

IIS7.0

服务器证书安装使用指南



上海数字证书认证中心有限公司

2010/01/05



文档说明:

本文档是 WEB 服务器 SSL 双向认证安装使用指南，详细描述了 WEB 服务器证书的申请、安装、备份、恢复以及 SSL 双向认证的配置。

版本信息:

当前版本 3.0 技术支持中心

版权信息:

SHECA 是上海市数字证书证书认证中心有限公司的注册商标和缩写。

UCA 是上海市数字证书证书认证中心有限公司研究开发的通用证书系统的商标和缩写。

本文的版权属于上海市数字证书证书认证中心有限公司，未经许可，任何个人和团体不得转载、粘贴或发布本文，也不得部分的转载、粘贴或发布本文，更不得更改本文的部分词汇进行转贴。

未经许可不得拷贝，影印。

Copyright @2008 上海数字证书认证中心有限公司

文档发行说明

当您阅读完本文档，您应该能解决如下问题：

- 1、WEB 服务器证书的请求文件 CSR 的产生；
- 2、WEB 服务器证书的在线申请；
- 3、WEB 服务器证书的安装；
- 4、WEB 服务器 SSL 安全配置；
- 5、WEB 服务器证书的导出（备份）和导入（恢复）；
- 6、SSL 双向认证的配置；

文档书写环境说明：

本文档的具体试验环境：

WEB 服务器：Windows 7 旗舰版 + IIS 7.0

客户端：Windows 7 旗舰版

WEB 服务器证书申请请求文件（CSR）产生

1、产生证书请求（CSR）文件

开始→所有程序→管理工具→IIS manager→服务器证书



2、界面左侧点击“创建证书申请”



3、在可分辨名称属性中输入用户信息（其中通用名称为用户的域名或者 IP）

注意：请确保您的以下填写的信息和您提交至上海 CA 的申请表上的信息一致，否则将会导致不能签发证书。

申请证书

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):

组织(O):

组织单位(U):

城市/地点(L):

省/市/自治区(S):

国家/地区(B): CN

上一页(B) 下一步(N) 完成(F) 取消

4、选择加密服务提供程序以及密钥长度

申请证书

加密服务提供程序属性

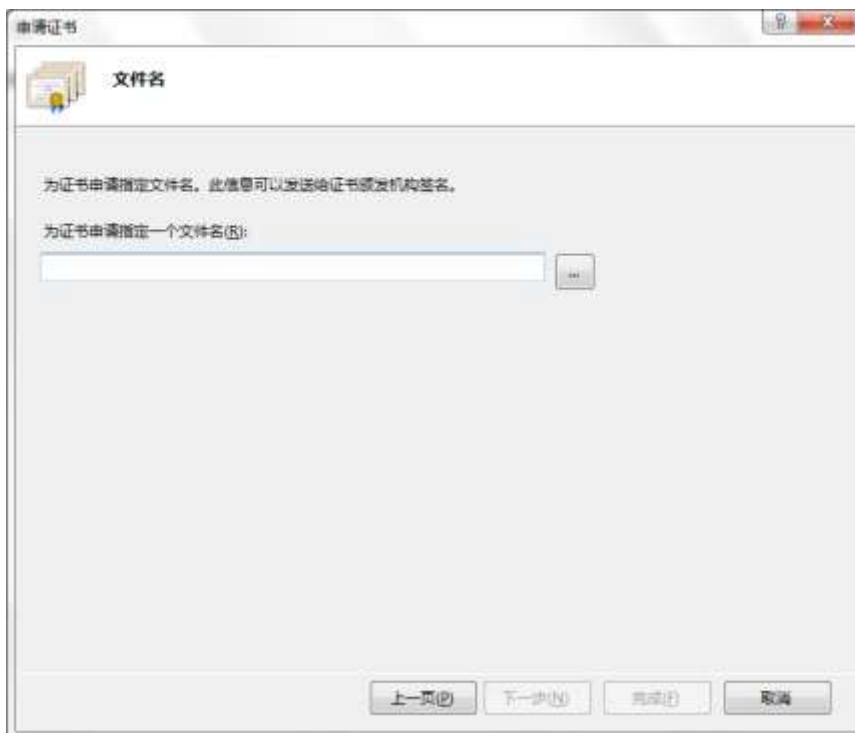
选择加密服务提供程序和位长。加密密钥的位长决定了证书的加密强度。位长越大，安全性越强，但较大的位长可能会降低性能。

加密服务提供程序(S):
Microsoft RSA SChannel Cryptographic Provider

位长(B):
1024

上一页(B) 下一步(N) 完成(F) 取消

5、鼠标单击下一步，将证书申请制定一个文件名并保存下来。



WEB 服务器证书在线申请

第一步：登陆<http://www.sheca.com>，点击证书申请 → [立即申请安全站点证书，请点击>>](#)；


在方框里输入从 SHECA 证书受理点获取的密码信封序列号和信封密码

(注:由于申请的是 WEB 服务器证书,所以设定的私钥密码不起作用)

第二步：完成输入后，进入下一个页面,此时选择勾选“高级选项”，并选择“用户自上送 P10 证书请求”并在最底部的输入框内贴入证书请求中去除 BEGIN 以及 END 的部分内容，如下图所示

第三步：请耐心等待证书签发


上送P10签发证书

 **上送P10签发证书**

证书签发中，请耐心等待...

第四步：请选择证书保存的路径，如需保存为 PEM 格式，则勾选“PEM”，并点击保存证书。

下载证书

 **下载证书**

请确定证书的保存位置：

请选择要同时保存的证书格式： PEM

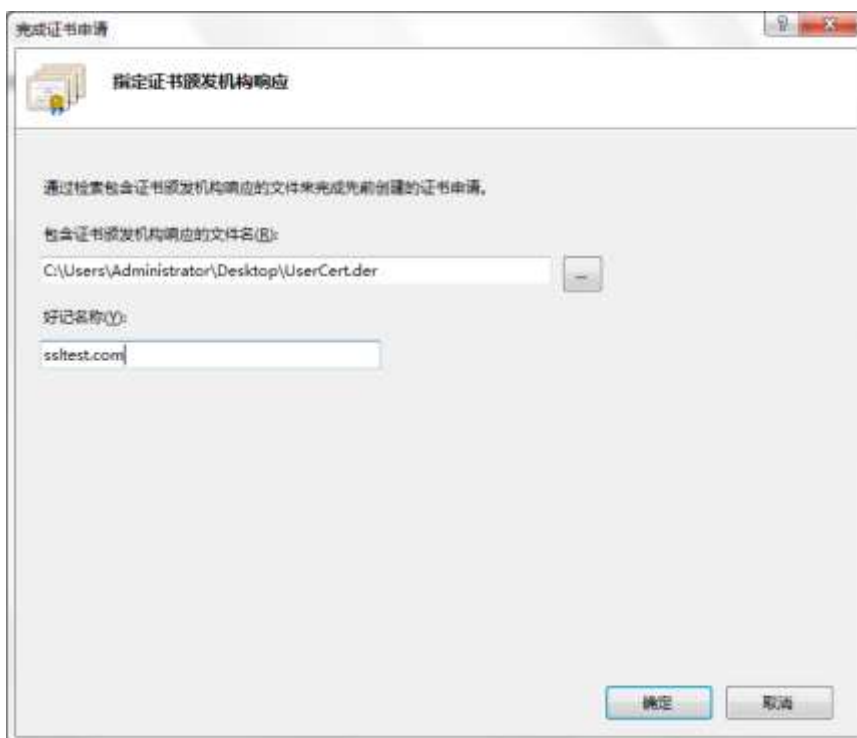
WEB 服务器证书的安装

1、进入 Internet Information Services 管理

开始→所有程序→管理工具→IIS manager→完成证书申请



2、选择从 SHECA 网站上签发得到的证书，并输入一个好记的名称



此时，您已经成功将服务器证书安装到 IIS 服务器当中。

WEB 服务器 SSL 安全配置

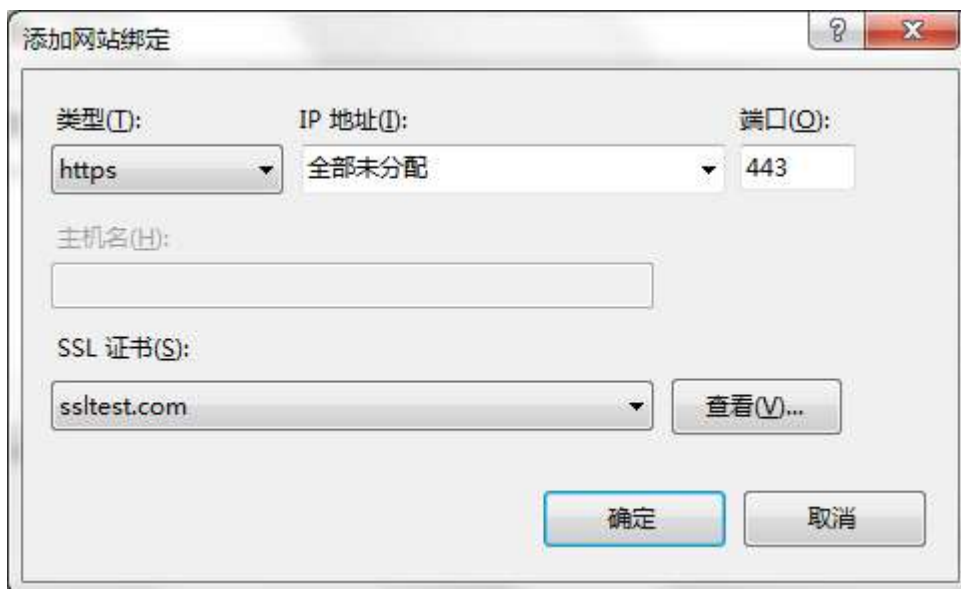
- 1、操作页面中选择“绑定...”



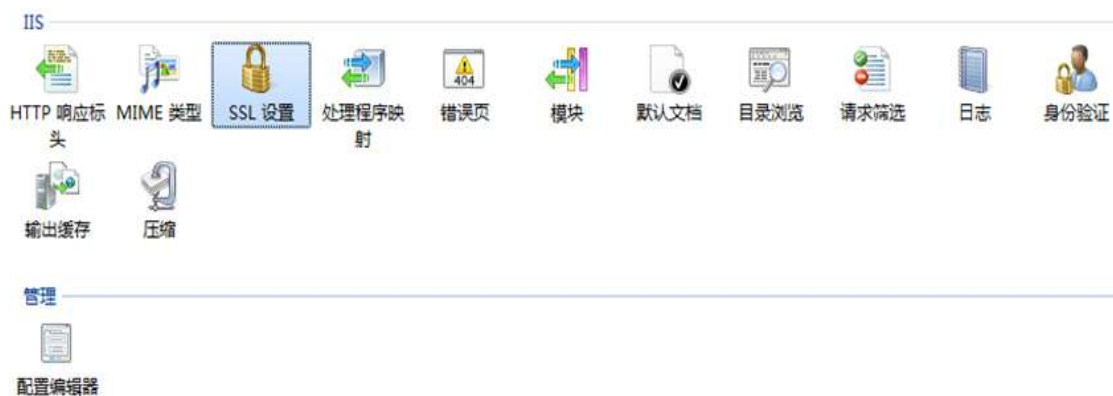
- 2、选择“添加”



3、将类型选择为 Https,并设置 IP 地址以及端口, 并选择需要绑定的证书。



4、选定所需要绑定服务器证书的网站, 选择 SSL 设置



5、勾选“要求 SSL”, 并根据您的实际情况选择是否需要客户端证书的认证。



注意:

- 如果您在**要求 SSL**前打上勾，则以后客户端浏览器仅可以通过 HTTPS 访问您的 WEB 服务器；
- 客户端证书选项分三种：
 - i. **忽略客户端证书:** 客户端访问 WEB 服务器的时候不需要提供客户端自己证书
 - ii. **接收客户端证书:** 客户端访问 WEB 服务器的时候弹出**客户端验证**窗口，允许客户端选择自己的证书，进行身份验证，然后访问 WEB 服务器，这时，如果客户端没有自己的证书，访问仍旧可以照常进行
 - iii. **必须客户端证书:** 这里仅当客户端拥有自己的证书，并通过验证之后，访问才可以进行下去

6、重启您的 IIS 服务器，通过客户端浏览器访问您的 WEB 服务器，假如在先前的设置中需要您设置了**需要客户端证书**的话，这时候会弹出客户端认证窗口，选择您相应的个人证书，确认密钥交换，请单击 OK 按钮。顺利实现 SSL 的双向认证，就可以访问 https 的站点了。

基本的 WEB 服务器安全配置（SSL）已经完成。

WEB 服务器证书的导出（备份）

1、进入 Internet Information Services 管理

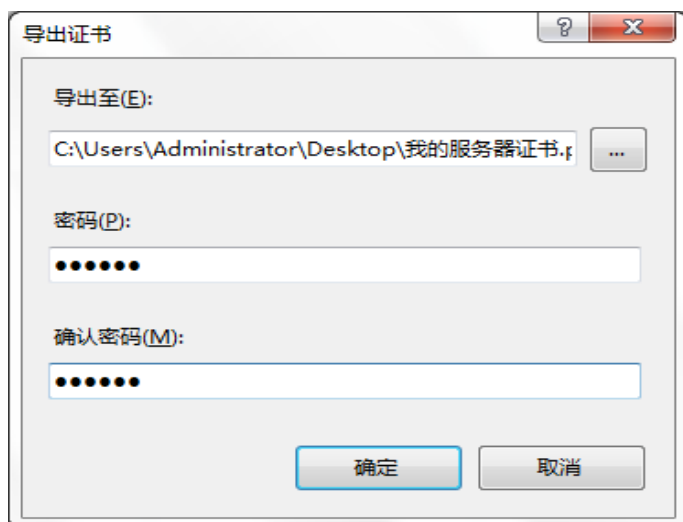
开始→所有程序→管理工具→IIS manager→服务器证书



2、选中需要导出的服务器证书，在右侧的操作框中点击“导出”



3、选择导出证书的位置，并设置证书保护密码。



注意：请将导出的 WEB 服务器证书妥善保管，以备不时之需。

WEB 服务器证书的导入（恢复）

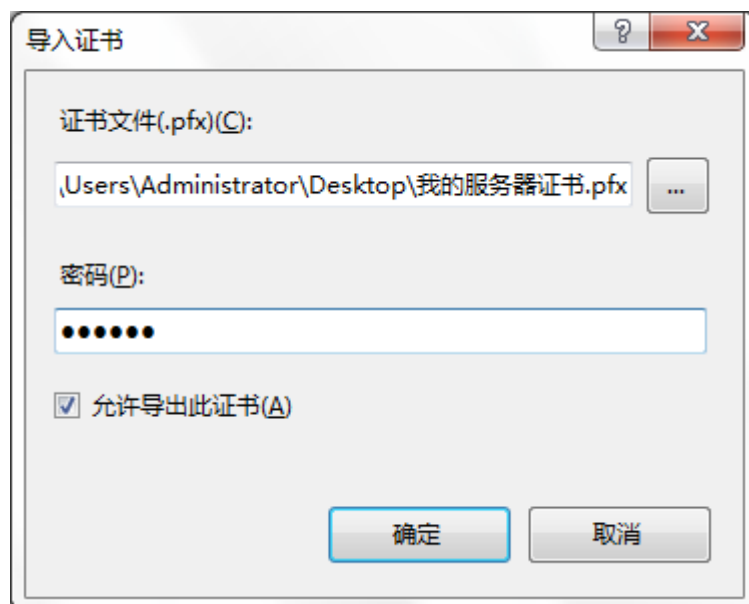
假如由于系统出了问题，导致 IIS 崩溃或其他不可测原因迫使你重新安装了 IIS 或操作系统，那么您可以通过以下方式来恢复您的 IIS WEB 服务器证书。

1、进入 Internet Information Services 管理

开始→所有程序→管理工具→IIS manager→服务器证书



2、选择需要导入的服务器证书，并输入密码（如需允许导出证书，请勾选）



此时您的服务器证书已经导入到服务器内，请按照服务器证书部署的相关步骤进行部署。