

服务器证书安装配置指南

IIS8

二〇二一年一月



第一步:生成证书签名请求文件(CSR)

打开 IIS 服务管理器,点击计算机名称,双击打开右侧的"服务器证书"图标



双击打开服务器证书后,点击右侧的"创建证书申请"

	Internet Information Services (IIS)管理器	_ D X
-OEGJKQ3ESQ6 →	😰 🚿 🟠 😧 •	
<mark>ф(</mark> Н)		
● 服务	器证书	操作 导入
使用此功能来申请	和管理 Web 服务器可以对配置了 SSL 的网站使用的证书。	创建证书申请
· 筛选:	▼ 〒 弁 (G) マ □ 全部 显示(A) 分组依据:	完成证书申请



输入申请证书信息,点击下一步

	申请证书	? X	
可分辨名称属性			
指定证书的必需信息。省/市/自	治区和城市/地点必须指定为正式名称,并且不得包含缩写。		
通用名称(M);	cn.globalsign.com		
组织(O):	GlobalSign China Co., Ltd.		
组织单位(U);	IT Dept.		
城市/地点(L)	Shanghai		
省/市/自治区(S):	Shanghai		
国家/地区(R):	CN v		
	上一页(P) 下一步(N) 完成(F)	取消	

选择加密服务提供程序和加密长度,建议默认,点击"下一步"

申请证书	?	×
加密服务提供程序属性		
选择加密服务提供程序和位长,加密密钥的位长决定了证书的加密强度。位长越大,安全性越强。但较大的 位长可能会降低性能。 加密服务提供程序(S):		
Microsoft RSA SChannel Cryptographic Provider		
位长(B): 2048 ~		
上一页(P) 下一步(N) 完成(F)	取消	



选择证书签名请求 (CSR) 文件保存的路径和文件名, 点击"完成"

申请证书	?	x
文件名		
为证书申请指定文件名。此信息可以发送给证书颁发机构签名。 为证书申请指定一个文件名(R):		
C:\Users\GlobalSign_CSR.txt		
上一页(P) 下一步(N) 完成(F)	取消	

第二步:提交 CSR, 申请证书

递交证书申请表及相关资料,并把证书请求文件(CSR)提交给我们。我们确认资料齐全后,三个工作日内完成证书颁发。

第三步:获取服务器证书

将证书签发邮件中的从BEGIN 到 END 结束的服务器证书内容(包括"-----BEGIN CERTIFICATE-----"和"-----END CERTIFICATE-----")粘贴到记事本等文本编辑器中,并修 改文件扩展名,保存为server.cer 文件。



第四步:安装服务器证书

打开 IIS 服务管理器,点击计算机名称,双击打开右侧的服务器证书图标



双击打开服务器证书后,点击右侧的"完成证书申请"

	Internet Information Services (IIS)管理器	_ D X				
DEGJKQ3ESQ6 🔸	EGJKQ3ESQ6					
(H)						
● 服祭	哭行书	操作				
		导入				
使用此功能来申请	创建证书申请					
辞讲.	- 雪田始(G) - 日 全部見示(A) 十分組織塀·	完成证书申请				



选择GlobalSign 颁发的服务器证书文件,并指定一个好记的名称(可选),点击确定

完成证书申请	? X
指定证书颁发机构响应	
通过检索包含证书颁发机构响应的文件来完成先前创建的证书申请。 包含证书颁发机构响应的文件名(<u>R</u>):	
C.(Osers(server.cer 好记名称①: cn.globalsign.com	
为新证书选择证书存储(<u>S</u>): 个人	
确定	取消

点击网站下的站点名称,点击右侧的"绑定"



打开网站绑定界面后,点击"添加"

			网站约	绑定	? ×
美型	主机名	端口	IP 地址	绑定信息	添加(A)
http		80	*		编辑(E)
				删降(R)	
					浏览(B)
					关闭(C)



添加网站绑定	? ×
类型(T): IP 地址(I): https ✓ 主机名(H): 需要服务器名称指示(N)	端囗(O): ✓ 443
SSL 证书(F): cn.globalsign.com	选择(L) 查看(V) 确定 取消

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,点击确定

添加完成后,网站绑定界面将会看到刚刚添加的内容

	网站纬	聢	? X
<mark>类型</mark> 主机名 http https	满口 IP 地址 80 * 443 *	绑定信息	添加(A) 编辑(E) 删除(R) 浏览(B)
			关闭(C)

第五步:配置中级 CA 证书

为保障服务器证书在IE7 以下客户端的兼容性,服务器证书需要安装两张中级CA证书(即中级证书和 交叉证书)。从邮件中获取中级证书和交叉证书:将证书签发邮件中的从BEGIN 到 END 结束的两张中 级CA 证书内容(包括"-----BEGIN CERTIFICATE-----"和"-----END CERTIFICATE-----")分别粘



贴到记事本等文本编辑器中,并修改文件扩展名,保存为intermediate1.cer和intermediate2.cer文件。

第六步:安装中级 CA 证书

点击"开始""运行""mmc"

🖾 运行	×
	Windows 将根据你所输入的名称,为你打开相应的程序、文 件夹、文档或 Internet 资源。
打开(<u>O</u>):	mmc ~
	确定 取消 浏览(<u>B</u>)

打开控制台,点击"文件""添加/删除管理单元"

	控制台1	- [控制台橋	時点							-	$\Box \rightarrow$
-	文件(F)	操作(A)	查看(V)	收藏夹(O)	窗口(W)	帮助	I(H)				- 8
4	 ◆ 新建(№) 打开(○) 保存(S) 另存为(A) 添加/删除管理单元(№) 选项(P) 				Ctrl+ Ctrl+ Ctrl+ Ctrl+	N O S M	何项目。 控制台根节点 更多操作				
	<u>1</u> C 2 C 3 C 4 C	:\Windows` :\Windows` :\Windows` :\Windows` :\Windows`	\\certmg \\compr \\service \system32	yr.msc ngmt.msc es.msc /\secpol.msc							



找到"证书"点击"添加"

漆加或删除管理单元							×
你可以在计算机上为此控制台	选择可用的管理单元	讲書	尼置所选的一组管	理单元。对于可扩展的)管理单元,你可以配	置要启用哪些扩展项。	
可用的管理单元(S):				听选管理甲元(E):			
管理单元	供应商	٨		🎬 控制台根节点		编辑扩展(X)	
🔍 服务	Microsoft Corp					mine (n)	
💣 高级安全 Windows Def	Microsoft Corp					創际(K)	
🕺 共享文件夹	Microsoft Corp						
🎥 计算机管理	Microsoft Corp					上移(U)	
④任务计划程序	Microsoft Corp						_
	Microsoft Corp					下移(D)	
🛃 事件查看器	Microsoft Corp		添加(A) >				
₩ 授权管理器	Microsoft Corp						
🚞 文件夹	Microsoft Corp						
◎ 性能监视器	Microsoft Corp						
🗊 证书	Microsoft Corp						
🧾 组策略对象编辑器	Microsoft Corp						
🕭 组件服务	Microsoft Corp					真切りの	
		~				100 MX (V)	
描述:							
证书管理单元允许你浏览自己	的、一个服务的或-	-台)	计算机的证书存储	内容。			

选择"计算机账户",点击"下一步"

证书管理单元	×
该管理单元将始终为下列帐户管理证书:	
○我的用户帐户(M)	
○服务帐户(S) ●计算机帐户(C)	
<上一步(B) 下一步(N) > 取消	



点击"完成"

选择计算机	\times
请选择需要这个管理单元管理的计算机。 这个管理单元将始终管理: ●本地计算机(运行此控制台的计算机)(L):	
○另一台计算机(A): 浏览(R)	
□从命令行启动时,允许更改所选计算机。这只有在保存控制台的情况下才适用(W)。	
< 上一步(B) 完成 取消	

点击"证书(本地计算机)",选择"中级证书颁发机构""证书",在空白处点击右键,选择"所有

任务""导入"。





通过证书向导分别导入中级 CA 证书 intermediate1.cer、intermediate2.cer

← 🦻 证书导入向导	×
要导入的文件 指定要导入的文件。	
文件名(F): C:\Users\GS\Desktop\intermediate1.cer.cer	
注意:用下列格式可以在一个文件中存储多个证书:	
个人信息交换- PKCS #12 (.PFX, P12) 加密消息语法标准- PKCS #7 证书(.P7B) Manual 変更形式 世界形式 (.SCT)	
MICLOPOLL 译令亦作[12] (1221)	
下一步(N)	取消

选择"将所有的证书放入下列存储",点击"下一步",点击"完成"

		\times	
ę.,	₣ 证书导入向导		
	证书存储		
	证书存储是保存证书的系统区域。		
	Windows 可以自动选择证书存储,你也可以为证书指定一个位置。		
	○根奮趾书奕型,自动选择业书仔储(U)		
	* 将所有的证书都放入下列存储(P)		
	证书存储:		
	中间证书颁发机构 浏览(已)		
			l



导入中级 CA 证书完成。

	_							2027444402	27.42 05.05 (1).16.1T do	
>	n a	企业信任	-					2027/11/27	股方器身份管证,各	<无>
v		中间证书颁发机构	-			GlobalSign Root CA		2028/1/28	<所有>	<无>
		🧾 证书吊销列表	-			GlobalSign		2034/12/10	<所有>	<无>
		🔛 证书	5			GlobalSign Demo Root CA		2026/7/20	<所有>	<无>
>		受信任的发布者		GlobalSign Extended Valia	datio	GlobalSign		2026/9/21	<所有>	<无>
>	1	不信任的证书		ClobalCian DCA DV/CCL/	A 20	ClobalSign		2028/11/21	日本日本 白 小 山 小 山 小 山 小 山 小 一 一 一 一 一 一 一 一 一 一 一	(T)
>		第三方根证书顾发机构	-	Globalsign KSA DV SSL C	A 20	Giobalsign		2020/11/21	服方器身切拉证,普	<无>
>		受信任人		GlobalSign RSA OV SSL C	A 20	GlobalSign		2028/11/21	<所有>	<无>
>	1	客户端身份验证颁发者	-					2012/12/10	<所有>	<无>
>		预宽版根				P	μ.	2020/7/12	客户端身份验证	<无>
>		其他人					ι.	2022/6/28	客户端身份验证	<无>
>		eSIM Certification Authoritie:		EDGVING /	^	the second second	1	2039/12/11	<所有>	< T >
>	1	Homegroup Machine Certific						2002/12/21	(http://www.inite.com	
>		Local NonRemovable Certific	-		•••	1A.		2002/12/31	代码登名, Windows…	<尤>
>		McAfee Trust		- 専入成功。				2024/12/8	1.3.6.1.4.1.311.21	<无>
>	1	MSIEHistoryJournal						2040/1/1	<所有>	<无>
>		远程桌面			d	the state of the s		2023/12/10	客户端身份验证,代	<无>
>	1	证书注册申请	-	税店	2	Procession and a second		2020/2/8	客户端身份验证,代	<无>
>		智能卡受信任的根						2016/10/25	服务黑自份验证 炙	< # >
>		受信任的设备	-	-				2010/10/25	BOOD BEOR DO SEALS TEL:	- 20-
×		Web 宿主								
>		Windows Live ID Token Issue								

按照以上的步骤配置完成,重启IIS服务后,就可以使用 https://www.domain.com访问了。

第七步:服务器证书的备份及恢复

在您成功安装和配置了服务器证书之后,请务必依据下面的操作流程,备份好您的服务器证书,以防 证书丢失给您带来不便。

(1) 服务器证书的备份

进入 IIS 管理控制台,并选择"服务器证书"





选中您的服务器证书项目,并右键选择"导出"

💐 Internet Information Ser	vices (IIS)管理器		1		- 🗆 X
← → •:•					🖬 🗟 🗿 •
文件(F) 视图(V) 帮助(H	0				
Sche(r) Secto(v) Herb(r) 連接 → 立 応用程序法 > 通 阿站 > 資料 Server Farms) 使用此功能本由新 等憑: 名称	证书 / 唐理 Web 服务器可以対配置了 SS ・ 〒 开始(G) 、 〜 全部超 - 一 愛愛培	. 的网站使用的证书。 示(A) 分相依据:不进行分组 • 双发者 · · · · · · · · · · · · ·	到期日期 2002/8/2	 場入 今天 创理证书申请 完成证书申请 创理自签名证书 创理自签名证书 查看 号出 续订 ★ 翻除 允许自动里新抑定续订的证书 ⑦ 報知
			(明)] (新)] (新)) (H))		
	<		W ###U		

输入导出的密钥文件名、存储路径,并为导出的 pfx 格式证书备份文件设置保护密码。

Internet Information Serv	vices (IIS)管理器				×
文件(F) 视图(V) 帮助(H))				
は 注意 はAPTOP-5BPUEBME ② 広用程序地 > ③ 内は > ④ Server Farms	服务器证书 使用此功能来申请和管理 情遇: 名称	 専出運书 専出至印: ①Desktop 電码(P): ●●●●●●●● ●●●●●●● ●●●●●● ●●●●●● ●●●●●● ●●●●● ●●●●● ●●●●● ●●●●● ●●●●● ●●●● ●●●● ●●●● ●●●● ●●●● ●●●● ●●● ●●● ●●● ●● ● ●● ●●	? ×	・ 受加時日期 / TLS 2022/8/2	母入 母入 创建证书申请 充成证书申请 希建城证书 创建城证书 创建成证书 合建加 登書 号出 受出 法行工 发行 金書 资出 支書 资出 支書 资出 支書 资出 支書 资计 支援 次行

保

存好备份的 pfx 文件即可完成备份操作。

(2) 服务器证书的恢复

进入 IIS 管理控制台的服务器证书管理页面,右键选择"导入"



文件(F) 视塑(V) 幹助(F	0					
設 ・ の 立用程序池 > 金 网站 > 4到 Server Farms	 服务器 使用此功能未申请 確認: 名称 名称 	3 証书 前管理 Web 服务時可以 ● ▼ 开始(G) 意义 ⁴	以前配置了 SSL 的际 - 全 全部显示(A 号入 创建证书申请 创建成证书申请 创建成证书申请 创建国签名证书. 允许自动重新讲 帮助	3% 使用的证书。) 分编成据: 不进行分组 ////////////////////////////////////	• 到明日期	■ 時入 例理证书申请 例理域证书 例理域证书 例理编述名证书 方;并目动型新规定体订的证书 和句

选择您的证书备份文件,并输入文件保护密码。

导入证书		?	×
证书文件(.pfx)(<u>C</u>):			
	Desktop\certificat	e.pfx	
密码(P):			
•••••			
选择证书存储(S):			
个人			~
✓ 允许导出此证书(A)			
	确定	取消	

如果选中"标志此密钥为可导出"则您稍后可以将私钥从该服务器导出。不选中此选项时,密钥将无法从当前服务器中导出。参考服务器证书安装部分内容,恢复对导入的证书配置操作。



请注意,此文档会不定期更新!

GlobalSign China Co., Ltd

环玺信息科技 (上海)有限公司

2021年1月