9ad1 mYl+VyzulmSgnZMCICZfn8LpHXZG1gtRYqWD783AnPqQVmo0fEeHXZUeFgm1eXvTB n+QggeJfT/muY05pxg51EFj8+XGRPHFAZJELvYAEb22hcaIvohSnUECGyicZc9G /13grno55pOQoTHGmC42yvi9Mvs= -----END CERTIFICATE-----</pre>
	<p>The source of the certificate can be from a file or from the clipboard.</p> <p>Paste the clipboard contents into this field.</p> <p>Note: The pasted certificate must include the "Begin Certificate" and "End Certificate" lines.</p>

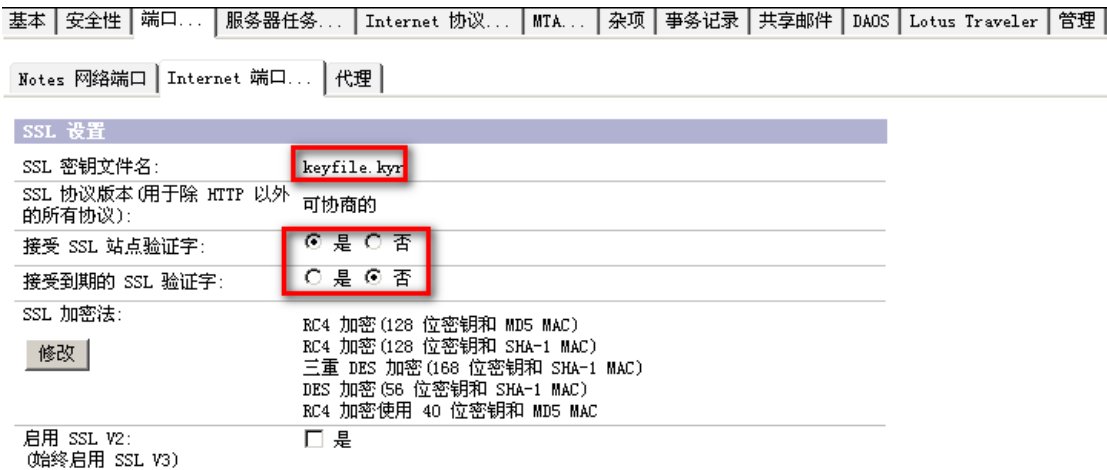
Merge Certificate into Key Ring

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。



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://test.wosign.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。

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！