

# SSL 证书 操作指南 产品文档





【版权声明】

©2013-2018 腾讯云版权所有

本文档著作权归腾讯云单独所有,未经腾讯云事先书面许可,任何主体不得以任何形式复制、修改、抄袭、传播全部 或部分本文档内容。

【商标声明】



及其它腾讯云服务相关的商标均为腾讯云计算(北京)有限责任公司及其关联公司所有。本文档涉及的第三方主体的 商标,依法由权利人所有。

【服务声明】

本文档意在向客户介绍腾讯云全部或部分产品、服务的当时的整体概况,部分产品、服务的内容可能有所调整。您所 购买的腾讯云产品、服务的种类、服务标准等应由您与腾讯云之间的商业合同约定,除非双方另有约定,否则,腾讯 云对本文档内容不做任何明示或模式的承诺或保证。



# 文档目录

操作指南

域名型证书申请流程

域名验证指引

自动诊断结果查看指引

域名身份如何自动验证

部署证书到负载均衡指引

私钥密码指引

证书安装指引

域名型证书吊销指引

苹果ATS特性服务器配置指南

安全签章指引



# 操作指南 域名型证书申请流程

最近更新时间:2018-05-28 18:06:09

# 申请域名型(DV)SSL证书

# 1. 申请入口

### 进入SSL证书管理控制台

								_
云产品 ヘ 🔅					間間□ ~	帮助 ∨	工单	6
云计算与网络	存储与CDN	数据库	安全服务	监控与管理		<b>找名服务</b>		
① 云服务器	色 对象存储服务	🖯 云数据库	晶 主机与网站安全	\$\$ 云监控		🖻 域名管理		
- 提 负载均衡	🛱 CDN		① 大禹网络安全	🖾 云拨测		鸣 云解析		
合 私有网络		🖯 云数据库MongoDB	⑦ 天御业务安全防护	₽ 云API密钥		🗈 域名备案		
202 弹性伸缩		🗔 云缓存Memcached	🖤 应用乐固	む 蓝鲸平台	L L	🖪 SSL证书管理		
		印 云数据库HBase	👌 云安全	29 用户与权限				
		📾 分布式云数据库						
		数据处理与AI	开发者工具					
▶ 点播	@ 短信	Q 云搜	🖺 操作日志					
▶直播	[] 云通信	@ 文智	◎ 云服务账号					
□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□	🔂 手游兼容性测试	⑦ 机智机器学习	🔓 移动开发工具					
□ 微视频		△ 万象优图						
		[] 人脸识别						



# 单击【申请证书】

於 勝讯云 总览	云产品~					帮助 ~   工单	C <mark>2</mark>   9
SSL证书管理	证书列表						
	证书申请成功之后可以直接下载到	刘本地					
证书管理	申请证书 上传证书						
	ID	域名	证书类型	到期时间	状态	操作	
	0 <mark>f02a3aa</mark> 上传证书	ım	GeoTrust DV SSL CA - G3(1 年)	2017-09-08 07:59:59	已颁发	下载详情	
	4fbe68cf 未命名		GeoTrust DV SSL CA - G3(1 年)		申请中	删除详情	
	9b3cd9c2 未命名	m	GeoTrust DV SSL CA - G3(1 年)		审核失败	删除详情	
	0ea81d44 未命名	om	GeoTrust DV SSL CA - G3(1 年)		审核失败	删除详情	
	0e5fb41e test	m	GeoTrust DV SSL CA - G3(1 年)	2017-06-16 07:59:59	已颁发	下载 详情	
	0e34231d 未命名	<b>v</b>	GeoTrust DV SSL CA - G3(1 年)		申请中	删除 详情	
	fa4dd82f Iala	v	GeoTrust DV SSL CA - G3(1 年)	2017-06-16 07:59:59	已颁发	下载详情	
	共7项				每页显示	行 20▼ K <	1/1 > >

# 查看申请域名型证书型号,单击【确定】

确认证书类型		×
	Symantec.	
	TrustAsia DV SSL证书	
	由赛门铁克(Symantec)顶级根证 书签发,亚洲诚信(TrustAsia)提 供技术支持,兼容支持所有浏览 器。保护用户与网站之前进行安 全数据传输,信息不被非法篡改 和窃取。价值1900元/年,腾讯 云用户可免费申请。	
	有效期1年	
	确定取消	



# 2. 填写申请

填写申请域名,例如qcloud.com, cloud.tencent.com, demo.test.qlcoud.com。

☆ 腾讯云 总覧	云产品 🗸 🏻 🔅			帮助 ~   工单	[2] (€
SSL证书管理	< 证书列表│	证书申请			
证书管理		1 免费证书申请	2)域名身份验证		
	绑定域名 *	www.qcloud.com			
	证书备注名	请输入证书备注名,不超过30个字			
	私钥密码	选辑,不填写则不设置私钥密码 目前 <mark>暂不支持密码找回</mark> 功能,若您忘记密码则素重新申请证书 下一步			

# 3.1 手动DNS验证方式

证书默认支持收到DNS验证,验证方法可查看详情。

於 時讯云 总宽	云 <u>추</u> 品 ∨ ☆	▼ 帮助 ▼ 工单 「 <sup>2</sup> ●
SSL证书管理	< 证书列表 │ 证书申请	
	(✔) 免费证书申请	(2) 域名身份验证
证书管理	$\widetilde{}$	<u> </u>
	<ul> <li>● 手动DNS验证</li> <li>需您手动为域名添加一条解析记录。 详细说明2</li> </ul>	
	上一步 确认申请	

# 3.2 选择自动DNS验证方式



如果所申请域名成功添加云解析平台,可以支持自动DNS验证,验证方法可查看详情。

於 購訊云 总览	云产品~ ◇	1 - 帮助 - 工单 - 2 - 3
SSL证书管理	< 证书列表│证书申请	
	→ 免费证书申请	2) 域名身份验证
证书管理		<u> </u>
	④ 自动DNS验证   您的域名已使用云解析服务,可自动添加DNS记录验证,无需您进行任何操作。 详细说明2   ⑤ 手动DNS验证   需您手动为域名添加一条解析记录。详细说明2   上一步   微认申请	

# 4.1 提交申请后验证身份

提交申请成功后弹窗提示如下,需要前往【证书详情页】获取CName记录添加解析:

温馨提示	×
您的申请已提交,请尽快添加DNS解析记录。	
<u> </u>	



获取CName记录如Tips中显示,需要尽快成功添加解析,方可通过CA机构审核:

於 購 訊 云	总览	云产品∨  {	¢ Point	帮助 ~	工单	2	Φ
SSL证书管理	«	< 返回列表 │	证书详情				
证书管理		您的申请信息已 > c201/	提交。请尽快添加DNS解析记录,扫描认证通过后即可颁布证书。请添加如下DNS记录:s96km <sup>201</sup> ************************************				
		> \$2010	, ., com				
		ID	5167f2c4				
		状态	申请中				
		证书类型	TrustAsia DV SSL CA - G5(1年)				
		绑定域名	g.com				
		提交时间	2016-09-11 16:31:59				

# 4.2 提交申请失败

如遇到下图所示弹窗,是提交域名未通过CA机构安全审核,具体原因参考安全审核失败原因。

温馨提示	×
抱歉,该域名未通过CA机构安全审查,无法申请域名型 证书。请尝试申请其他域名。查看安全审核详情	<u>1</u>
重新申请取消	



# 域名验证指引

最近更新时间:2018-07-26 15:51:43

申请域名型证书,可以通过以下方式验证域名的所有权:

# 1. 手动 DNS 验证

通过解析指定的 DNS 记录验证您的域名所有权,指定如 主机记录 -> TXT记录类型 -> 记录值 的解析格式。

例如为申请证书的域名 www.domain.com 添加一条记录类型为TXT的DNS记录 , www.domain.com –> TXT –> 201704262209564gw0...hj37i4xai8m7uii2a23l :

SSL证书管理    《	← 证书	详情								
证书管理										
	您的申请们	您的申请信息已提交。请尽快添加DNS解析记录,扫描认证通过后即可颁布证书。								
	基本信息	L								
	ID	MJNdgq5S								
	状态	待DNS验证								
		请添加如下解析记录	操作指引							
		域名	主机记录	记录类型	记录值					
		m	_dnsauth	ТХТ	201807241 5n3a0w9ekk2783cjk8ix7odopx7wfowpd2vvitsnyv7xhm					
		自助诊断查询								
	证书类型	TrustAsia TLS RSA CA	(1年)							
	通用名称	www.	com							
	提交时间	2018-07-25 18:15:35								

以腾讯云云解析平台为例说明如何进行操作:

#### 1.1 添加域名

单击【添加解析】,在弹窗内输入您要解析域名的主域名 domain.com,并点【确定】



域名服务《	我的域名	全部项目 ▼					品 手机管理域名	a 🗧 🗧 返回旧#	版 🔲 指引
我的域名	全部域名	未实名认证	DNS未修改	未备案					
域名信息模板									
域名转入	【重要通知】 1、请尽快完	 	『存量域名(包括2017年	年7月18日之前注册/转	入的域名)未通过实名将	被注册局暂停解析	, 网站/邮箱无法访问!	查看详情	
解析套察管理	2、仕中国ス 3、根据《关 情形 法形	[吨地区开展网站服务] [于建立境内违法互联网 时联系工作部队理 _ 避	,请先将或名进行奋柔 列站黑名单管理制度的 岳被影响 <b>了解再</b> 多	8。开始音繁 的通知》要求,域名解析	服务提供商将停止为黑	黑名单域名提供解析	, 建议您前往黑名单网	刚站查询页进行自检	,如存在上述
协作子域名	4、系统已于	2018年2月1日10:00	陆续删除域名列表里的	尚未注册的域名,建议	您先注册域名再添加解	析,上述操作对已》	主册域名的解析业务没	有任何影响,请知暇	8。立即注册
	云服务器、 注册域名	云数据库等热门产品3 添加解析 购3	fi起,服务更稳,速度 <b>厌解析赛餐</b> 批量	程更快,价格更优。立即 接作  ▼	196月9日	请	▲入您要搜索的域名 ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓	Q 全部域名 新	○ 時用表注册域名

#### 1.2 添加解析记录

域名添加完成后,单击右侧的【解析】进入域名解析页面。

域名服务《	我的域名	全部项目 ▼				品手机管理域名	⇒ 返回旧版 🔲	指引
我的域名	全部域名	未实名认证	DNS未修改	未备案				
域名信息模板								
域名转入	<ul> <li>【里要週知】</li> <li>1、请尽快完</li> <li>2 在中国士</li> </ul>	;成域名实名认证,全部 注地区开展网站距冬	存量域名(包括2017年 法生物域名进行条束	7月18日之前注册/转入的域名)未通过	过实名将被注册局暂停前	解析,网站/邮箱无法访问!	查看详情	
解析套餐管理	2、在中国へ 3、根据《关 述情形,语初	,西西区川展网络服务, 于建立境内违法互联网 及时联系工信部处理,通	情光将爆石运行菌菜。  站黑名单管理制度的過 醫免被影响。了解更多	7月1日美 19日》要求,域名解析服务提供商将	停止为黑名单域名提供第	解析,建议您前往黑名单网络	皆查询页进行自检,如存在」	F
协作子域名	4、系统已于 册	2018年2月1日10:00	陆续删除域名列表里尚	未注册的域名,建议您先注册域名甲	再添加解析,上述操作对	把注册域名的解析业务没有	;任何影响,请知晓。立即注	E
	云服务器、艺	员数据库等热门产品3折	起,服务更稳,速度更	包快,价格更优。立即抢购				
								Ŷ
	注册域名	添加解析	(解析套餐 批量描	ére ≖	请	輸入您要搜索的域名 Q	全部域名 腾讯云注	
		域名	服务状态()	解析状态 ()	备案()	到期时间 🛊 操作		
	免	3	-	域名 DNS 未修改()	未备案	- 解析	管理 更多 ▼	

单击【添加记录】



域名服务《	← bowang	gedu.com	全部项目 ▼						品 手机管	理域名
我的城名 城名信息模板 城名转入	域名信息 注意:在中国7	<b>域名解析</b>	服务,请先将域领	名进行备案,否则将无 2d pat <b>ls</b> fig1ps2 dps	法正常访问。开始智	滨 <u>Ľ</u>				×
解析套餐管理	修改DNS服务器 遇到问题?查君	器需要最长72个小 FAQ文档 ☑	时的全球生效时	间,请耐心等待。						
1271日丁364日	记录管理	负载均衡   解	析量统计   均	城名设置   自定义	线路   线路分组					
	添加记录	新手快速添加	暂停	开启删除	分配至项目			请输入您	要搜索的记录	$\odot$
	主机证	禄	录类型 ▼	线路类型	记录值	MX优先级	TTL(秒)	最后操作时间	操作	
	www	A		默认		-	600	2018-07-26 10:32:30	修改 暫停 删除	

#### 1.3 完成指定的 TXT 记录添加

TXT 记录是对域名进行标识和说明的一种方式:

- 记录类型选择为 TXT
- 主机记录根据证书详情填入,如:\_\_dnsauth
- 线路类型选择默认
- 记录值为系统提供的文本内容,此处为 201712270743...t5bfctnq ,注意记录值须完整填写
- TTL选择默认值 600 秒即可



域名服务 《	← bowangedu.co	m 全部项目 ▼					品手机管	き理域名
我的域名	域名信息 域名解析	ĥ						
域名信息模板								
城名转入	注意:在中国大陆地区开 请到域名注册商处将DNS	展网站服务,请先将域名进 修改为:f1g1ns1.dnspod.r	挂行备案,否则将无法正常访问。升 net <mark>Ⅰ</mark> f1g1ns2.dnspod.net <b>Ⅰ</b>	始备案 🖸				×
解析套察管理	修改DNS服务器需要最长 遇到问题?查看FAQ文档	72个小时的全球生效时间, 【	, 请耐心等待。					
协作子域名								
	记录管理 负载均衡	解析量统计 域名	设置 自定义线路 线路分	迓组				
	添加记录新手快	速添加 暂停 引	开启 删除 分配至项目			请输入您要	搜索的记录	Q,
	主机记录	记录类型 ▼      纟	线路类型 记录值	MX优先级	TTL (秒)	最后操作时间	操作	
	按如下提	A	<b>默认</b> 按如下提:	-	600	-	保存目	取消
	提示 要解析 www.too	■ lu.com,请填写 www。 解析后的域名为 www.	主机记录就是域名前缀,常见用法	5有:				
	@	直接解析主域名	.com					
	*	泛解析,匹配其他所有均	域名 *					
	mail	将域名解析为 mail.L	com,通常用于解析邮箱	服务器				
	二级域名	如:abc1.co	om,填写abc					
	手机网站	如:m.t	n,填写m					
	WWW	A I	默认		600	2018-07-26 10:32:30	修改 暫停 删除	
	共1项				每页显示行	20 -	1/1 👻 🕨	H

#### 解析添加成功后如下:

域名服务。	← bowangedu.	<b>:om</b> 全部项目	•					品手机管	管理域名
我的域名	域名信息 域名角	¥析							
域名信息模板									
域名转入	注意:在中国大陆地区 请到域名注册商处将DI	廾展网站服务,请先将 №修改为:f1g1ns1.dn	域名进行备案,合则 spod.net <mark>而</mark> f1g1ns2	」将无法止常访问。开始 dnspod.net <b>后</b>	諸葉 12				×
解析賽餐管理	修改DNS服务器需要最 遇到问题?查看FAQ文	长72个小时的全球生刻 档 🖸	(时间,请耐心等待。						
协作子域名									
	□ · · · · · · · · · · · · · · · · · · ·	新 解析量统计	域名设置 自	定义线路 🔰 线路分组	1				-9
	※ 하기크 호텔						注於 \ 你	亜肉志がつき	0
	12000年 新子	"快速除加 首行		际历史现日			<b>「</b>	安诺奈的旧家	ų
	主机记录	记录类型 ▼	线路类型	记录值	MX优先级	TTL(秒)	最后操作时间	操作	
	www	A	默认	177 T. S.	-	600	2018-07-26 10:32:30	修改 暫停 删除	

www.domain.com TXT 记录值的系统会定时检查,若能检测到并且与指定的值匹配,即可完成域名所有权验证。



# 2. 自动DNS验证

#### 注: 仅限使用云解析的域名

如果申请证书的域名已经在云解析平台进行解析,可以选择自动验证。

系统为将为该域名自动添加指定的DNS解析记录,记录被检测匹配成功,完成域名所有权验证后,该记录将自动清除。

#### 3. 文件验证

#### 3.1 指定目录下创建文件

按指定文件目录、文件名、文件内容新增文件,例如

文件目录	文件名	文件内容
/.well- known/pki- validation	fileauth.txt	201608241742072yvt8bxp9jv0ycginrnnebwgy1nvwgvxtssucy39w7b20nelfa

如果申请文件验证的域名是 example.www.domain.com ,那么进行验证访问的链接地址是 http://example.www.domain.com/.well-known/pki-validation/fileauth.txt 或者 https://example.www.domain.com/.well-known/pki-validation/fileauth.txt

对于 www 开头的二级域名,如: www.domain.com ,在对该域名本身添加文件验证信息之外,还需增加对 其主域名 domain.com 的文件验证,验证值与验证方法与该二级域名文件验证相同。

如果申请文件验证的域名是泛域名 \*.domain.com ,那么进行验证访问的链接地址是 http://domain.com/.wellknown/pki-validation/fileauth.txt 或者 https://domain.com/.well-known/pki-validation/fileauth.txt

访问链接可获取到内容为 201608241742072yvt8bxp9jv0ycginrnnebwgy1nvwgvxtssucy39w7b20nelfa。

http 和 https 访问支持任意一个均可 ; 文件验证不支持任何形式的跳转 , 需要直接响应 200 状态码和文件内容。

#### 3.2 等待审核

建立完成文件后,请耐心等待 CA 机构扫描审核。证书颁发完成后,文件和目录即可清除。



#### 3.3 Window 系统不支持创建/.well-known 目录问题

在 Windows 下无法通过 右键=>新建 命令来创建以点开头的文件和文件夹 , 例如 .log , 会提示必须输入文件名。可以通过命令行来创建 :

新建文件夹

mkdir .well-known



# 自动诊断结果查看指引

最近更新时间:2018-09-17 15:33:23

选择了手动 DNS 验证方式没有通过审核时,可以通过自助诊断排查问题:

### 1. 检查域名状态是否正常

请先确定域名可以正常解析。例如域名未实名认证时、域名刚刚购买入手时,都存在无法正常解析的情况。

#### 2. 检查 DNS 服务器

请先确认在正确的解析服务商处添加了解析。例如, DNS 服务器为万网的服务器, 则在腾讯云云解析添加了 TXT 解析 是无法生效的。

#### 3. 检查解析记录

如果域名解析正常、也在正确的解析服务商处添加了解析,仍然没有审核通过,很可能是主机记录、记录值等输入时发生手误。请确认 TXT 记录已经完整无误添加,耐心等待 24 个小时。

如果超过 24 个小时仍未审核通过,可以提交工单联系腾讯云工程师协助您处理。



# 域名身份如何自动验证

最近更新时间:2018-01-16 17:24:44

#### 1. 自动DNS验证原理

提交证书申请后,CA机构会指定添加一条CNAME解析记录来验证域名的所有权,如果该域名在腾讯云云解析平台进行解析,则可以立即自动添加指定的CNAME解析记录,等待CA机构的定时扫描审核,以最快最便捷的方式完成证书申请。

#### 2. 云解析添加域名

如果您的域名不在云解析平台进行解析,可以参考如下流程将域名加入云解析: 添加域名到云解析

#### 3. 修改DNS服务器

切记,完成添加域名后,需要修改域名的DNS服务器为腾讯云指定的DNS地址,解析方可生效。 参考修改域名DNS指引

# 部署证书到负载均衡指引

最近更新时间:2018-01-16 17:25:39

SSL证书支持部署到负载均衡,步骤如下所示:

# 1. 选择证书

首先成功申请获取证书(参考如何免费申请域名型证书),或者选择上传的证书,展开【更多】操作,选择【部署到 负载均衡】。

於 購 訊 点 意 意	云产品 ~   CDN   贷					qcloud $\checkmark$	帮助 〜	工单	⊂ <mark>155</mark>	Φ
SSL证书管理	证书列表									
	证书申请成功之后可以直接下载到:	本地								
证书管理	申请证书 上传证书									
	ID	域名	证书类型	到期时间	状态		操作			
	ca861922 未命名	m	GeoTrust DV SSL CA - G3(1 年)	2017-10-12 07:59:59	已颁发		下载	详情 更 野到命載均	<u>多 へ</u> 御	^
	c915db06 未命名		GeoTrust DV SSL CA - G3(1 年)	2017-10-12 07:59:59	已颁发		下载	详情 更	多 >	
	f9a1569b test	Jm	TrustAsia DV SSL CA - G5(1 年)		审核失败		删除	详情		
	<b>b57e1306</b> 未命名		TrustAsia DV SSL CA - G5(1 年)	2017-09-22 07:59:59	上传托管		下载	删除 详情	更多~	
	dfff103d Ialalal		TrustAsia DV SSL CA - G5(1 年)		审核失败		删除	详情		
	7bb4fc1b Highwinds-Ping	m	TrustAsia DV SSL CA - G5(1 年)	2017-09-14 07:59:59	已颁发		下载	详情 更	多∨	
	f0830dbf 擼哥的证书	, i	clue test(10年)	2026-08-23 22:58:44	上传托管		下载	删除 详情	●更多~	
	f072fbed clue的证书	n	clue test(10年)	2026-08-23 22:58:44	上传托管		下载	删除 详情	更多∨	
	e6654916	- F	GeoTrust DV SSL CA - G3(1	2017 00 26 07 50 50	TATUS			**** -	æ	•
	共16项					每页显示行	20 🔻	К <	1/1 >	К

2. 选择LB实例



根据项目和地区筛选LB实例(目前不支持华南地区-深圳金融),且只能选择一个实例。

# 部署到负载均衡

X

证书ID:	BB73J	GnP(TestKMS	)						
证书类型:	ca1								
选中LB实例:	默认工	项目 🗸	华南地区(	「广州)	~		可輸入	VIP或云主机内网IP搜索	Q
		ID	华南地区(	(广州)	<b>^</b>	VIP		所属网络	
	$\bigcirc$	lb-61s3opol	华南地区 ( 华东地区 (	(深圳金融…) (上海) 。(hr	-{hη)	111.230.79.206		vpc-k8aux2cr	<b>^</b>
	0	lb-myaluvfl	华东地区( <u>化北地区(</u>	上海金融  北京	+	111.230.79.110		vpc-k8aux2cr	
	0	lb-hnxm3six		melody1		111.230.78.221		vpc-l12bfw9t	
		lb-9wz8syx5		ccs_cls-4i10	qeho8_hell	111.230.4.176		vpc-a2hcwbl5	
	0	lb-gc9grq4j		59ed9d08-(	D	111.230.79.106		vpc-mnd20y33	
		lb-cbgrrgi3		59e2e9d2-(	D	111.230.75.187		vpc-mnd20y33	
	~ 共1	14 项				每页显示行 20	) -	< < 1/1 >	К
				确定	1 取消	ä			

#### 3. 创建监听器

跳转到负载均衡控制台,打开创建监听器弹窗,并且监听协议端口已切换到Https,服务器证书为已选中的证书,然后 完成剩余的基本配置。



於 勝讯云 总宽	云产品 ~   CDN   贷		qcloud ~   帮助 ~   工单   〜 <mark>155</mark>   ④
负载均衡 《	< 返回   24b536-0		
		创建监听器 ×	
LB 实例列表	基本信息 监听器监		
证书管理		1     基本配置     2     高級配置     3     健康检查	
	基本信息		
	名称 24b536-0 🖌	名称	
	ID Ib-7m3bjj9n	监听协议端口 HTTPS v :	
		后端端口	
	所属网络基础网络	SSL解析方式 単同从並(推荐) / 计描述/IC 2 注意:如果用户访问您的Web服务时,您需要对用户做身份验证,您可以选择SSL双向	
	域名 24b536-0.gz.1251	认证	
	VIP 119.29.49.192	服务器证书 ③ 选择已有 ○ 新建	
	创建时间 2016-10-10 15:12	未命名/ca861922 >	
	监听器 + 新建	当选用HTTPS监听转发封,客户读到负载均衡的访问,使用HTTPS协议进行加密。 X 负载均衡到后端云服务器的转发为HTTP协议。负载均衡器代理了SSL加解密的开销,并保证WEB访问 安全。	
	监听器名称	取消 下一步	<b>操作</b>

# 4. 继续完成配置

继续完成创建监听器的其他配置,即可实现负载均衡的Https。



# 私钥密码指引

最近更新时间:2018-01-16 17:29:07

私钥密码是申请证书时的选填项,如图所示:

SSL证书管理	< 证书列表│证书申请	
	1 免费证书申请	
<b>祉</b> 书管理		
	绑定域名 * www.domain.com 📿	
	证书备注名 — 个DV证书 🛇	
	私钥密码         ••••••           目前 暂不支持密码找回 功能,若您忘记密码则需重新申请证书	
	确认密码 ••••••	
	下一步	

#### 注意事项:

- 1、如果填写了私钥密码,请您牢记该密码,该密码不支持找回和修改;
- 2、该密码在证书下载完成进行解压时需要输入;
- 3、在您的服务器上进行证书导入、导出、安装等操作时可能会需要输入;
- 4、如果私钥密码不慎遗忘,请工单联系腾讯云工程师删除该证书,然后重新申请该域名证书。



# 证书安装指引

最近更新时间:2018-08-16 09:52:12

下载得到的 www.domain.com.zip 文件,解压获得3个文件夹,分别是Apache、IIS、Nginx 服务器的证书文件,下面提供了4类服务器证书安装方法的示例:

### 1. Apache 2.x 证书部署

#### 1.1 获取证书

Apache文件夹内获得证书文件 1\_root\_bundle.crt, 2\_www.domain.com\_cert.crt 和私钥文件

3\_www.domain.com.key,

1 root bundle.crt 文件包括一段证书代码 "-----BEGIN CERTIFICATE-----"和"-----END CERTIFICATE-----",

2\_www.domain.com\_cert.crt 文件包括一段证书代码 "-----BEGIN CERTIFICATE-----"和"-----END CERTIFICATE------",

3\_www.domain.com.key 文件包括一段私钥代码"-----BEGIN RSA PRIVATE KEY-----"和"-----END RSA PRIVATE KEY-----"。

#### 1.2 证书安装

编辑Apache根目录下 conf/httpd.conf 文件,

找到 #LoadModule ssl\_module modules/mod\_ssl.so 和 #Include conf/extra/httpd-ssl.conf , 去掉前面 的 # 号注释 ;

编辑Apache根目录下 conf/extra/httpd-ssl.conf 文件,修改如下内容:

#### <VirtualHost 0.0.0:443>

DocumentRoot "/var/www/html" ServerName www.domain.com SSLEngine on SSLCertificateFile /usr/local/apache/conf/2\_www.domain.com\_cert.crt SSLCertificateKeyFile /usr/local/apache/conf/3\_www.domain.com.key SSLCertificateChainFile /usr/local/apache/conf/1\_root\_bundle.crt </VirtualHost>

配置完成后,重新启动 Apache 就可以使用 https://www.domain.com 来访问了。

注:

配置文件参数	说明
SSLEngine on	启用SSL功能
SSLCertificateFile	证书文件



配置文件参数	说明
SSLCertificateKeyFile	私钥文件
SSLCertificateChainFile	证书链文件

# 2. Nginx 证书部署

#### 2.1 获取证书

Nginx文件夹内获得SSL证书文件 1\_www.domain.com\_bundle.crt 和私钥文件 2\_www.domain.com.key, 1\_www.domain.com\_bundle.crt 文件包括两段证书代码 "-----BEGIN CERTIFICATE-----"和"-----END CERTIFICATE-----", 2\_www.domain.com.key 文件包括一段私钥代码"-----BEGIN RSA PRIVATE KEY-----"和"-----END RSA PRIVATE

KEY-----"。

#### 2.2 证书安装

将域名 www.domain.com 的证书文件1\_www.domain.com\_bundle.crt 、私钥文件2\_www.domain.com.key保存到 同一个目录 , 例如/usr/local/nginx/conf目录下。 更新Nginx根目录下 conf/nginx.conf 文件如下 :

```
server {
listen 443;
server_name www.domain.com; #填写绑定证书的域名
ssl on;
ssl_certificate 1_www.domain.com_bundle.crt;
ssl_certificate 1_key 2_www.domain.com.key;
ssl_session_timeout 5m;
ssl_protocols TLSv1 TLSv1.1 TLSv1.2; #按照这个协议配置
ssl_protocols TLSv1 TLSv1.1 TLSv1.2; #按照这个协议配置
ssl_ciphers ECDHE-RSA-AES128-GCM-SHA256:HIGH:!aNULL:!MD5:!RC4:!DHE;#按照这个套件配置
ssl_prefer_server_ciphers on;
location / {
root html; #站点目录
index index.html index.htm;
}
```

配置完成后,先用 bin/nginx -t 来测试下配置是否有误,正确无误的话,重启nginx。就可以使用 https://www.domain.com 来访问了。

注:

配置文件参数

说明



配置文件参数	说明
listen 443	SSL访问端口号为443
ssl on	启用SSL功能
ssl_certificate	证书文件
ssl_certificate_key	私钥文件
ssl_protocols	使用的协议
ssl_ciphers	配置加密套件,写法遵循openssl标准

#### 2.3 使用全站加密,http自动跳转https(可选)

对于用户不知道网站可以进行https访问的情况下,让服务器自动把http的请求重定向到https。 在服务器这边的话配置的话,可以在页面里加js脚本,也可以在后端程序里写重定向,当然也可以在web服务器来实现 跳转。Nginx是支持rewrite的(只要在编译的时候没有去掉pcre) 在http的server里增加 rewrite ^(.\*) https://\$host\$1 permanent; 这样就可以实现80进来的请求,重定向为https了。

### 3. IIS 证书部署

#### 3.1 获取证书

IIS文件夹内获得SSL证书文件 www.domain.com.pfx。

#### 3.2 证书安装



1、打开IIS服务管理器,单击计算机名称,双击'服务器证书'





# 2、双击打开服务器证书后,单击右则的导入

<ul> <li>             ・ 10.104_179_163              </li> <li>             文件① 视图() 帮助(L)             </li> </ul> を決していたいでは、                のとの                  を決していたいたいたいたいたいたいたいたいたいたいたいたいたいたいたいたいたいたいた	<b>9</b> ]	Internet Information	Services (IIS)管理器	_ 0 ×
文件①       视图()       帮助()         连接        服务器证书         ● 起始页       使用此功能来申请和管理 Web 服务器可以对配置了 SSL 的网站       创建证书申请         ● 盈 网站       ● ⑦ Default Web Site       ● 派 ① ① ① ①         ● ③ Default Web Site       ● 派 ① ① ② ○       ● 创建如证书         ● ③ Default Web Site       ● ③ Default Web Site       ● ③ ① ① ②         ● ③ Default Web Site       ● ③ ② ① ③       ● ③ ② ● ③ ○         ● ③ Default Web Site       ● ③ ③ ● ③ ○       ● ③ ◎ ● ③         ● ③ Default Web Site       ● ③ ◎ ● ⑤ ○       ● ③ ◎ ● ⑤ ○         ● ③ Default Web Site       ● ③ ● ⑤ ○       ● ③ ● ⑤ ○       ● ③ ● ⑤ ○         ● ③ ● ○       ● ⑤ ○       ● ⑤ ○       ● ◎ ◎ ● ◎ ○         ● ◎ ● ○       ● ◎ ● ○       ● ◎ ● ◎ ○       ● ◎ ● ◎ ● ◎         ● ◎ ● ○       ● ◎ ● ○       ● ◎ ● ◎ ● ○       ● ◎ ● ◎ ● ◎         ● ● ○       ● ○       ● ◎ ● ○       ● ◎ ● ○       ● ○         ● ● ● ○       ● ○       ● ○       ● ◎ ● ○       ● ○       ● ○         ● ● ●       ● ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●	€ 10_104_179_163	•		🖸 📉 🟠 🕡 🗸
连接     服务器证书       ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●	文件(E) 视图(V) 帮助(H)			
>         UEII - VJBET/UEI         UEII - VJBET/UEII         UEII - VJBET/UEI         UEII - VJBET/UEI         UEII - VJBET/UEII         UEII - VJBET/UEII         UEII - VJBET/UEI         UEII - VJBET/UEII         UEII - VJBET/UEIII         UEIII - VJBET/UEIII <td< td=""><td>连接 ● ● 記始页 ▲ ● ● © 应用程序池 ▲ • ● ◎ 网站 ▷ • ● ● ● Default Web Site</td><td>服务器证书           使用此功能来申请和管理 Web 服使用的证书。                筛选:                  ශා选:                  ダネ                  パンC</td><td>客器可以对配置了 SSL 的网站 开始(G) ・ 反分 WMSvc- &gt;</td><td>操作 导入 创建证书申请 完成证书申请 创建域证书 创建自签名证书 允许自动重新绑定续订的证书 ⑦ 帮助</td></td<>	连接 ● ● 記始页 ▲ ● ● © 应用程序池 ▲ • ● ◎ 网站 ▷ • ● ● ● Default Web Site	服务器证书           使用此功能来申请和管理 Web 服使用的证书。                筛选:                  ශා选:                  ダネ                  パンC	客器可以对配置了 SSL 的网站 开始(G) ・ 反分 WMSvc- >	操作 导入 创建证书申请 完成证书申请 创建域证书 创建自签名证书 允许自动重新绑定续订的证书 ⑦ 帮助
	( ) ) ) ) ) ) ) ) ) ) ) ) ) ) ) ) ) ) )			€ <u></u>

3、选择证书文件,如果输入申请证书时有填写私钥密码需要输入密码,否则输入文件夹中密码文件keystorePass.txt的密码内容,单击确定。参考私钥密码指引



导入证书 ? ×
证书文件(.pfx)( <u>C</u> ):
\dministrator\Desktop\www.incom.pfx
密码(D):
选择证书存储( <u>S</u> ):
☆人 v
✓ 允许导出此证书(A)
确定 取消



#### 4、单击网站下的站点名称,单击右则的绑定





### 5、打开网站绑定界面后,单击添加

				网站绑定		? ×
[	类型	主机名	端口	IP 地址	绑定信息	添加( <u>A</u> )
	http net.msmq msmq.form net.tcp		80	*	localhost localhost 808:*	编辑(E) 删除(R)
	net.pipe				*	浏览( <u>B</u> )
					,	关闭( <u>C</u> )

# 6、添加网站绑定内容:选择类型为https,端口443和指定对应的SSL证书,单击确定

	添加网站绑定		? X
类型①: https    ✓	IP 地址(]): 全部未分配	端口( <u>O</u> ): ✓ 443	
主机名(出):	下(N)		
SSL 证书(E):			
www.zg.co	m v	选择( <u>L</u> )	查看(⊻)
	<b>₽</b>	确定	取消



#### 7、添加完成后,网站绑定界面将会看到刚刚添加的内容

			网站绑定	ł	? X
类型 http net.msmq msmq.form net.tcp net.pipe https	主机名	端口 80 443	IP 地址 *	绑定信息 localhost localhost 808:* *	<b>添加(A)…</b> 編辑(E)… 删除(R) 浏览(B)
					关闭( <u>C</u> )

#### 4. Tomcat 证书部署

#### 4.1 获取证书

如果申请证书时有填写私钥密码,下载可获得Tomcat文件夹,其中有密钥库 www.domain.com.jks;

如果没有填写私钥密码,证书下载包的Tomcat文件夹中包括密钥库文件www.domain.com.jks 与密钥库密码文件 keystorePass.txt

当用户选择粘贴CSR时,不提供Tomcat证书文件的下载,需要用户手动转换格式生成,操作方法如下:

可以通过 Nginx 文件夹内证书文件和私钥文件生成jks格式证书 转换工具:https://www.trustasia.com/tools/cert-converter.htm 使用工具时注意填写 **密钥库密码**,安装证书时配置文件中需要填写。

#### 4.2 证书安装

配置SSL连接器,将 www.domain.com.jks 文件存放到conf目录下,然后配置同目录下的 server.xml 文件:

```
<Connector port="443" protocol="HTTP/1.1" SSLEnabled="true"
maxThreads="150" scheme="https" secure="true"
```



keystoreFile="conf/www.domain.com.jks"
keystorePass="changeit"
clientAuth="false" sslProtocol="TLS" />

#### 注:

配置文件参数	说明
clientAuth	如果设为true , 表示Tomcat要求所有的SSL客户出示安全证书 , 对SSL客户进行身份验证
keystoreFile	指定keystore文件的存放位置,可以指定绝对路径,也可以指定相对于(Tomcat安装目录)环 境变量的相对路径。如果此项没有设定,默认情况下,Tomcat将从当前操作系统用户的用户目 录下读取名为 ".keystore"的文件。
keystorePass	密钥库密码,指定keystore的密码。(如果申请证书时有填写私钥密码,密钥库密码即私钥密 码,否则填写密钥库密码文件中的密码)
sslProtocol	指定套接字(Socket)使用的加密/解密协议,默认值为TLS

#### 4.3 http自动跳转https的安全配置

到conf目录下的web.xml。在 </welcome-file-list> 后面 , </web-app> ,也就是倒数第二段里 ,加上这样一段

```
<login-config>
<I-- Authorization setting for SSL --->
<auth-method>CLIENT-CERT</auth-method>
<realm-name>Client Cert Users-only Area</realm-name></login-config>
<security-constraint>
<I-- Authorization setting for SSL --->
<web-resource-collection>
<web-resource-name>SSL</web-resource-name>
<url-pattern>/*</url-pattern>
</web-resource-collection>
<user-data-constraint>
</user-data-constraint>
```

这步目的是让非ssl的connector跳转到ssl的connector去。所以还需要前往server.xml进行配置:

```
<Connector port="8080" protocol="HTTP/1.1"
connectionTimeout="20000"
redirectPort="443" />
```

redirectPort改成ssl的connector的端口443,重启后便会生效。



# 域名型证书吊销指引

最近更新时间:2018-01-16 17:32:14

# 1. 提交工单

提交工单寻求腾讯云工程师协助您完成证书吊销。

### 2. 提供相关信息

提供证书信息:包括证书ID、域名、证书序列号。

### 3. 证书序列号获取方法

#### 3.1 下载证书到本地,双击打开



3.2 切换到【详细信息】,获取证书序列号



证书	×
常规 详细信息 证书路径	
显示 (2): 〈所有〉	<b></b>
字段	值
□□版本	V3 =
<ul> <li>序列号</li> <li>● 签名算法</li> <li>● 签名哈希算法</li> <li>● 颁发者</li> <li>● 有效期从</li> <li>● 到</li> <li>1f 59 ba d2 17 fe 79 db 28</li> </ul>	If 59 ba d2 17 fe 79 db sha256RSA sha256 TrustAsia DV SSL CA - G 2016年9月26日 8:00:00 2017年9月27日 7:59:59 ▼
」 了解 <u>证书详细信息</u> 的更多信息	歸歸属性 健) <b>复制到文件 ℃)</b> ]
	确定

# 4. 重新验证域名身份

腾讯云工程师会要求您完成相应的DNS验证或者文件验证,完成身份验证后,CA机构方可继续完成证书吊销流程。



# 苹果ATS特性服务器配置指南

最近更新时间:2018-05-28 18:16:28

#### 配置指南:

 需要配置符合PFS规范的加密套餐,目前推荐配置: ECDHE-RSA-AES128-GCM-SHA256:ECDHE:ECDH:AES:HIGH:!NULL:!aNULL:!MD5:!ADH:!RC4
 需要在服务端TLS协议中启用TLS1.2,目前推荐配置:

TLSv1 TLSv1.1 TLSv1.2

# 1.Nginx 证书配置

更新Nginx根目录下 conf/nginx.conf 文件如下:

```
server {
```

```
ssl_ciphers ECDHE-RSA-AES128-GCM-SHA256:ECDHE:ECDH:AES:HIGH:!NULL:!MD5:!ADH:!RC4;
ssl_protocols TLSv1 TLSv1.1 TLSv1.2;
```

}

# 2.Apache 证书配置

更新Apache根目录下 conf/httpd.conf 文件如下:

```
<IfModule mod_ssl.c>
<VirtualHost *:443>
SSLProtocol TLSv1 TLSv1.1 TLSv1.2
SSLCipherSuite ECDHE-RSA-AES128-GCM-SHA256:ECDHE:ECDH:AES:HIGH:!NULL:!MD5:!ADH:!RC
4
</VirtualHost>
</IfModule>
```

### 3.Tomcat 证书配置

更新 %TOMCAT\_HOME%\conf\server.xml 文件如下:

```
<Connector port="443" protocol="HTTP/1.1" SSLEnabled="true"
scheme="https" secure="true"
SSLProtocol="TLSv1+TLSv1.1+TLSv1.2"
SSLCipherSuite="ECDHE-RSA-AES128-GCM-SHA256:ECDHE:ECDH:AES:HIGH:!NULL:!MD5:!ADH:!
RC4" />
```

#### 4.IIS 证书配置



#### 4.1 方法一

Windows 2008及更早的版本不支持TLS1\_2协议 所以无法调整 2008R2 TLS1\_2协议默认是关闭的 需要启用此协议达 到ATS要求

以2008 R2为例,导入证书后没有对协议及套件做任何的调整。

证书导入后检测到套件是支持ATS需求的,但协议TLS1\_2没有被启用,ATS需要TLS1\_2的支持。可使用的ssltools工具 (亚洲诚信提供,单击下载)启用TLS1\_2协议

6	SSL Tools for IIS							x
	SSL Tools for IIS			扂	亞洲詞 TRU	:信 ST <mark>/</mark>	Ksia	
欢	迎 证书 安全 关于							
	安全协议 · 重启系统生效]							
#	协议							
1	SSL 2.0							
2	SSL 3.0							
3	TLS 1.0							
4	TLS 1.1 🔽							
5	5 TLS 1.2 🛛							
	如率存件,[[明时生态,司协步的图数优生纪]							
	加密各件「国動主衆、可把約崩進化元級」	合田	<b>主持执</b> 动	FIDE	六格	the star	r∆≫	
1		后刑	又付100以 11912			ЛШШШ AEC	4日4日 CUA 25C	Â
	TIS BSA WITH AES 128 CBC SHA	×	TIS12 TIS11 TIS10	正旦	BSA	AES	SHA1	
2	TLS_RSA_WITH_AES_120_000_51A		TIS12	是	BSA	AES	SHA256	Ξ
	TLS BSA WITH AES 256 CBC SHA		TLS 1.2. TLS 1.1. TLS 1.0	是	BSA	AES	SHA1	
5	TLS RSA WITH RC4 128 SHA	<b>V</b>	TLS 1.2, TLS 1.1, TLS 1.0, SSL 3.0	否	RSA	RC4	SHA1	
6	TLS_RSA_WITH_3DES_EDE_CBC_SHA	<b>V</b>	TLS 1.2, TLS 1.1, TLS 1.0, SSL 3.0	是	RSA	3DES	SHA1	
7	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256_P256	<b>V</b>	TLS 1.2	是	ECDH_P256	AES	SHA256	
8	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256_P384	<b>V</b>	TLS 1.2	是	ECDH_P384	AES	SHA256	
9	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P256	<b>V</b>	TLS 1.2, TLS 1.1, TLS 1.0	是	ECDH_P256	AES	SHA1	
1	D_TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P384	<b>V</b>	TLS 1.2, TLS 1.1, TLS 1.0	是	ECDH_P384	AES	SHA1	
1	1 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA_P256	1	TLS 1.2, TLS 1.1, TLS 1.0	是	ECDH_P256	AES	SHA1	
1	2 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA_P384	<b>V</b>	TLS 1.2, TLS 1.1, TLS 1.0	是	ECDH_P384	AES	SHA1	-
	DITIC ECHUE ECHON WITH NEC 100 COM CHADEC DOEC	12	TIC10	8	ECUN DORE	VEC	CUADEC	

勾选三个TLS协议并重启系统即可。

如果检查到PFS不支持,在加密套件中选中带ECDHE和DHE就可以了。

#### 4.2 方法二

开始——运行 输入regedit

找到HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols右 键->新建->项->新建TLS 1.1,TLS 1.2

TLS 1.1和TLS 1.2 右键->新建->项->新建Server, Client

在新建的Server和Client中都新建如下的项(DWORD 32位值), 总共4个



DisabledByDefault [Value = 0]

Enabled [Value = 1]

a 🐌 SSL 2.0	*	名称	类型	数据
Client	Г	ab)(默认)	REG_SZ	(数值未设置)
4 🌗 TLS 1.1		🕫 DisabledByDefault	REG_DWORD	0x00000000 (0)
Client		颵 Enable	REG_DWORD	0x0000001 (1)
Server				
4 · [] ILS 1.2				
	_	[		
⊿ - 🎽 SSL 2.0	^	名称	类型	数据
Client		ab](默认)	REG_SZ	(数值未设置)
A	-	🔀 DisabledByDefault	REG_DWORD	0x0000000 (0)
Client		👹 Enable	REG_DWORD	0x0000001 (1)
Server				
Client				
Server				
SSL 2.0	^	名称	类型	数据
<ul> <li>▲ - → SSL 2.0</li> <li>→ → Client</li> <li>↓ → ↓ S 1.1</li> </ul>	^	名称 •••) (默认)	类型 REG_SZ	数据 (数值未设置)
	*	名称 •••) (默认) எ DisabledByDefault	类型 REG_SZ REG_DWORD	数据 (数值未设置) 0x0000000 (0)
<ul> <li>→ SSL 2.0</li> <li>→ Client</li> <li>→ TLS 1.1</li> <li>→ Client</li> <li>→ Server</li> </ul>	Ŷ	名称 •••) (默认) 瓍 DisabledByDefault 瓍 Enable	<u>类型</u> REG_SZ REG_DWORD REG_DWORD	数据 (数值未设置) 0x00000000 (0) 0x0000001 (1)
	^	名称 •••• (默认) 1000 Disabled By Default 1000 Enable	类型 REG_SZ REG_DWORD REG_DWORD	数据 (数值未设置) 0x00000000 (0) 0x00000001 (1)
<ul> <li>▲</li></ul>	^	名称 •••) (默认) 1989 DisabledByDefault 1989 Enable	<u>类型</u> REG_SZ REG_DWORD REG_DWORD	数据 (数值未设置) 0x00000000 (0) 0x00000001 (1)
<ul> <li>SSL 2.0</li> <li>Client</li> <li>TLS 1.1</li> <li>Client</li> <li>Server</li> <li>TLS 1.2</li> <li>Client</li> <li>Server</li> </ul>	-	名称 動 (默认) 聰 DisabledByDefault 聰 Enable	类型 REG_SZ REG_DWORD REG_DWORD	数据 (数值未设置) 0x00000000 (0) 0x00000001 (1)
SSL 2.0  Client  Client  Client  Client  Client  Client  Server  Server  SSL 2.0  SSL 2.0	-	名称 (默认) 聞 DisabledByDefault 聞 Enable	类型 REG_SZ REG_DWORD REG_DWORD	数据 (数值未设置) 0x00000000 (0) 0x0000001 (1) 数据
<ul> <li>SSL 2.0</li> <li>Client</li> <li>TLS 1.1</li> <li>Client</li> <li>Server</li> <li>TLS 1.2</li> <li>Client</li> <li>Server</li> <li>Server</li> <li>Server</li> <li>Client</li> <li>Server</li> </ul>	^	名称 (默认) ) DisabledByDefault ) Enable 名称 (默认)	类型 REG_SZ REG_DWORD REG_DWORD	数据 (数值未设置) 0x00000000 (0) 0x0000001 (1) 数据 (数值未设置)
SSL 2.0     Client     Client     Client     Server     TLS 1.1     Client     Server     SsL 2.0     SsL 2.0     SsL 2.0     Client     SSL 2.0     Client     TLS 1.1	^	名称 (默认) 聞 DisabledByDefault 聞 Enable 名称 ④(默认) 聞 DisabledByDefault	業型 REG_SZ REG_DWORD REG_DWORD          業型         REG_SZ REG_DWORD	数据 (数值未设置) 0x00000000 (0) 0x0000001 (1) 数据 (数值未设置) 0x00000000 (0)
<ul> <li>SSL 2.0</li> <li>Client</li> <li>TLS 1.1</li> <li>Client</li> <li>Server</li> <li>TLS 1.2</li> <li>Client</li> <li>Server</li> <li>SSL 2.0</li> <li>SSL 2.0</li> <li>TLS 1.1</li> <li>Client</li> <li>TLS 1.1</li> <li>Client</li> <li>Client</li> <li>Client</li> <li>Client</li> </ul>		名称 (默认) 题 DisabledByDefault 题 Enable 名称 @ (默认) 题 DisabledByDefault 题 Enable	業型 REG_SZ REG_DWORD REG_DWORD 業型 REG_SZ REG_DWORD REG_DWORD	数据 (数值未设置) 0x00000000 (0) 0x0000001 (1) 数据 (数值未设置) 0x0000000 (0) 0x0000000 (1)
SSL 2.0     Client     Client     Client     Client     Server     Client     Server     SSL 2.0     Client     Server     SSL 2.0     Client     SSL 2.0     Client     Server     SSL 2.0     Client     Server	^ * *	名称 (默认) 聞 DisabledByDefault 聞 Enable 名称 (默认) 聞 DisabledByDefault 麗 Enable	業型 REG_SZ REG_DWORD REG_DWORD          業型         REG_SZ         REG_DWORD         REG_DWORD         REG_DWORD	数据 (数值未设置) 0x00000000 (0) 0x0000001 (1) 数据 (数值未设置) 0x00000000 (0) 0x00000000 (1)
<ul> <li>SSL 2.0</li> <li>Client</li> <li>TLS 1.1</li> <li>Client</li> <li>Server</li> <li>TLS 1.2</li> <li>Client</li> <li>Server</li> <li>SSL 2.0</li> <li>Client</li> <li>SSL 2.0</li> <li>Client</li> <li>TLS 1.1</li> <li>Client</li> <li>TLS 1.1</li> <li>TLS 1.2</li> </ul>		名称 (默认) 聞 DisabledByDefault 聞 Enable 名称 @ (默认) 聞 DisabledByDefault 聞 Enable	業型 REG_SZ REG_DWORD REG_DWORD          美型         REG_SZ         REG_DWORD         REG_DWORD         REG_DWORD	数据 (数值未设置) 0x00000000 (0) 0x0000001 (1) 数据 (数值未设置) 0x00000000 (0) 0x00000001 (1)
SSL 2.0     Client     Client     Client     Server     TLS 1.1     Client     Server     SSL 2.0     Client     SSL 2.0     Client     Server     TLS 1.1     Client     Server     TLS 1.1     Client     Server     TLS 1.1     Client     Server     TLS 1.2     Client     Server     TLS 1.2     Client		名称 (默认) 题 DisabledByDefault 题 Enable 名称 (默认) 题 DisabledByDefault 题 Enable	業型 REG_SZ REG_DWORD REG_DWORD          業型         REG_SZ         REG_DWORD         REG_DWORD         REG_DWORD         REG_DWORD	数据 (数值未设置) 0x00000000 (0) 0x0000001 (1) 数据 (数值未设置) 0x00000000 (0) 0x00000001 (1)

完成后重启系统

加密套件调整

对于前向保密加密套件不支持的话可通过组策略编辑器进行调整。

开始菜单——运行、输入gpedit.msc 进行加密套件调整 在此操作之前需要先开启TLS1\_2协议



🗐 本地组策略编辑器			- • ×
文件(F) 操作(A) 查看(V	) 帮助(日)		
🗢 🄿 🖄 🖬 🔒 👔			
🣔 Windows 设置 🔹 🔺	🧾 SSL 配置设置		
	选择一个项目来查看它的描述。	设置	
▷ 🧧 Windows 组件		🗈 SSL 密码套件顺序	
BranchCache			
🦰 DNS 客户端			
🣔 Lanman 服务			
▷ 🧰 Microsoft 对≇ <sup>=</sup>			
▷ 📔 QoS 数据包计			
₩indows文即			
☐ 后台智能传送月			
📔 链路层拓扑发现			
🧮 脱机文件			
▷ 🦳 网络连接			
□□ 网络连接状态持 🚽		•	Þ
	\扩展 \标准/		
1 个设置			

双击SSL密码套件顺序



■ cci 家双春州顺度			52
Sol and the lith of the			~
🔚 SSL 密码套件顺序		上一个设置(P) 下一个设置(N)	
◎ 未配置( <u>C</u> ) 注释:			*
◎ 已启用(F)			
			-
□ □無用( <u>U</u> ) 支持的平台:	Taband L. M.		_
2000 F H.	至少 Windows Vista		^
			Ŧ
选项:		帮助:	
			٦.
SSL 密码套件			
TLS_RSA_WITH_AES_128_CB	C_SHA256	如何修改此设置:	
		2. 复制可用套件的列表并将其粘贴到该文档中。	
		  3. 按正确顺序排列套件;删除不想使用的所有套件。	
		4. 在每个套件名称的末尾键入一个逗号(最后一个套件名称除外)。 确保没有嵌入空格。	
		5. 删除所有换行符,以便密码套件名称位于单独的一个长行上。	
		6. 悠恋砚春代行复制到前贴板。然后悠其软贴到编辑框中,是于	
		长度为 1023 个字符。	≡
			Ŧ
		确定 取消 应用( <u>A</u> )	

把支持的ECDHE加密套件加入SSL密码套件中 以逗号 (,)分隔

打开一个空白写字板文档。

复制下图中右侧可用套件的列表并将其粘贴到该文档中。

按正确顺序排列套件;删除不想使用的所有套件。

在每个套件名称的末尾键入一个逗号(最后一个套件名称除外)。确保没有嵌入空格。

删除所有换行符,以便密码套件名称位于单独的一个长行上。

将密码套件行复制到剪贴板,然后将其粘贴到编辑框中。最大长度为1023个字符。



🎨 SSL 密码套件顺序				x
📰 SSL 密码套件顺序	<del>7</del>		上一个设置(P) 下一个设置(N)	
<ul> <li>○ 未配置(<u>C</u>)</li> <li>注料</li> <li>○ 已启用(<u>E</u>)</li> <li>○ 已禁用(<u>D</u>)</li> <li>支持</li> </ul>	¥: 韩的平台:	至少 Windows Vista		4 >
选项:			帮助:	
SSL 密码套件 TLS_RSA_WITH_AES	S_128_CB(	C_SHA256	如果禁用或不配置此设置,则将使用出厂默认密码套件顺序。 SSL2、SSL3、TLS 1.0 和 TLS 1.1 密码套件: TLS_RSA_WITH_AES_128_CBC_SHA TLS_RSA_WITH_AES_256_CBC_SHA TLS_RSA_WITH_AES_256_CBC_SHA TLS_RSA_WITH_RC4_128_SHA TLS_RSA_WITH_3DES_EDE_CBC_SHA TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P256 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P384 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P521 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA_P521 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA_P384 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA_P384 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P521 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P521 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P521 TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA_P384 TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA_P384 TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA_P521 TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA_P521	× E
			确定 取消 应用(A	)

可将以下套件加入密码套件中

TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256 TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA384 TLS\_ECDHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256 TLS\_ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384

#### 附:

推荐套件组合:

TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA\_P256



TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA\_P384 TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA\_P521 TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA\_P256 TLS ECDHE RSA WITH AES 256 CBC SHA P384 TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA\_P521 TLS ECDHE RSA WITH AES 128 CBC SHA256 P256 TLS ECDHE RSA WITH AES 128 CBC SHA256 P384 TLS\_ECDHE\_RSA\_WITH\_AES\_128 CBC SHA256 P521 TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA384\_P256 TLS ECDHE RSA WITH AES 256 CBC SHA384 P384 TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA384\_P521 TLS DHE RSA WITH AES 256 GCM SHA384 TLS RSA WITH AES 128 CBC SHA TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA TLS\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA256 TLS RSA WITH AES 256 CBC SHA256 TLS\_RSA\_WITH\_AES\_128\_GCM\_SHA256 TLS RSA WITH AES 256 GCM SHA384



# 安全签章指引

最近更新时间:2018-01-16 17:33:57

# 什么是安全认证签章?

诺顿安全认证签章是由Symantec SSL证书提供、互联网上最受认可的信任标记。由赛门铁克开展的个人用户调查表明,诺顿安全认证签章保留了电子商务网站所有人和其他注重隐私的网站所有人所重视的高知名度和信赖度。 2013年 1月展开的独立调查也显示,诺顿安全认证签章让个人用户对互联网的信任度达到最高。



# 使用安全认证签章的原因

诺顿安全认证签章在 170 个国家或地区每天显示近 10 亿次。

通过获得客户认可来拓展在线业务:根据一个国际在线消费者研究报告,90%的调查对象表示如果在结账流程中看到 诺顿安全认证签章,他们很可能会继续在线购买,这一数字高于任何其他签章或没有签章显示的情况。

在全球范围内,有超过4000多万台使用诺顿网页安全的台式机会在搜索结果中的可信网站链接旁显示诺顿安全认证签章。

赛门铁克强大的 PKI 基础架构包括军用级数据中心和灾难恢复站点,可以为客户数据提供无与伦比的保护和可用性, 让客户高枕无忧。

此签章是您致力于执行 PCI 遵从的可见图像证明,因为电子商务站点必须验证其身份并加密通过其站点的交易通信, 从而保护客户数据。

#### 签章安装说明

用户可以通过诺顿安全签章在线生成工具,输入自己的域名来获取相应的安全签章代码。

如下所示, www.domain.com 网站的安全签章代码:

```
<div id="symantecSeal" style="text-align: center" title="单击即可验证 - 该站点选择 SymantecSSL 实现安
全的电子商务和机密通信">
<script type="text/javascript" src="https://seal.verisign.com/getseal?host_name=www.domain.com&am
p;size=L&use_flash=YES&use_transparent=YES&lang=zh_cn"></script>
</div>
```