

# IIS6.0

## 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

2009/01/05



文档说明:

本文档是 IIS6.0 SSL 双向认证安装使用指南, 详细描述了用于 IIS6.0 服务器的 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：

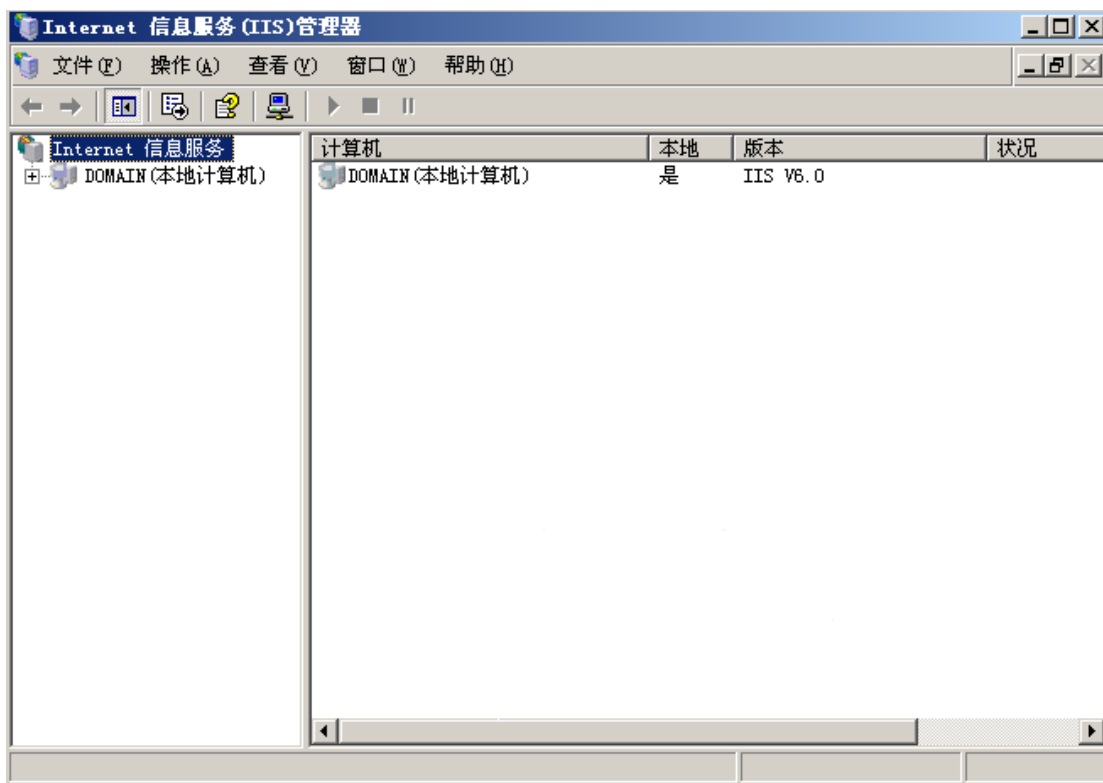
**WEB 服务器：Windows 2003 Enterprise Server Edition + IIS 6.0**

**客户端：Windows XP Professional Version + Service Pack 3**

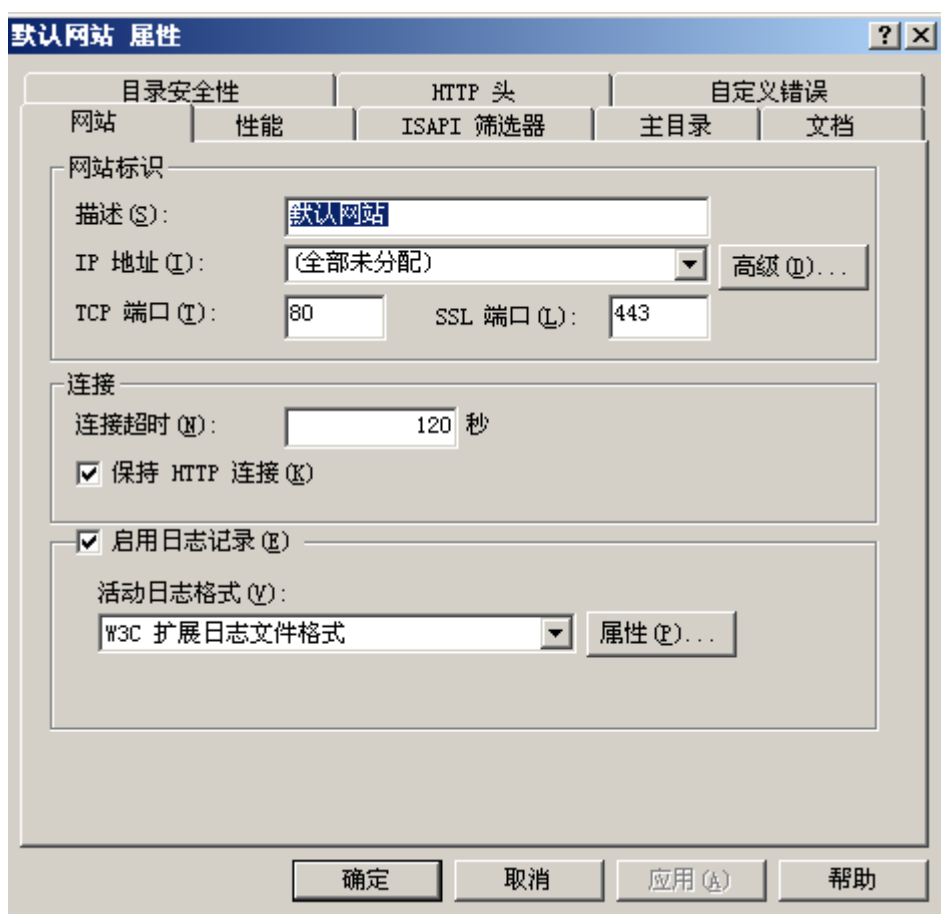
## WEB 服务器证书申请请求文件（CSR）产生

### 1、产生证书请求（CSR）文件

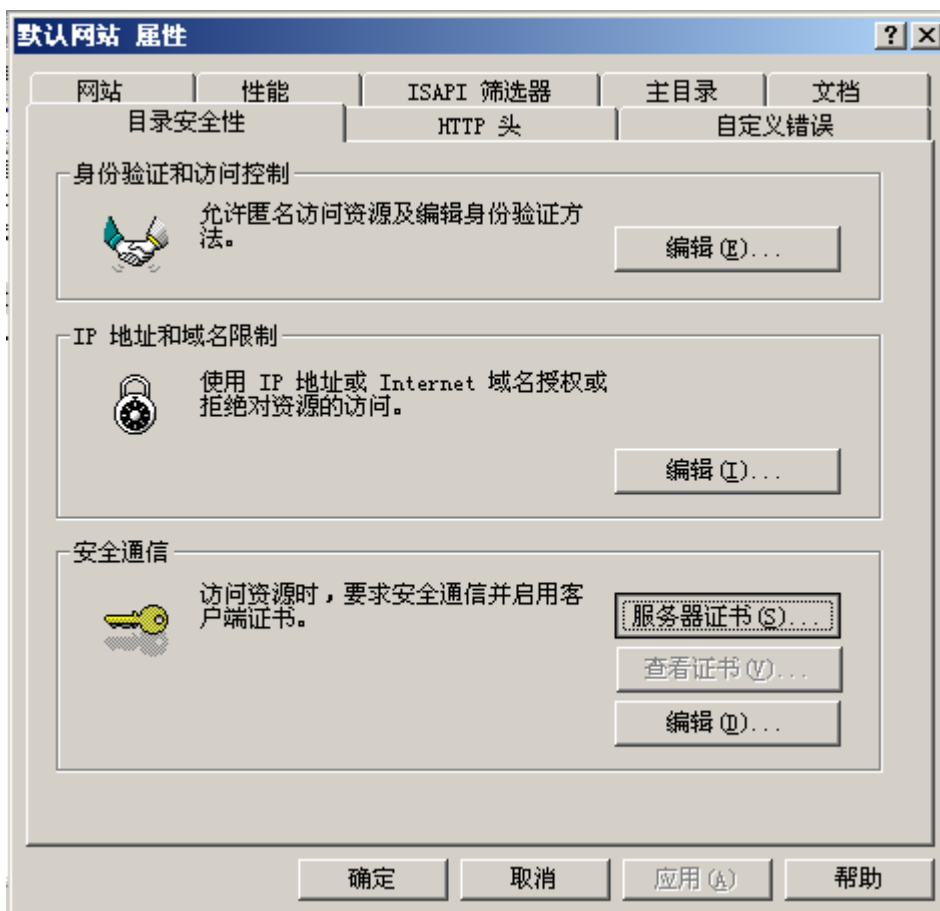
开始→程序→管理工具→Internet 信息服务管理



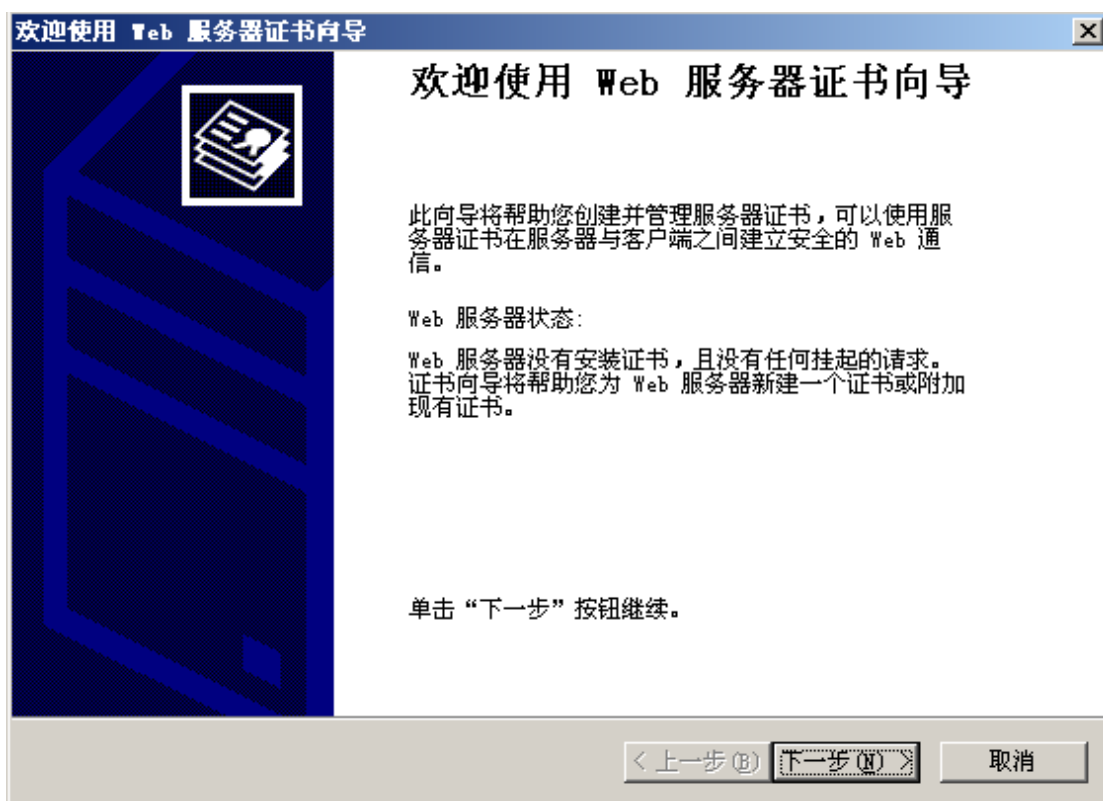
2、鼠标右键单击“默认站点”，并在弹出菜单中选择“属性”



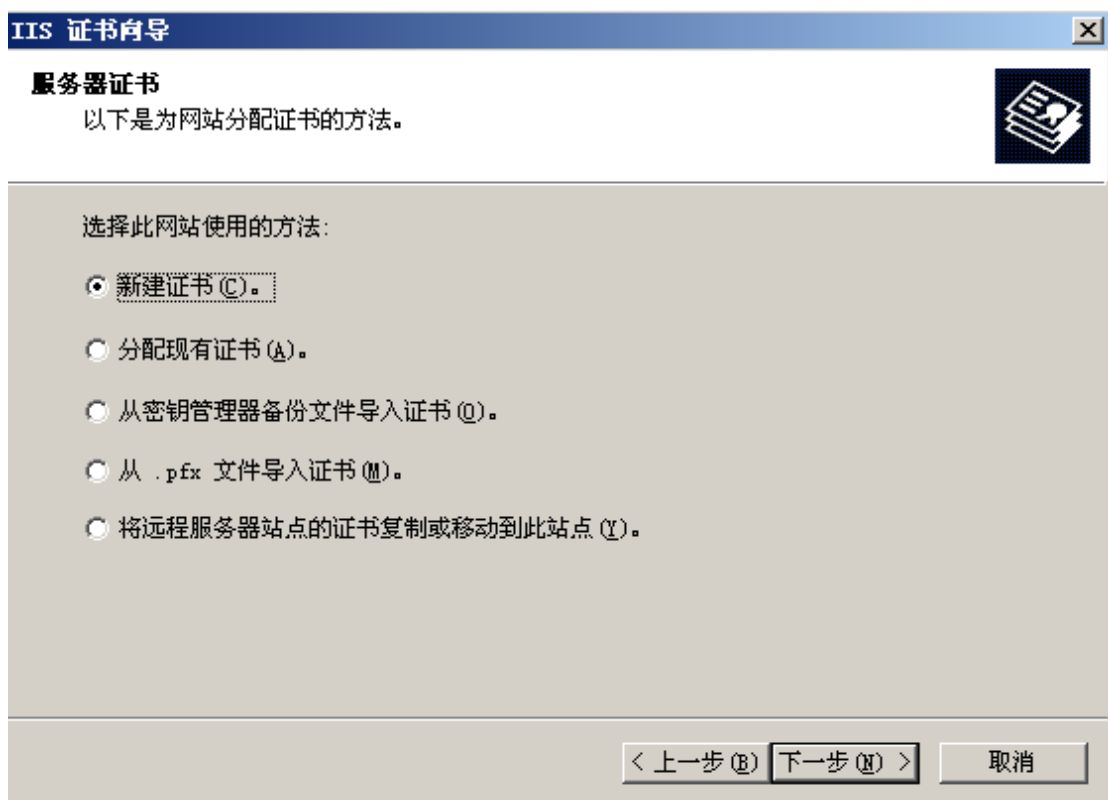
### 3、在默认 WEB 站点属性窗口选择“目录安全性”



4、在“安全通讯”栏目中用鼠标点击“服务器证书”，出现WEB服务器证书向导



2、鼠标单击下一步，选择创建一个新证书，开始证书请求向导





3、选择产生请求文件，不直接发送



4、以下根据提示按照您的 WEB 服务器的实际信息输入

**IIS 证书向导**

**名称和安全性设置**  
新证书必须具有名称和特定的位长。

输入新证书的名称。此名称应易于引用和记忆。

名称 (N):

密钥的位长决定了证书的加密程度。位长越长，安全性越高。然而，位长过长将使性能降低。

位长 (K):

选择证书的加密服务提供程序 (CSP) (P)

< 上一步 (B) 下一步 (N) > 取消

注意：选择 **1024** 位密钥长度

**IIS 证书向导**

**单位信息**  
证书必须包含您单位的相关信息，以便与其他单位的证书区分开。

选择或输入您的单位和部门名称。通常是指您的合法单位名称及部门名称。

如需详细信息，请参阅证书颁发机构的网站。

单位 (U):

部门 (D):

< 上一步 (B) 下一步 (N) > 取消

**IIS 证书向导**

**站点公用名称**

站点公用名称是其完全合格的域名。

输入站点的公用名称。如果服务器位于 Internet 上，应使用有效的 DNS 名。如果服务器位于 Intranet 上，可以使用计算机的 NetBIOS 名。

如果公用名称发生变化，则需要获取新证书。

公用名称 (C):

< 上一步 (B)   下一步 (N) >   取消

注意：通用名一定是 WEB 服务器的域名（FQDN），如果在这一步你输入不正确，那会对您以后正确使用 WEB 服务器证书有影响。

**IIS 证书向导**

**地理信息**

证书颁发机构要求下列地理信息。

国家 (地区) (C):

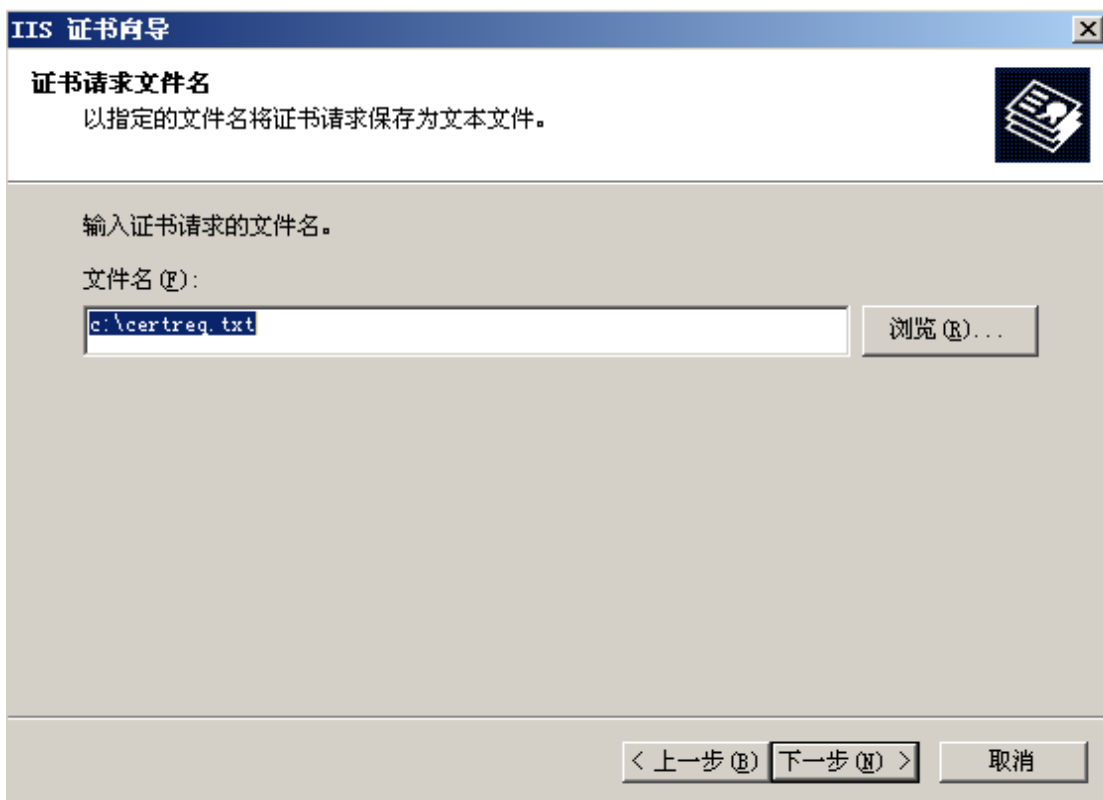
省/自治区 (S):

市县 (L):

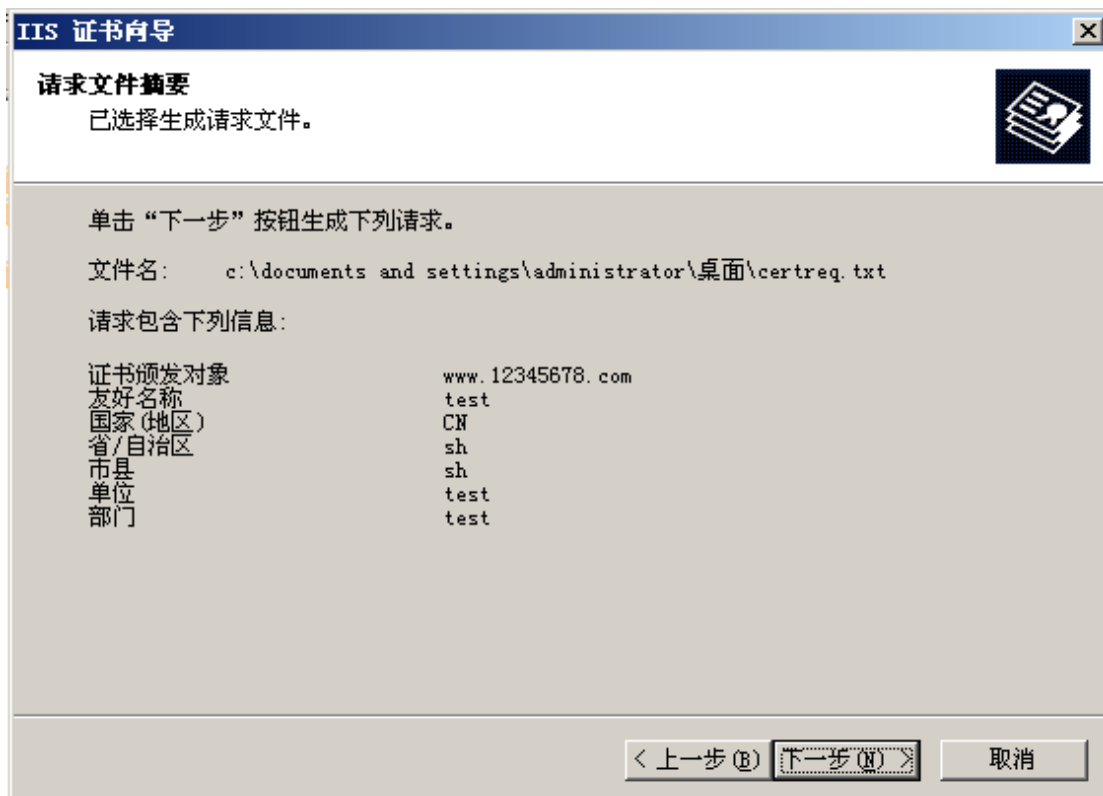
省/自治区和市县必须是完整的官方名称，且不能包含缩写。

< 上一步 (B)   下一步 (N) >   取消

注意：请确保您的以上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。



注意：请确认证书请求文件（CSR）保存位置



注意：确认刚才您输入的信息的正确性



## WEB 服务器证书在线申请

Web 服务器证书网上申请流程:

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

### 生成P10

**生成P10**  
请生成P10的方式

\*没有检测到USBKey，使用证书管理器下载证书。  
如果您有USBKey但没有插上的话，请插上USBKey并点击重新检测。  
如果您要下载到其他地方请勾选“高级选项”！

高级选项

下一步 重新检测

\*请选择生成密钥对和P10证书请求的方式

通过密码设备生成  
 通过证书管理器生成  
 用户自上传P10证书请求

\*如果P10证书请求中存在“-BEGIN...”与“-END...”部分，请自行去除后上传。

在此贴入证书请求当中去除“-BEGIN...”“-END...”的部分

下一步

第三步：请耐心等待证书签发


### 上传P10签发证书

**上传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:

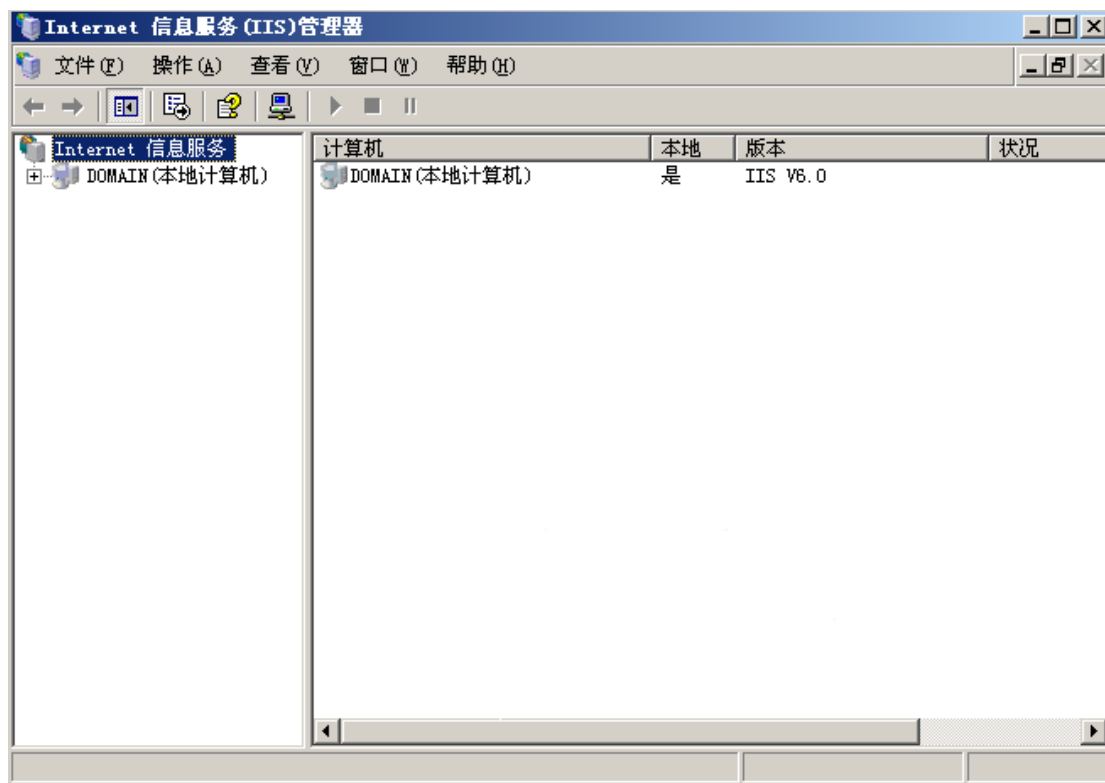
请选择要同时保存的证书格式:  PEM



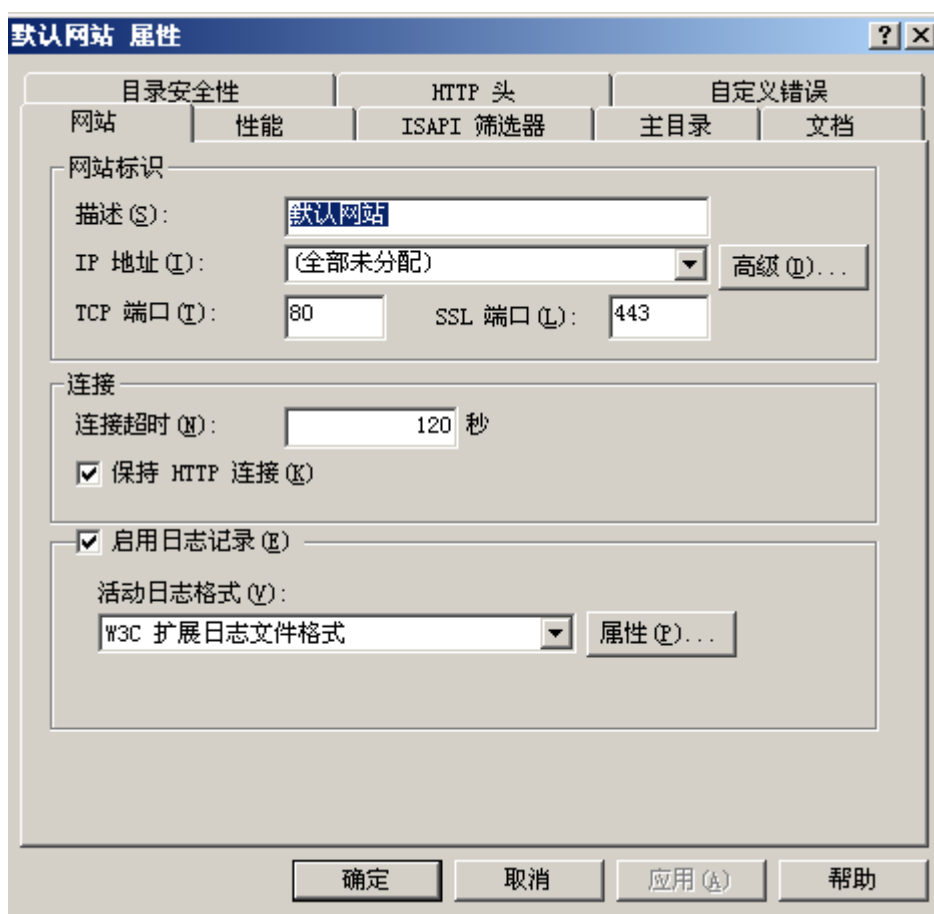
## WEB 服务器证书的安装

### 1、进入 Internet Information Services 管理

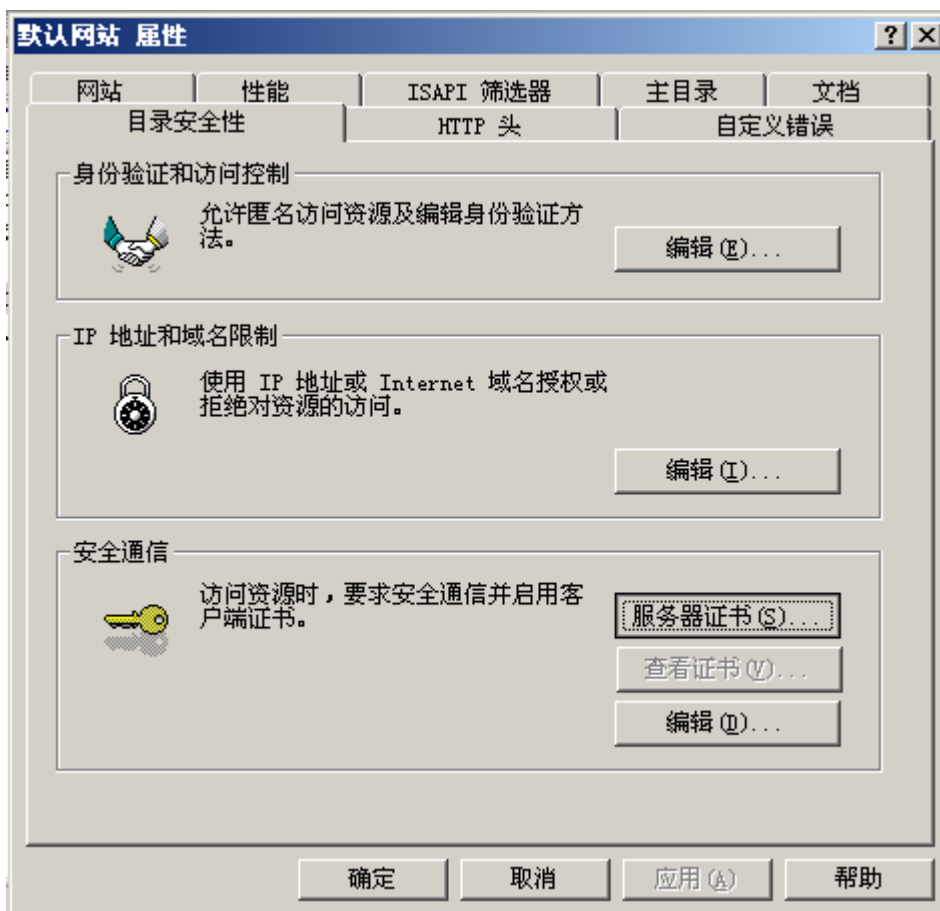
开始→程序→管理工具→Internet Information Services 管理



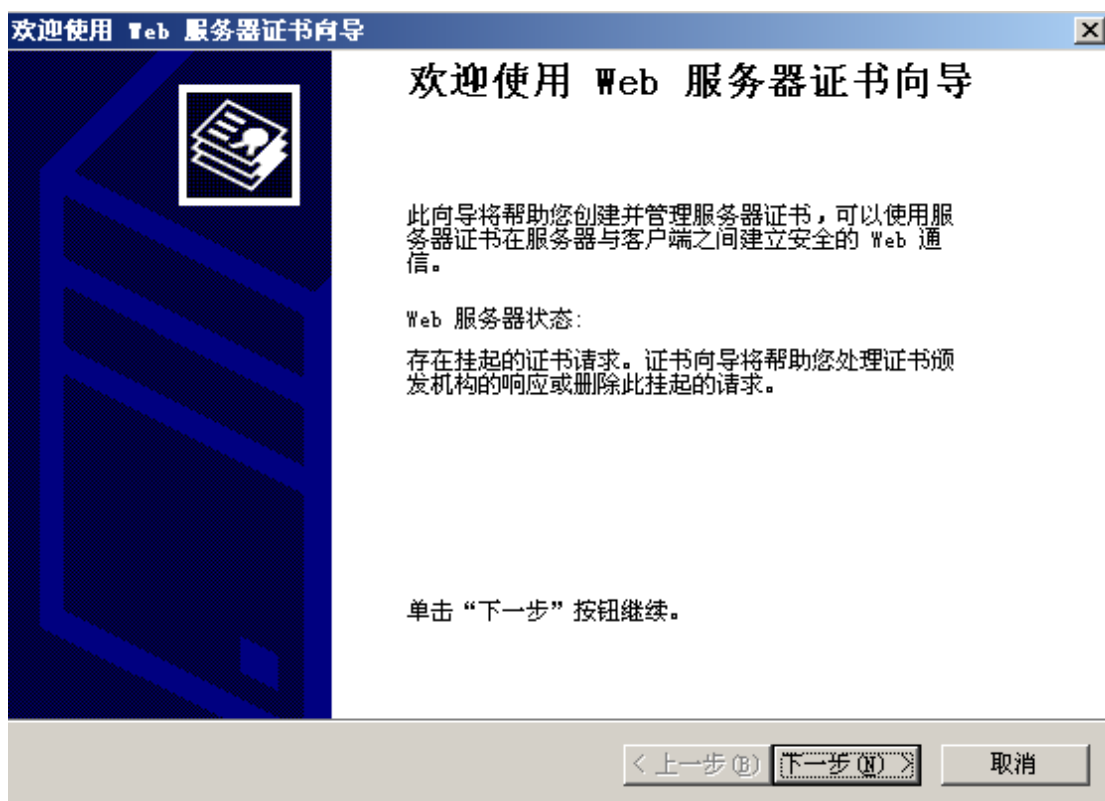
2、鼠标右键单击**默认 WEB 站点**，并在弹出菜单中选择**属性**



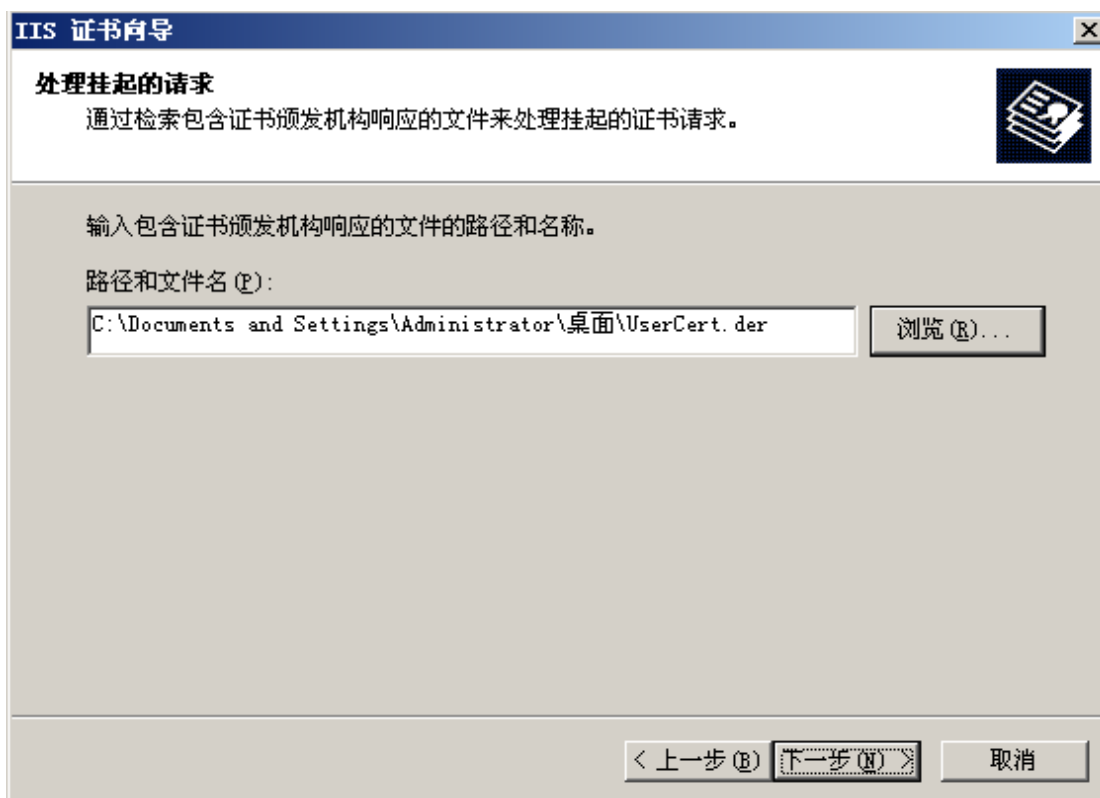
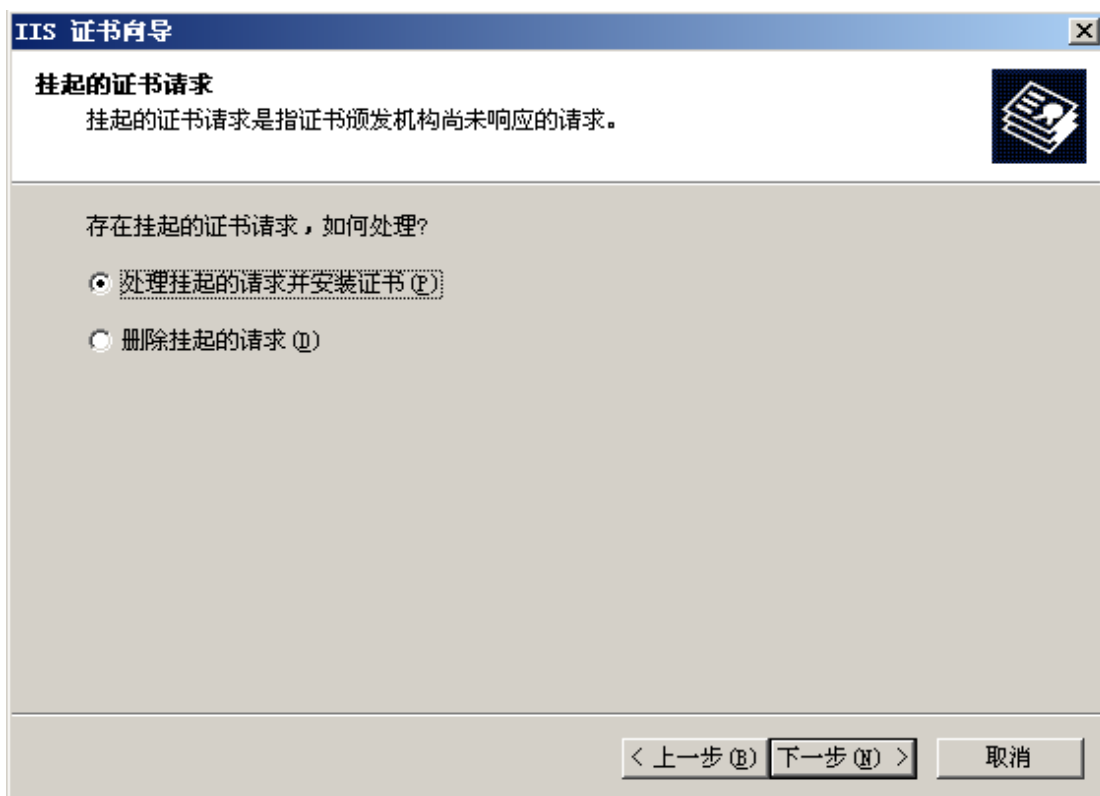
### 3、在默认 WEB 站点属性窗口选择目录安全性



4、在安全通讯栏目中用鼠标点击服务器证书，出现 **WEB 服务器证书向导**



5、鼠标单击下一步，开始进行 **WEB 服务器证书安装向导**，然后按照提示操作



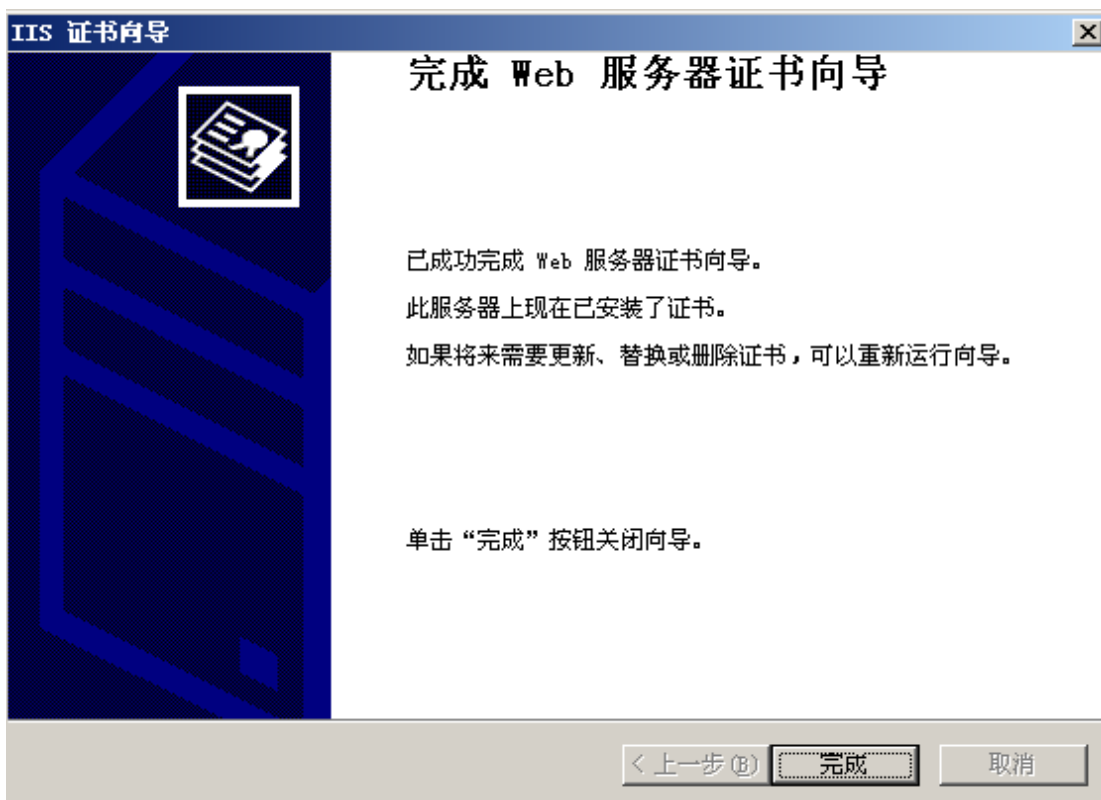
注意：这个文件是你从 SHECA 网站申请成功下载的证书



端口默认的是 **443**，您也可以根据实际情况更改



注意：仔细确认 WEB 服务器证书的具体信息



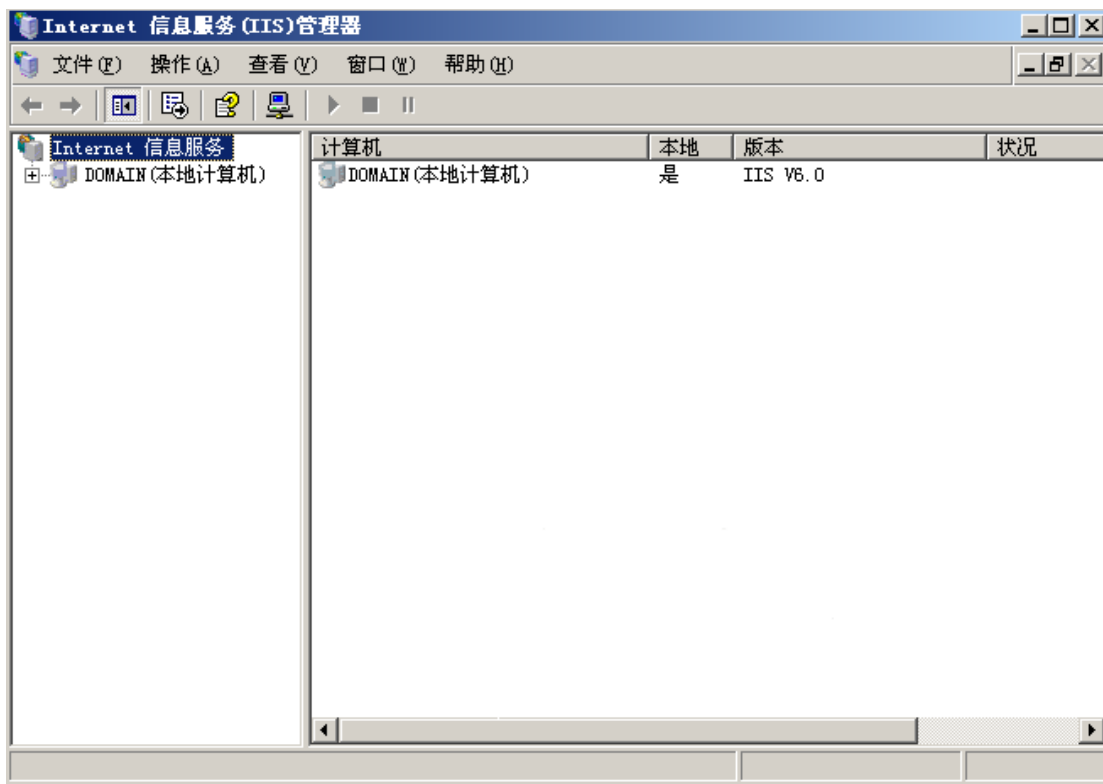
注意：完成 WEB 服务器证书的安装



## WEB 服务器 SSL 安全配置

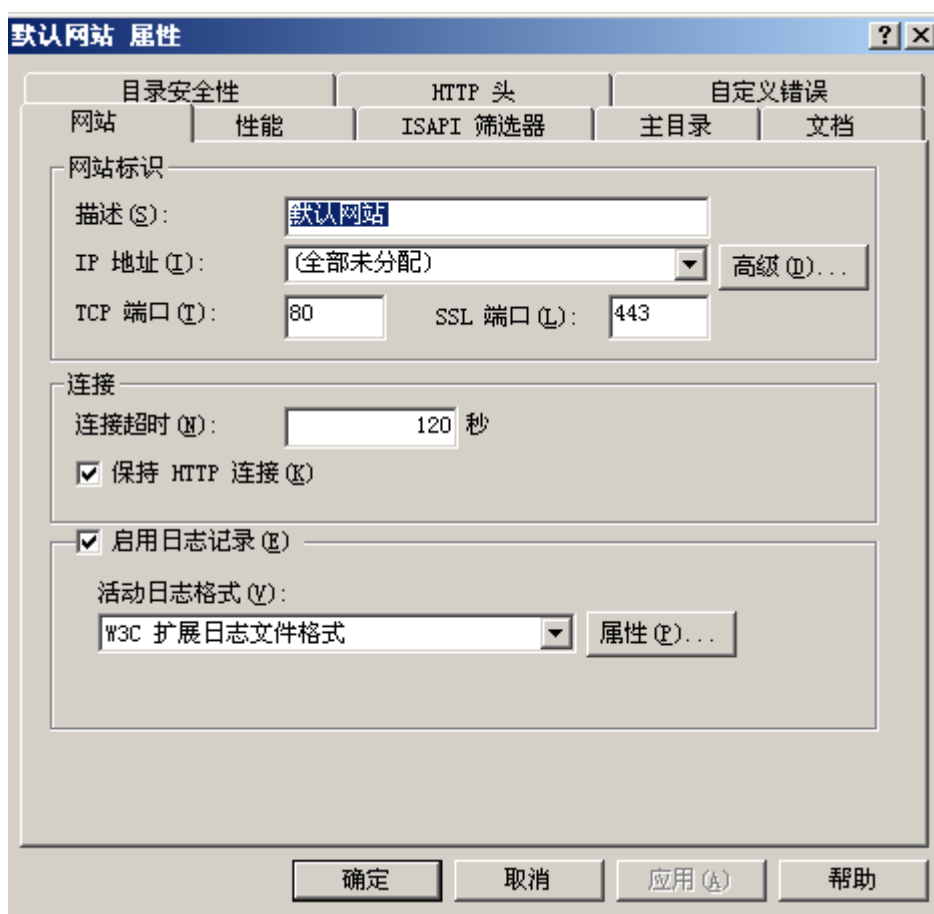
### 1、进入 Internet Information Services 管理

开始→程序→管理工具→Internet Information Services 管理

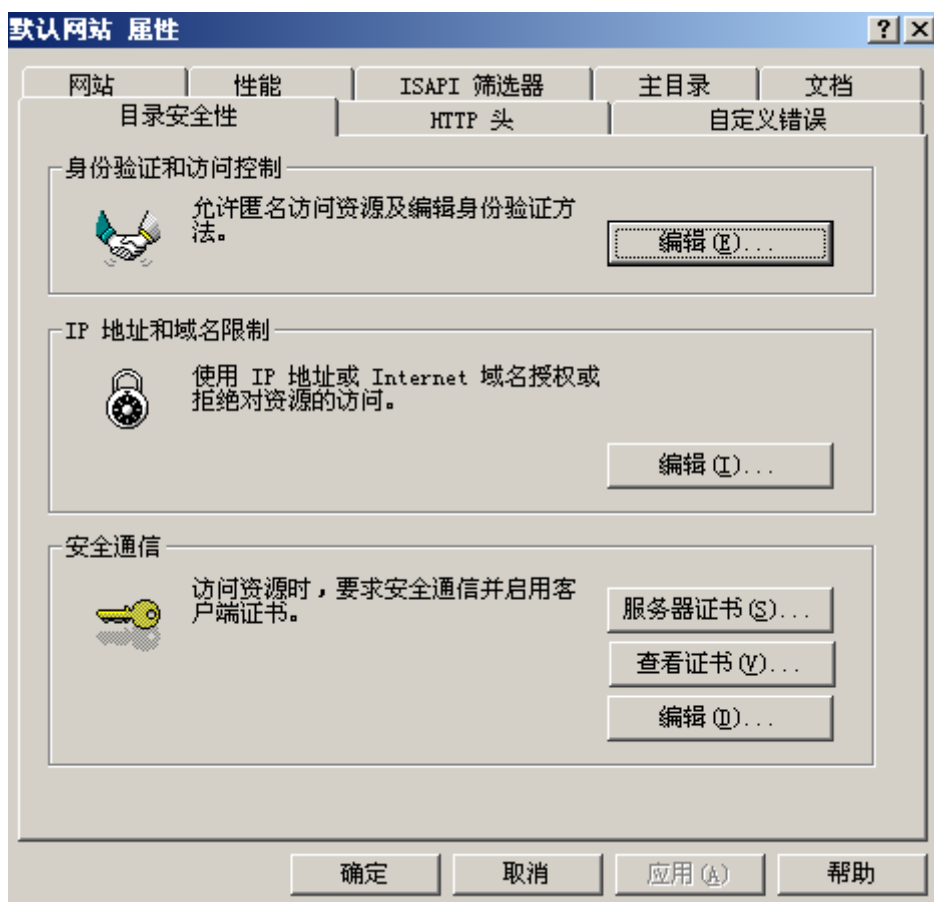




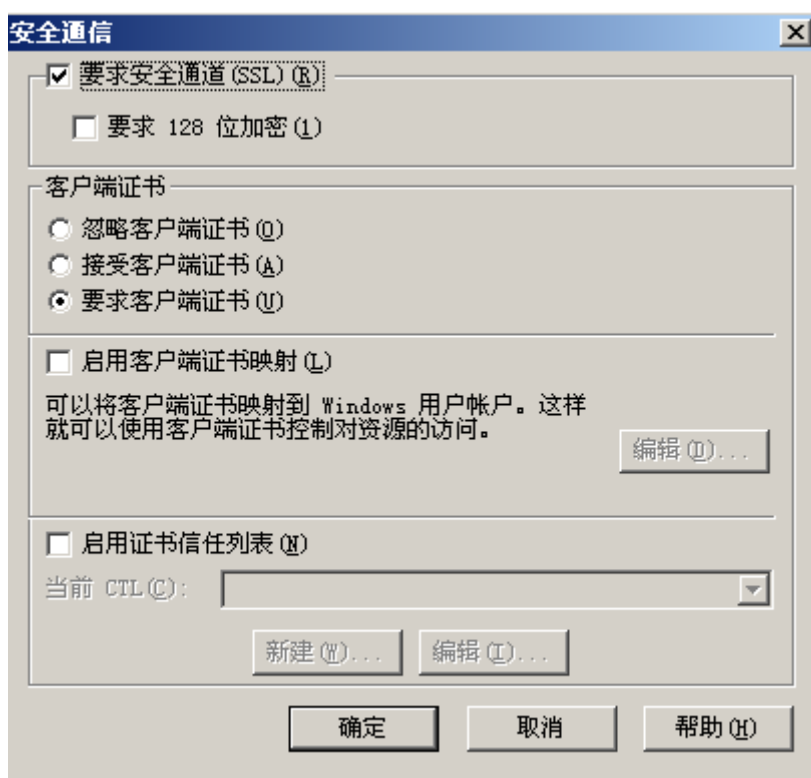
2、鼠标右键单击**默认 WEB 站点**，并在弹出菜单中选择**属性**



### 3、在默认 WEB 站点属性窗口选择目录安全性



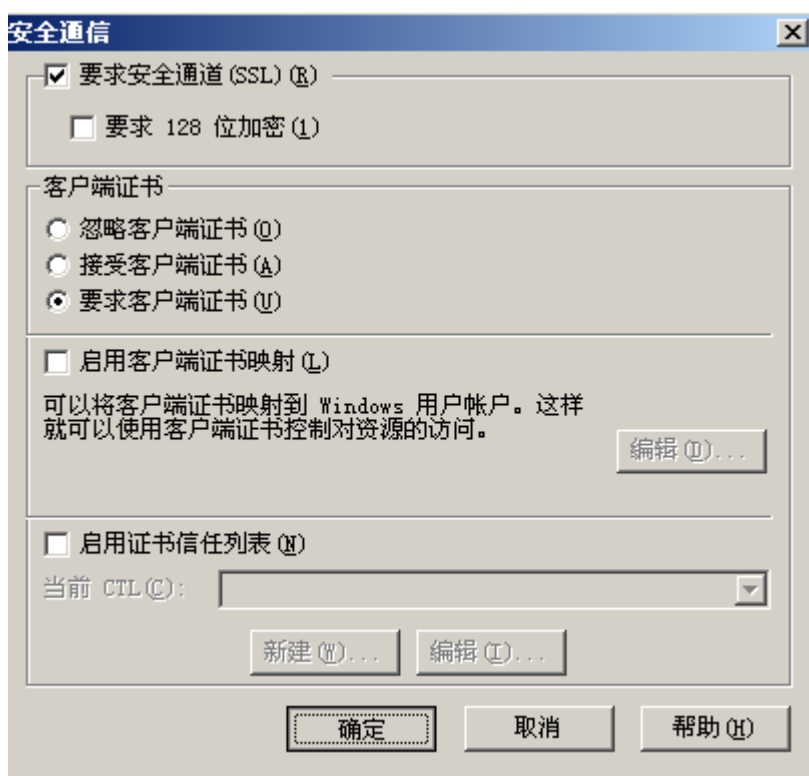
#### 4、在安全通讯栏目中用鼠标点击编辑，出现安全通讯界面



注意：

- 如果您在**需要安全通道 (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；
- 如果您在**需要 128 位加密**前打上勾，则以后客户端浏览器只有具备 128 位加密强度之后才可以访问您的 WEB 服务器；有关浏览器的加密强度请咨询相关软件开发商；
- 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. **需要客户端证书**：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
- **允许客户端证书映射**，这项功能是将您的 WEB 服务器上的资源和 WINDOWS 帐号下的用户通过证书捆绑。

## 5、根据实际需要完成了安全通讯的设置



- 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。

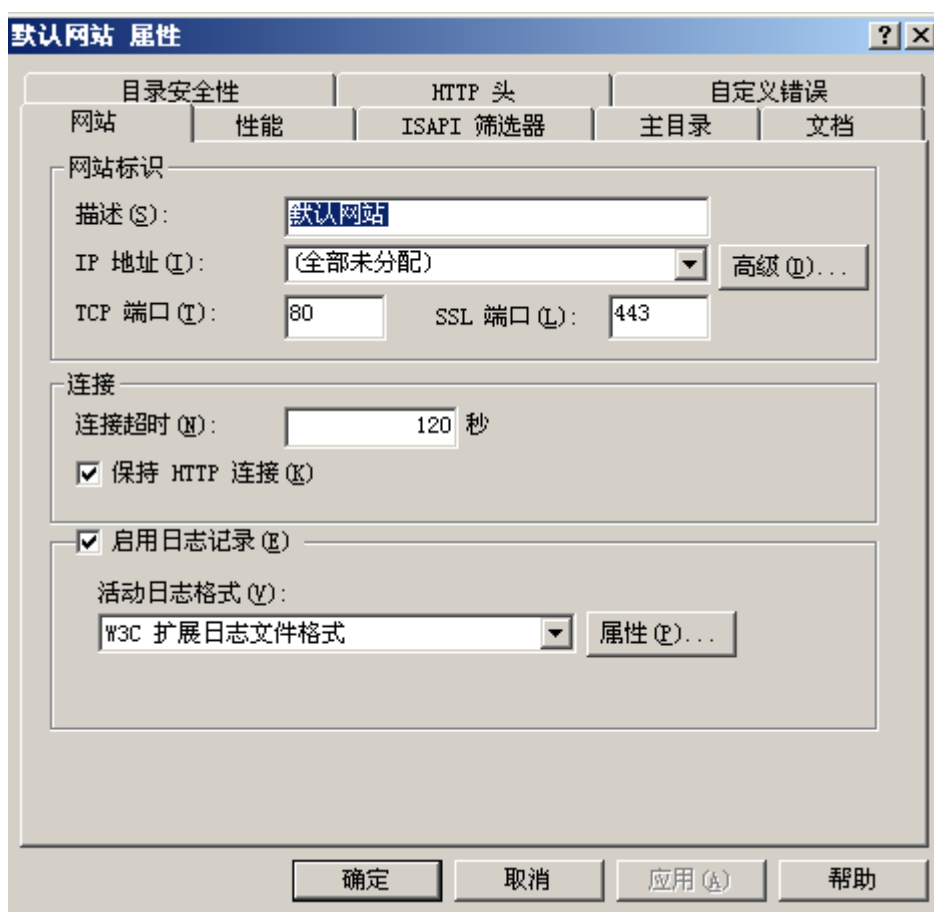
## WEB 服务器证书的导出（备份）

### 1、进入 Internet Information Services 管理

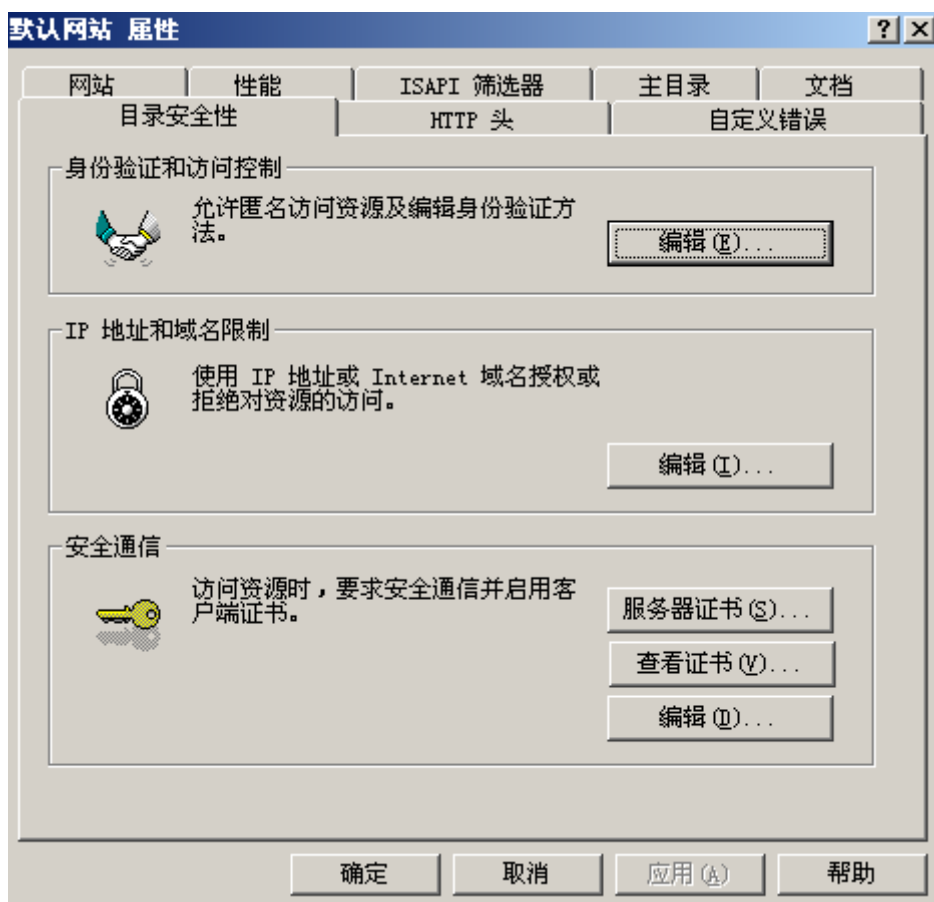
开始→程序→管理工具→Internet Information Services 管理



2、鼠标右键单击**默认 WEB 站点**，并在弹出菜单中选择**属性**

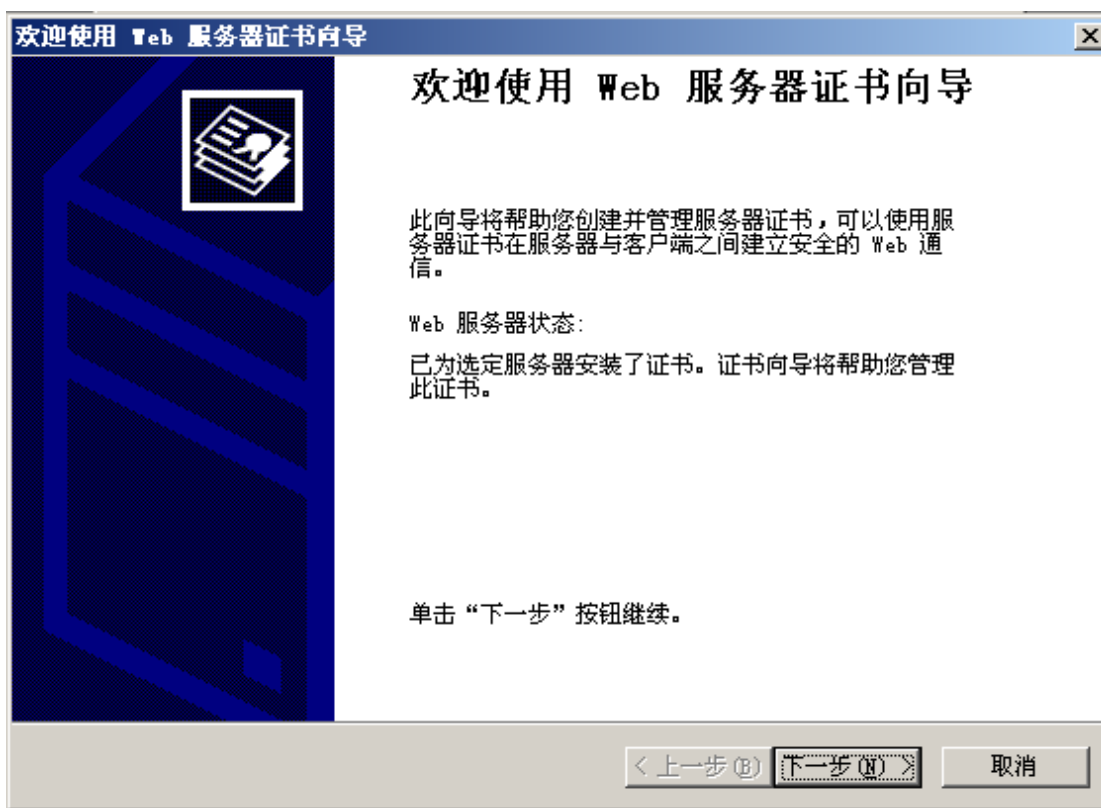


### 3、在默认 WEB 站点属性窗口选择目录安全性

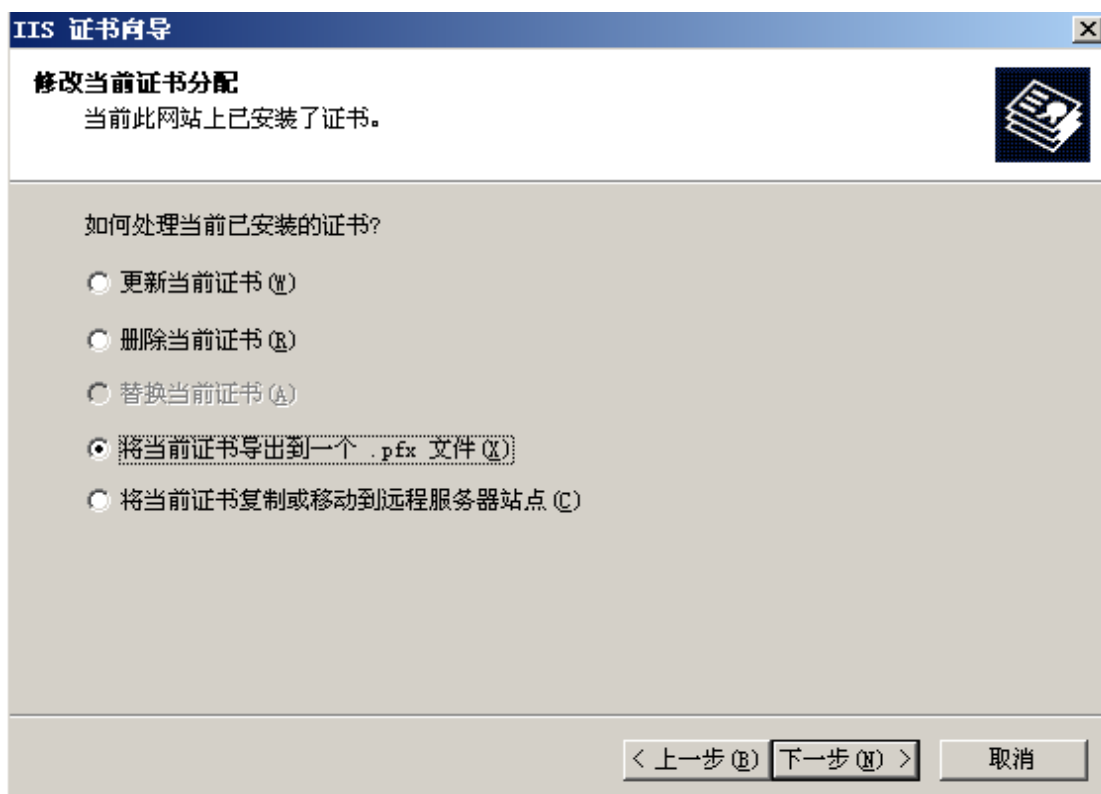




- 4、在安全通讯栏目中用鼠标点击服务器证书，出现 **WEB 服务器证书向导** 界面



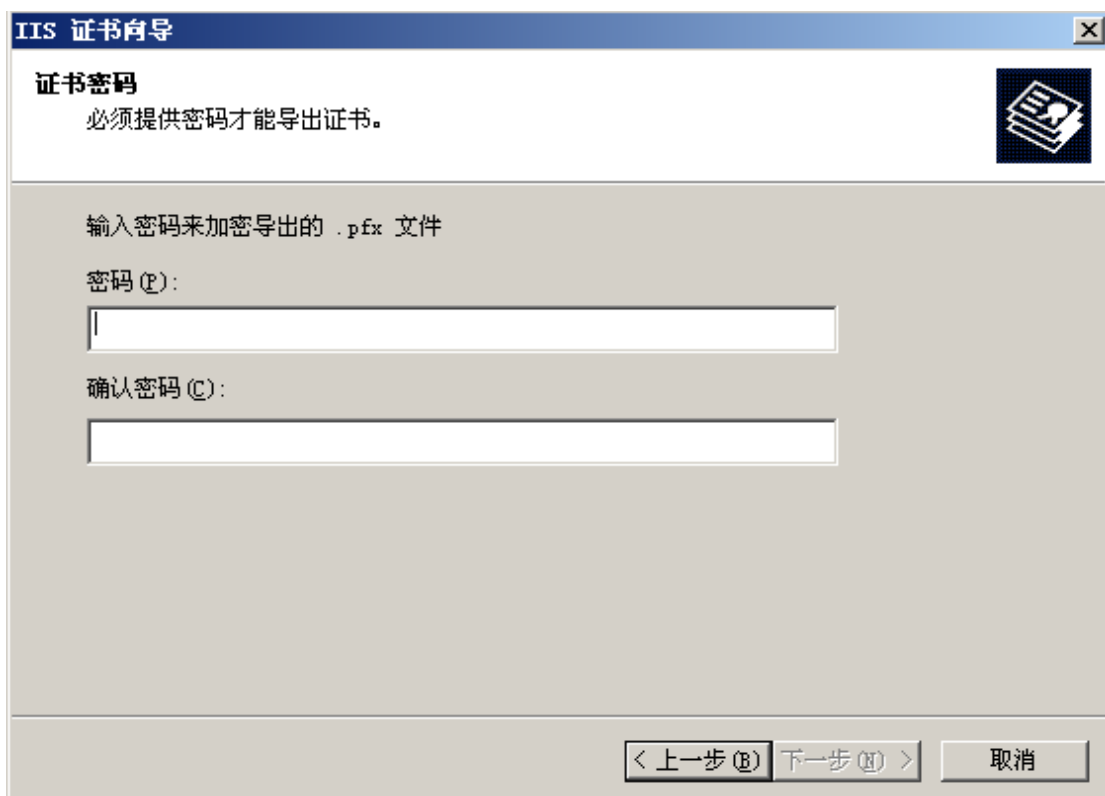
- 5、单击下一步，出现 IIS 证书向导界面，这时候您有若干种选择来处理您已安装的 WEB 服务器证书。



- 6、我们选择导出当前证书到.pfx 文件，这样，我们以后就可以通过这个文件恢复这个 WEB 服务器证书。选择一个保存路径，单击下一步



## 7、输入.pfx 文件的保护口令

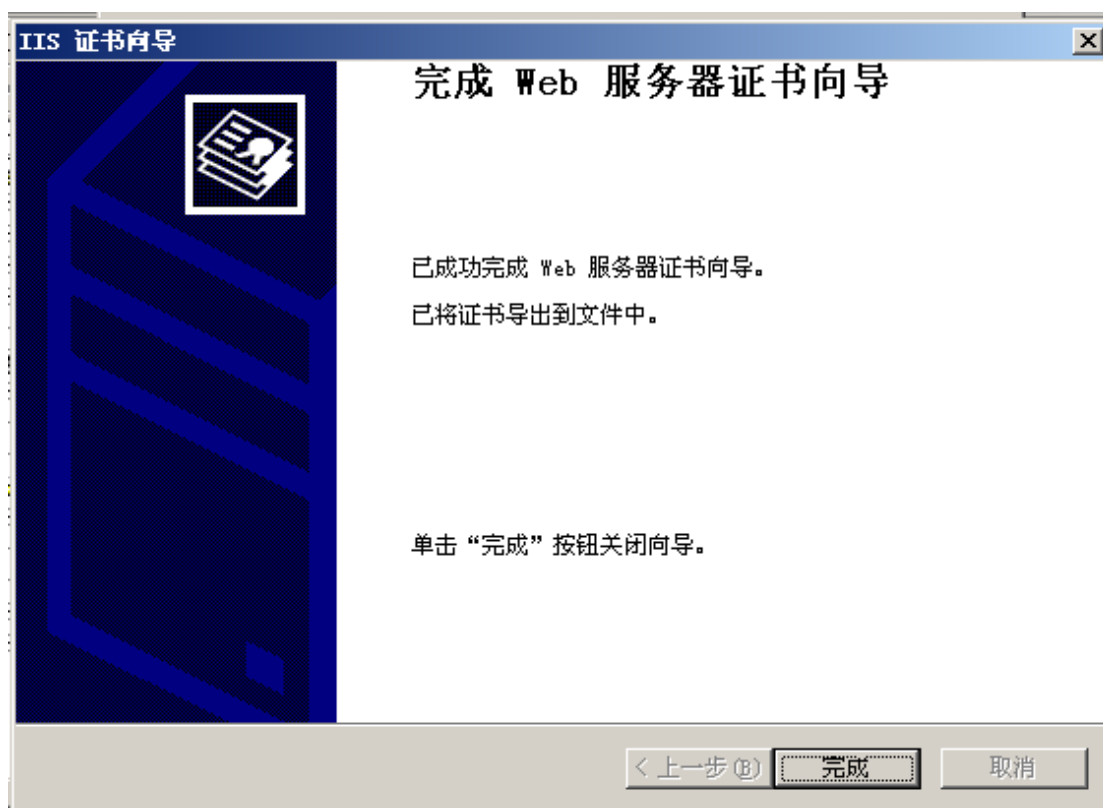


The screenshot shows a Windows dialog box titled "IIS 证书向导" (IIS Certificate Wizard) with a sub-header "证书密码" (Certificate Password). The main text reads "必须提供密码才能导出证书。" (A password must be provided to export the certificate). Below this, it says "输入密码来加密导出的 .pfx 文件" (Enter a password to encrypt the exported .pfx file). There are two input fields: "密码 (P):" (Password) and "确认密码 (C):" (Confirm Password). At the bottom, there are three buttons: "< 上一步 (P)" (Previous Step), "下一步 (N) >" (Next Step), and "取消" (Cancel).

8、出现导出证书的简要说明，确认之后，单击下一步



9、完成您的 WEB 服务器证书的备份工作



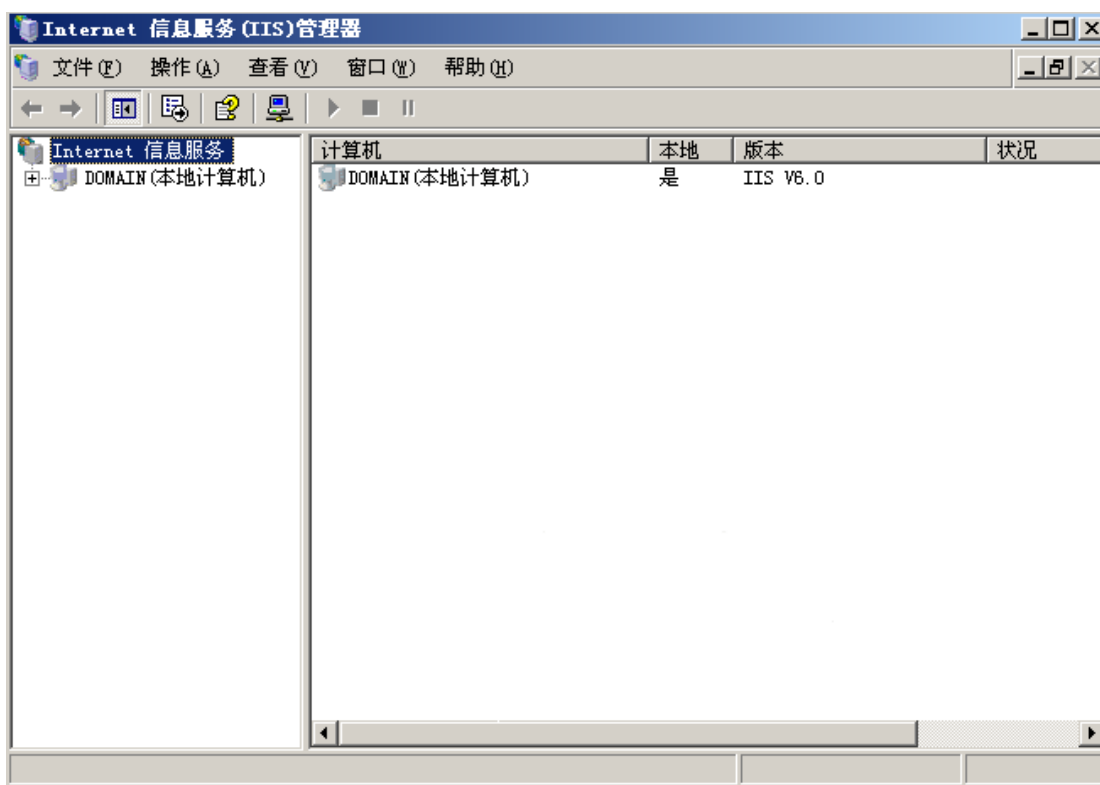
注意：请将导出的 WEB 服务器证书妥善保管，以备不时之需。

## WEB 服务器证书的导入（恢复）

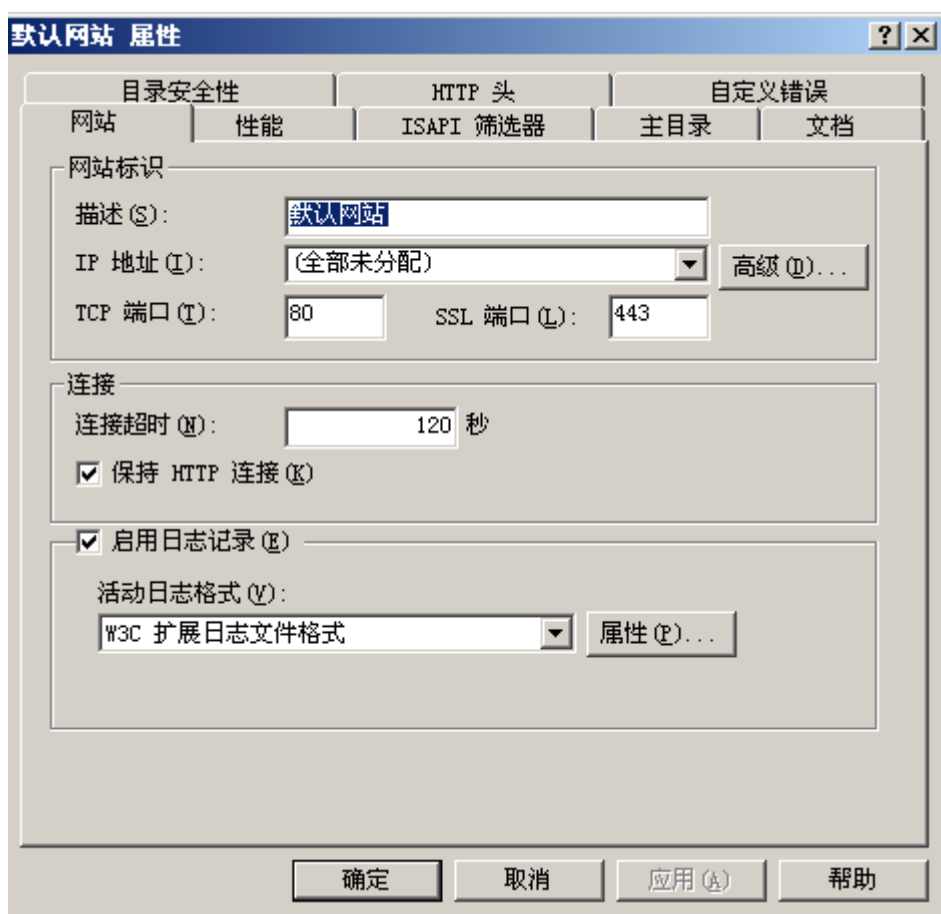
假如由于系统出了问题，导致 IIS 崩溃或其他不可测原因迫使你重新安装了 IIS 或操作系统，那么您可以通过以下方式来恢复您的 IIS WEB 服务器证书。

### 1、进入 Internet Information Services 管理

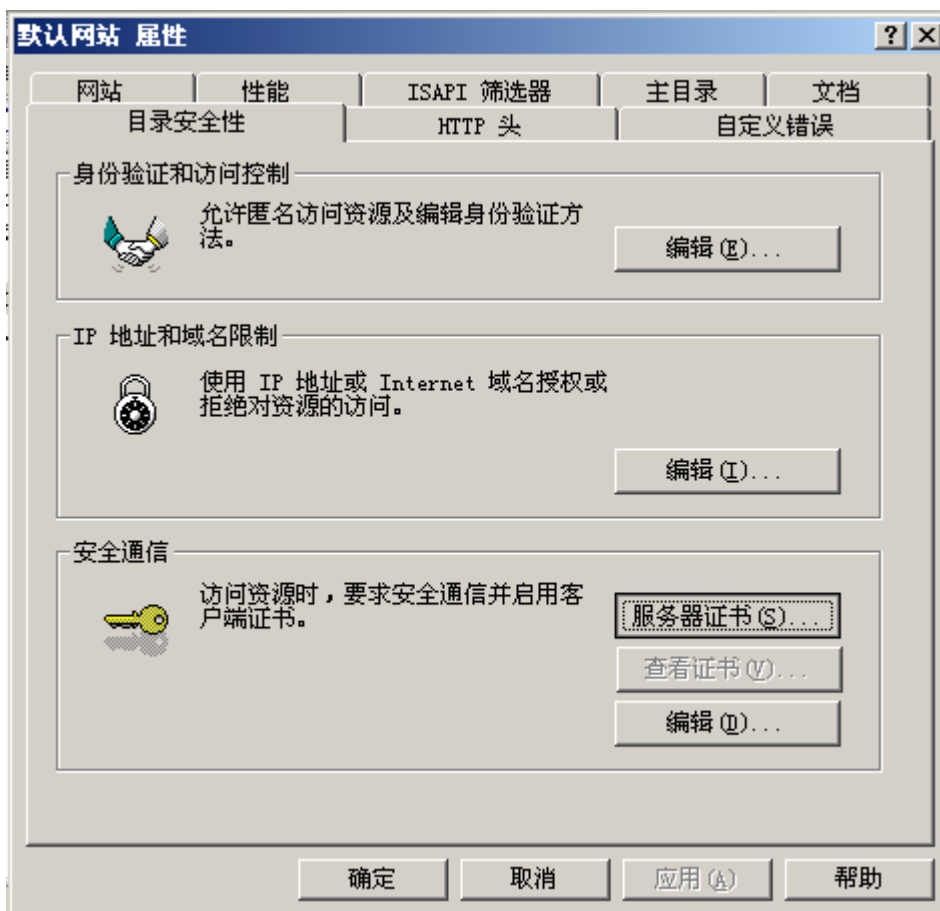
开始→程序→管理工具→Internet Information Services 管理



2、鼠标右键单击**默认 WEB 站点**，并在弹出菜单中选择**属性**

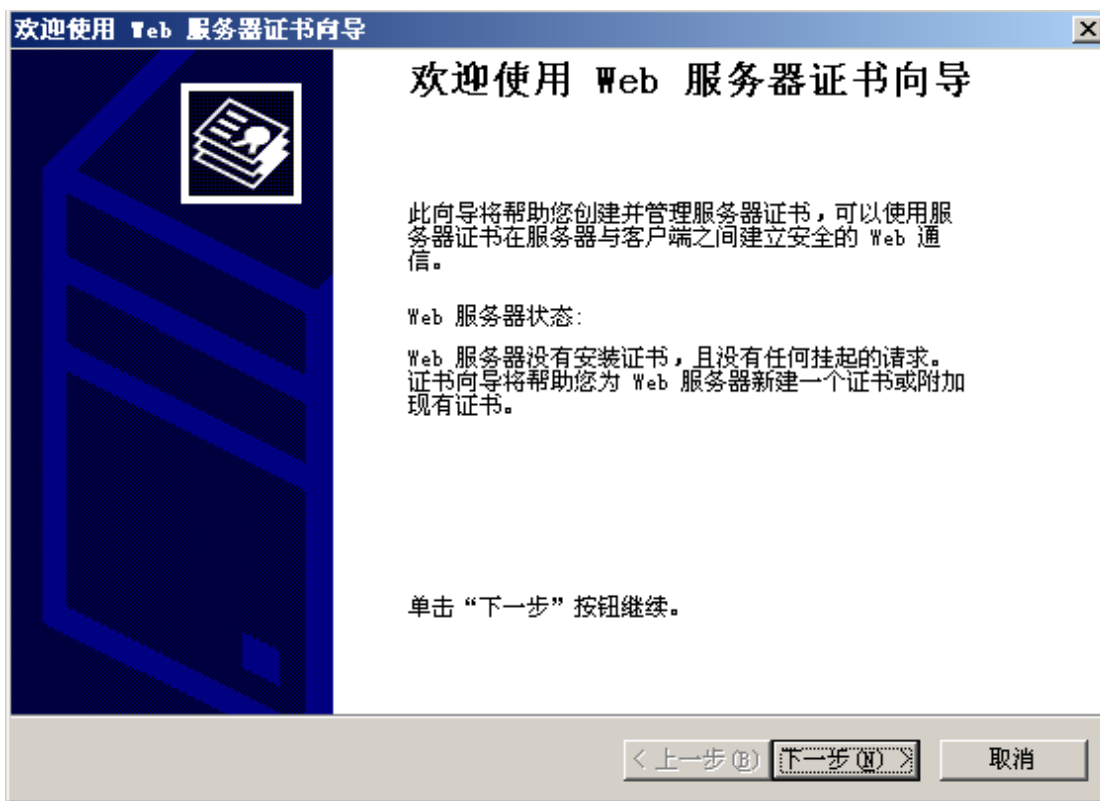


### 3、在默认 WEB 站点属性窗口选择目录安全性



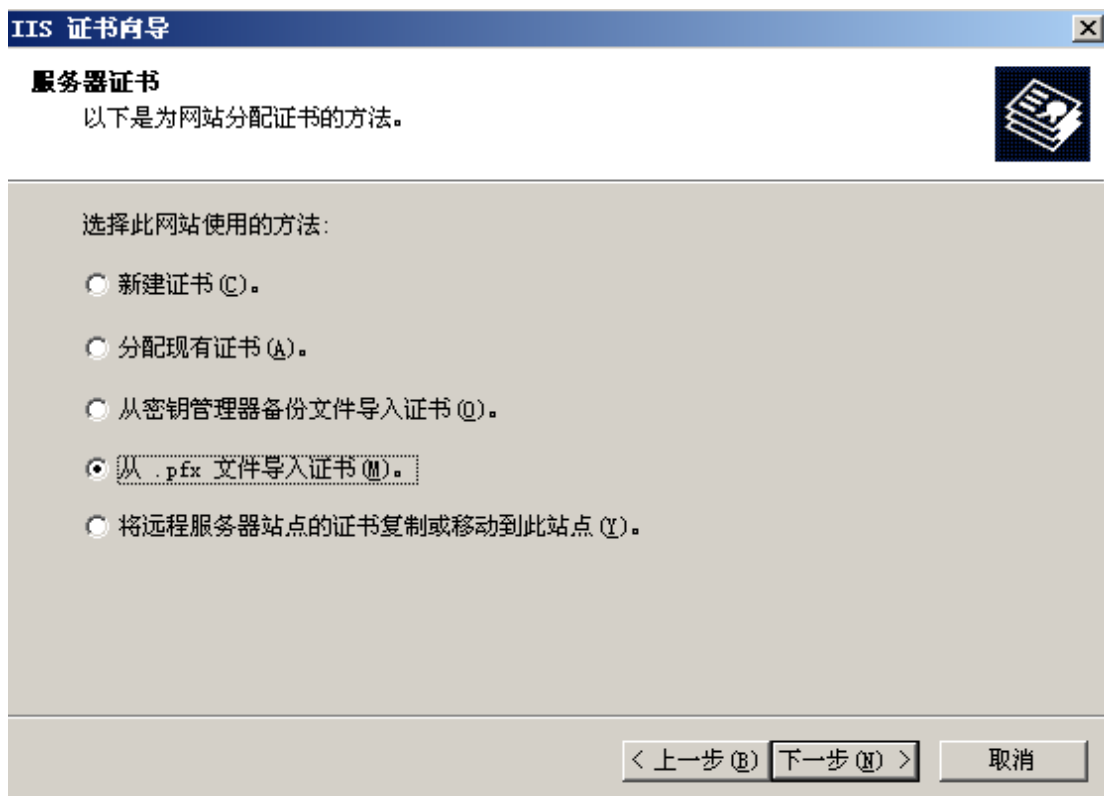


4、在安全通讯栏目中用鼠标点击服务器证书，出现 **WEB 服务器证书向导** 界面



5、单击下一步，出现 IIS 证书向导。这里分两种情况：

- a) 仅仅是重新安装了 IIS，或者丢失了 WEB 服务器证书：这时候我们可以选择指派一个已经存在本地容器里的证书
  
- b) 假如说您重新安装了您的 WINDOWS 操作系统，那还可以通过导入先前我们备份的 WEB 服务器证书.pfx 文件来恢复您的 WEB 服务器证书，所以我们这时候选择从一个.pfx 文件导入证书



为了便于以后导出（备份），请在标记证书可导出前打勾。

**IIS 证书向导**

**导入证书密码**  
必须提供密码才能导入证书。

输入要导入的证书的密码。

密码 (P):

< 上一步 (B) 下一步 (N) > 取消

输入您在先前导出 WEB 服务器证书时输入的.pfx 保护口令

**IIS 证书向导**

**SSL 端口**  
为此网站指定 SSL 端口。

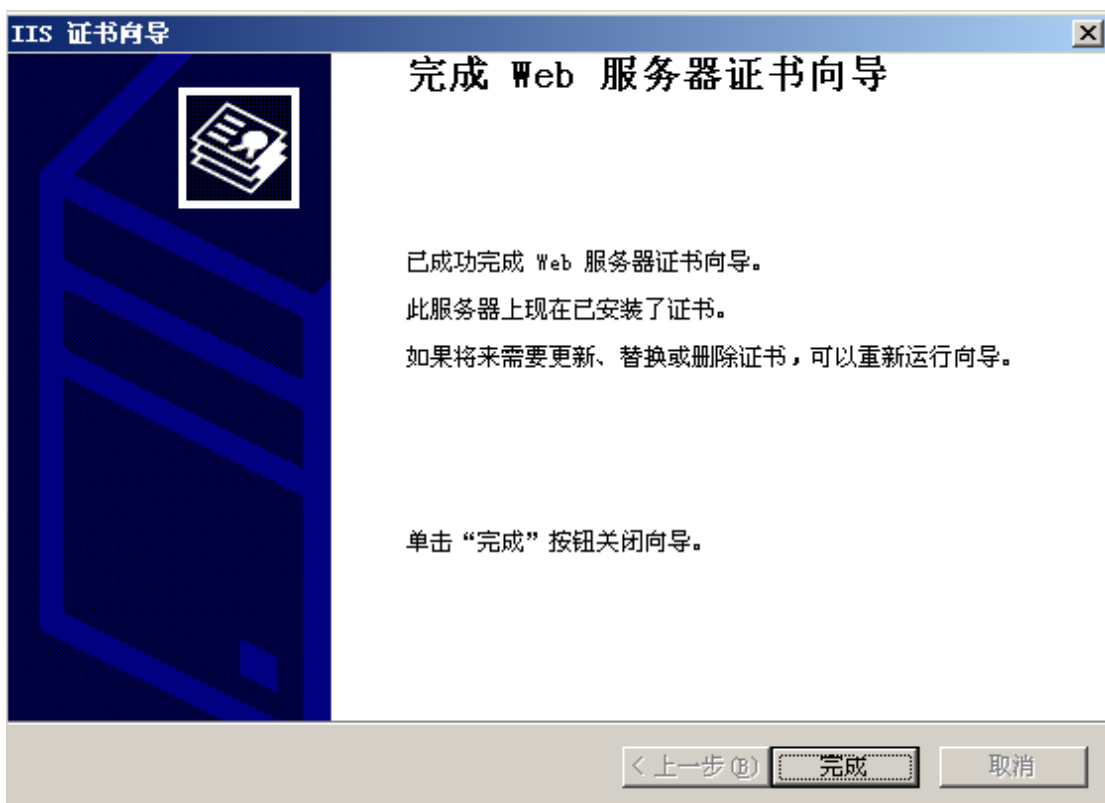
此网站应该使用的 SSL 端口 (L):

< 上一步 (B) 下一步 (N) > 取消

确认端口，默认是 443



请确认证书简要说明



完成证书导入（恢复）

## IIS 服务器的信任列表添加

在 SSL 双向认证中，假如客户端需要信任其他的根签发的证书，则需要做一下的配置：

- 1、点击“目录安全性”标签中的“编辑”按钮



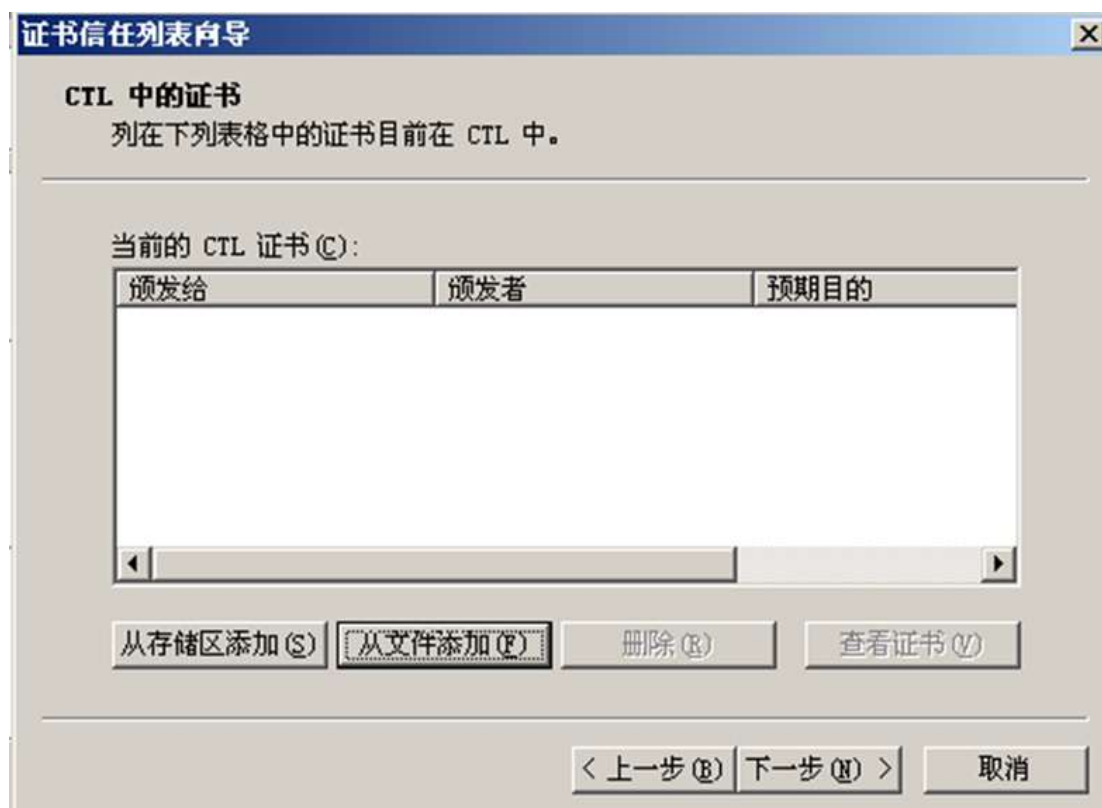
- 2、勾选“启用证书信任列表”并点击“新建”按钮



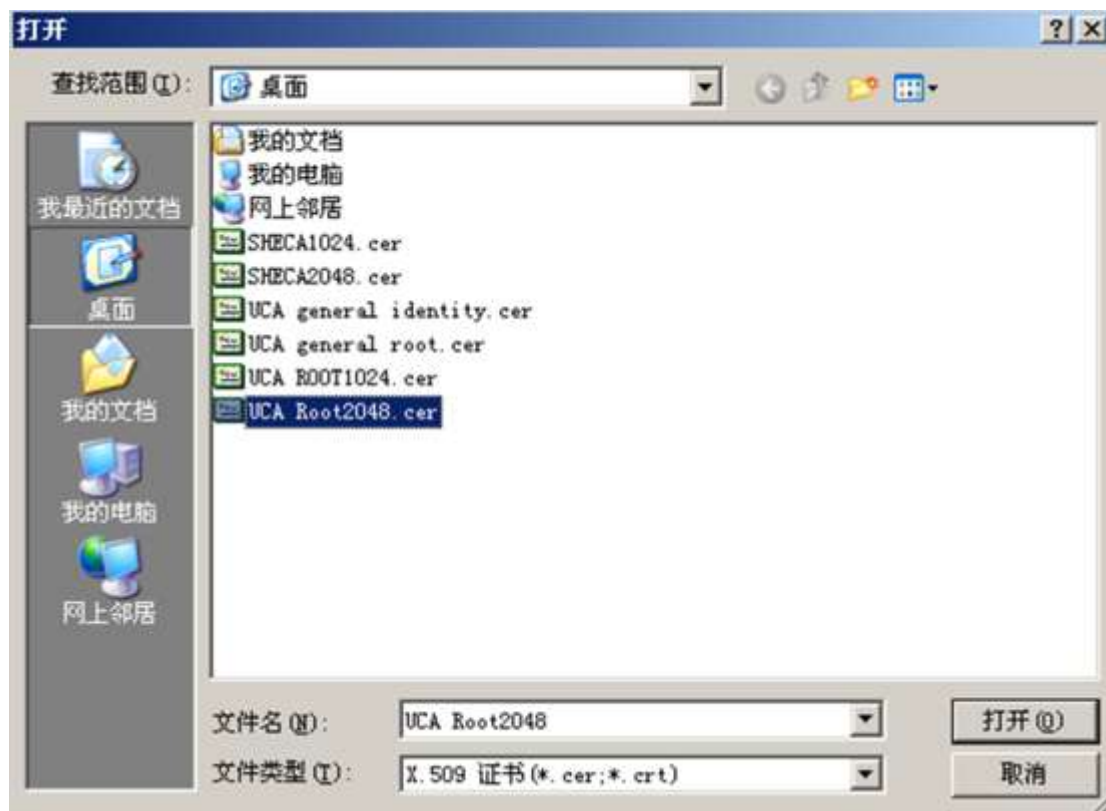
3、点击“下一步”



5、点击“从文件中添加”

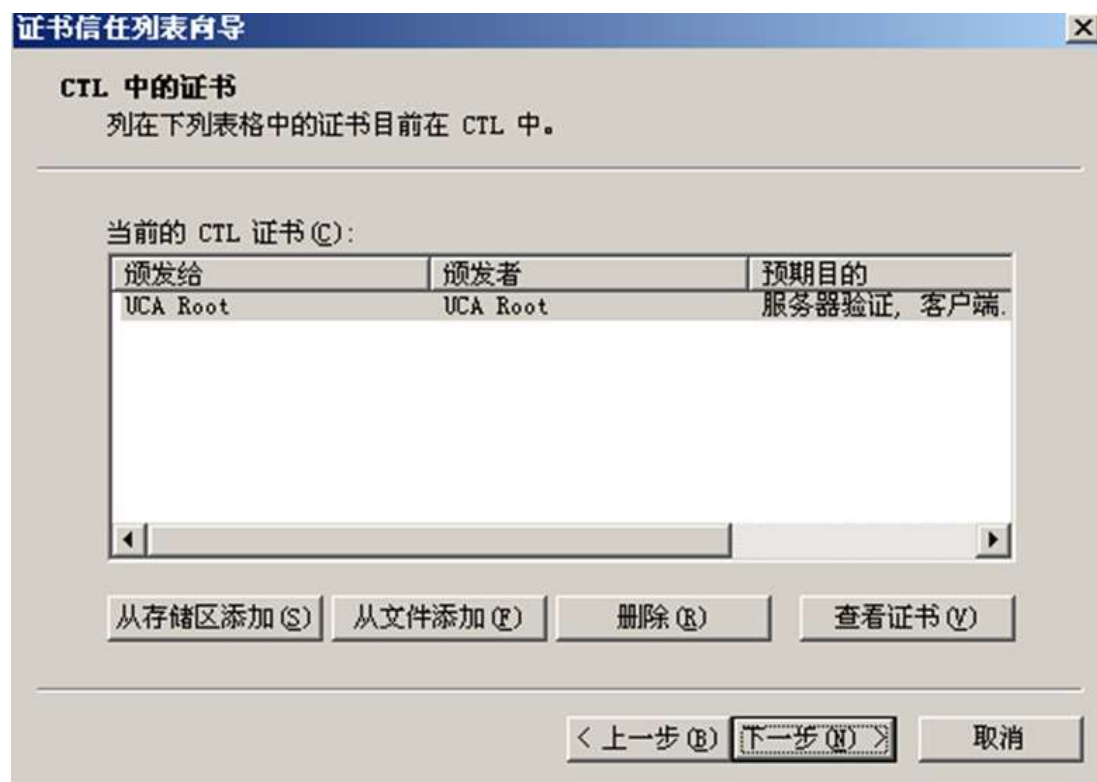


#### 6、选择你需要信任的根证书

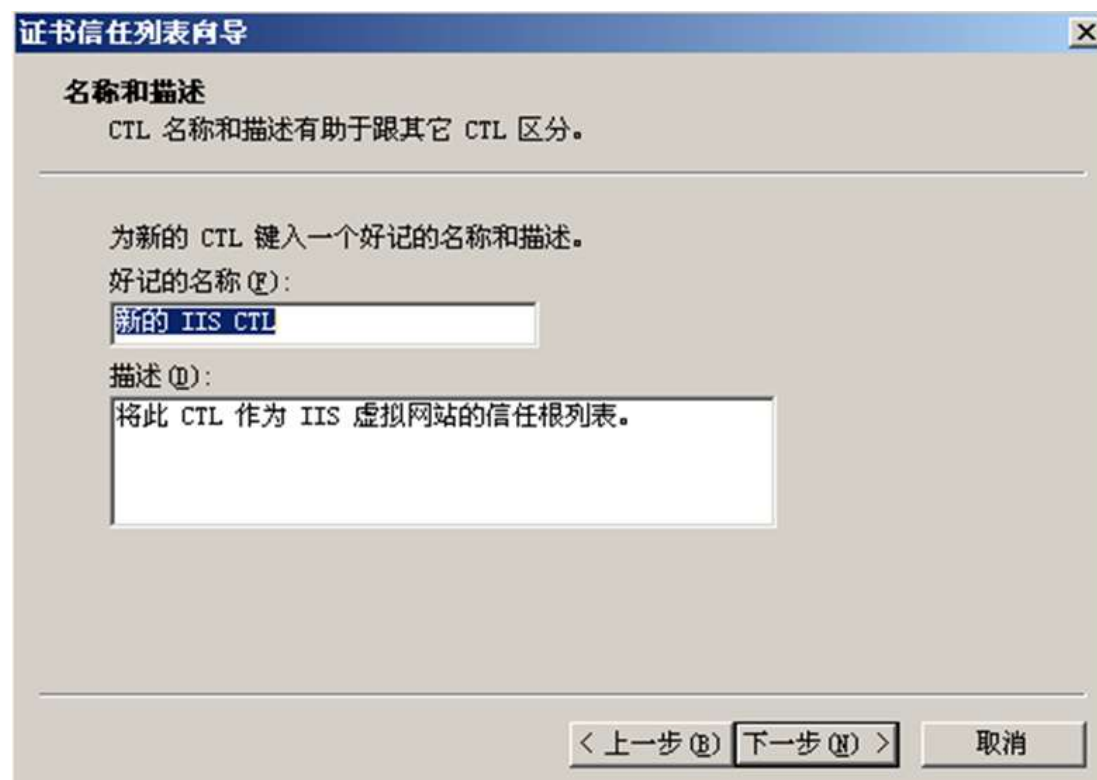


7、如图所示，在当前的 CTL 证书里面会有一个刚才添加的根证书，点击“下一步”继续。

如需信任多张根证书，只需重复步骤 5、6 的操作。



8、给新的 CTL 键入一个名称，并点击下一步继续

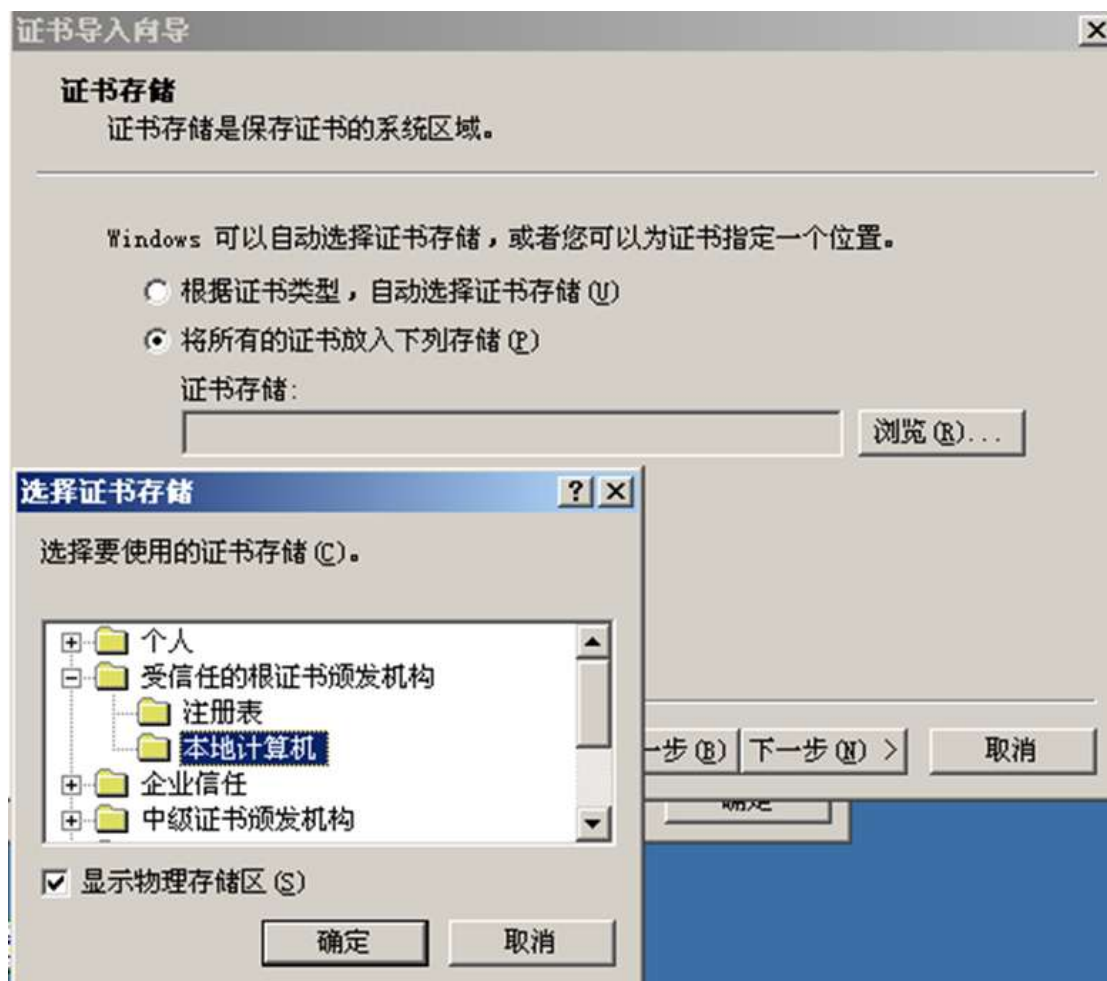




## 9、完成向导



- 10、 接下来,需要将您刚才添加到 CTL 的根证书以及对应的中级证书安装到你的服务器中的本地计算机中,如下图所示



11、安装成功后，重启服务器即可测试添加到 CTL 中的根证书颁发的客户端证书是否可以访问服务器。