

目录

目录	1
导出证书信息	2
前提条件	2
操作步骤	2
导出文件中包含哪些证书信息	2
Apache	2
前提条件	2
获取证书文件	2
安装证书文件	3
效果验证	3
IIS7	3
前提条件	3
获取证书文件	3
安装证书文件	3
中级证书导入-安装服务器证书中级CA证书	3
导入服务器证书	7
Apache for Linux	9
前提条件	9
安装准备	9
下载OpenSSL	9
安装Apache	9
安装服务器证书	9
获取服务器证书	9
获取CA证书	9
配置Apache	9
服务器证书的备份及恢复	10
服务器证书的备份	10
服务器证书的恢复	10
Nginx	10
前提条件	10
获取证书文件	10
安装服务器证书	10
Tomcat	11
下载证书文件	11
JKS证书安装	11
配置Tomcat	11
访问测试	11
IIS6	11
前提条件	11
安装中级CA证书	11
获取服务器证书中级CA证书	11
安装服务器证书中级CA证书	11
删除一张服务端(EV)根证书	13
安装服务器证书	13
保存服务器证书	13
进入IIS控制台	14
服务器证书的备份及恢复	14
服务器证书的备份	15
服务器证书的恢复	15

导出证书信息

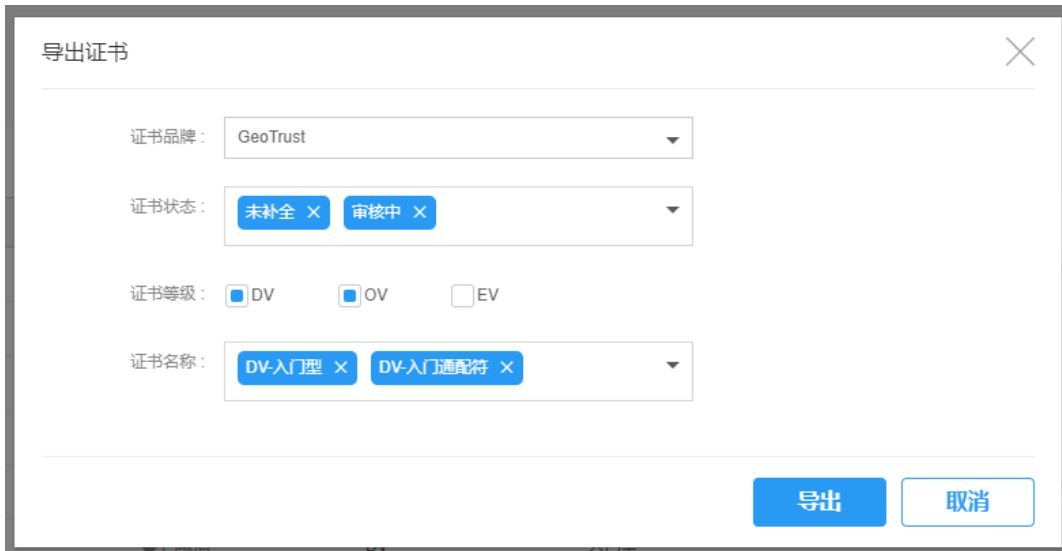
针对用户因持有证书量较大，不便在控制台对所购证书进行统一管理和信息查询这一场景，金山云SSL证书管理支持用户在控制台批量导出所选证书，方便用户管理和查询证书信息。

前提条件

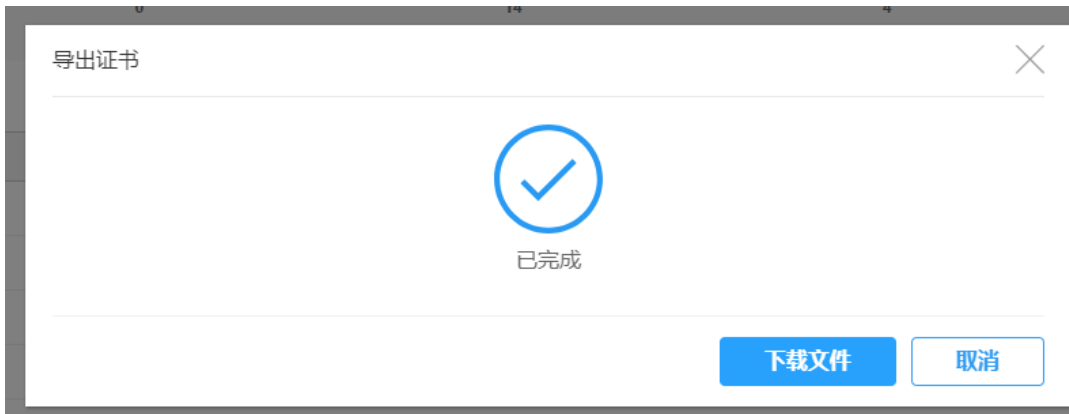
您已购买至少一本SSL证书。

操作步骤

1. 登录[金山云SSL证书管理控制台](#)。
2. 点击证书列表上方的**导出**按钮。
3. 在**导出证书**对话框中，按条件筛选需导出的证书。证书品牌为单选，证书状态、证书等级、证书名称均可多选。



4. 点击对话框中的**导出**按钮，等待导出结束
5. 点击**下载文件**按钮，将excel文件下载到本地。



导出文件中包含哪些证书信息

打开导出完成的excel文件，字段包括证书ID、证书绑定主域名、证书品牌、证书等级、证书类型、域名个数、通配符个数、通配符域名、证书签发日期、证书到期时间、证书状态、证书年限、附加域名、申请人姓名、申请人邮箱和申请人电话的信息。

Apache

本文档介绍如何将证书安装到Apache服务器上。若您使用的是Apache服务器，请阅读本文档内容，完成安装操作。

前提条件

1. 证书状态为“已签发”。
2. 已获取证书文件压缩包。

获取证书文件

1. 在本地解压已下载的证书文件，解压后获得 .key 和 .pem 文件。
2. 将pem文件使用记事本打开，将第一段编码内容（包括“-----BEGIN CERTIFICATE-----”和“-----END CERTIFICATE-----”）粘贴到记事本

等文本编辑器中，保存为server.crt文件。

3. 将剩余部分（包括“-----BEGIN CERTIFICATE-----”和“-----END CERTIFICATE-----”）粘贴到记事本等文本编辑器中，保存为ca.crt文件。

安装证书文件

1. 将制作完成的“.key”文件和“server.crt”文件、“ca.crt”文件复制到apache的conf目录下
2. 打开Apache安装目录下conf目录中的“httpd.conf”文件，找到如下参数

```
#LoadModule ssl_module modules/mod_ssl.so
```

3. 删除行首的配置语句注释符号“#”
4. 修改后，保存“httpd.conf”文件并退出编辑。
5. 打开Apache安装目录下conf目录中的“ssl.conf”文件，查到“LoadModule ssl_module”如下：

```
#LoadModule ssl_module modules/mod_ssl.so
#include conf/extra/httpd_ssl.conf
```

6. 删除行首的配置语句注释符号“#”
7. 修改后，保存“ssl.conf”文件并退出编辑。
8. 打开Apache安装目录下conf/extra目录中的httpd-ssl.conf（或conf目录中的ssl.conf）文件，在配置文件中的 <VirtualHost *:443>……</VirtualHost> 之间添加或编辑如下配置项

```
SSLProtocol all -SSLv2 -SSLv3 #openssl的版本建议使用 1.0.0, 1.0.1, 1.0.2 最新版本
SSLHonorCipherOrder on
SSLCipherSuite HIGH:!RC4:!MD5:!aNULL:!eNULL:!NULL:!DH:!EDH:!EXP:+MEDIUM
SSLCertificateFile conf/server.crt #将服务器证书配置到该路径下
SSLCertificateKeyFile conf/server.key #将服务器证书私钥配置到该路径下
#SSLCertificateChainFile conf/ca.crt #删除行首的“#”号注释符，并将CA证书ca.crt配置到该路径下
```

9. 保存退出，并重启Apache。
10. 重启方式：进入Apache安装目录下的bin目录，运行如下命令

```
./apachectl -k stop
./apachectl -k start
```

效果验证

通过https方式访问您的站点，部署成功后，可在浏览器的地址栏中输入“<https://域名>”，如果浏览器地址栏显示安全锁标识，则说明证书安装成功。

IIS7

本文档介绍如何将证书安装到IIS7服务器上。若您使用的是IIS7服务器，请阅读本文档内容，完成安装操作。

前提条件

1. 证书状态为“已签发”。
2. 已获取证书文件压缩包。

获取证书文件

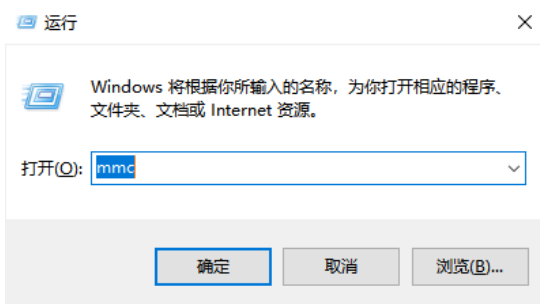
1. 在本地解压已下载的证书文件，解压后获得 .pfx文件和.pem文件。
2. 将pem文件使用记事本打开，将第二段证书编码内容（包括“-----BEGIN CERTIFICATE-----”和“-----END CERTIFICATE-----”）粘贴到记事本等文本编辑器中，保存为intermediate.cer文件。

安装证书文件

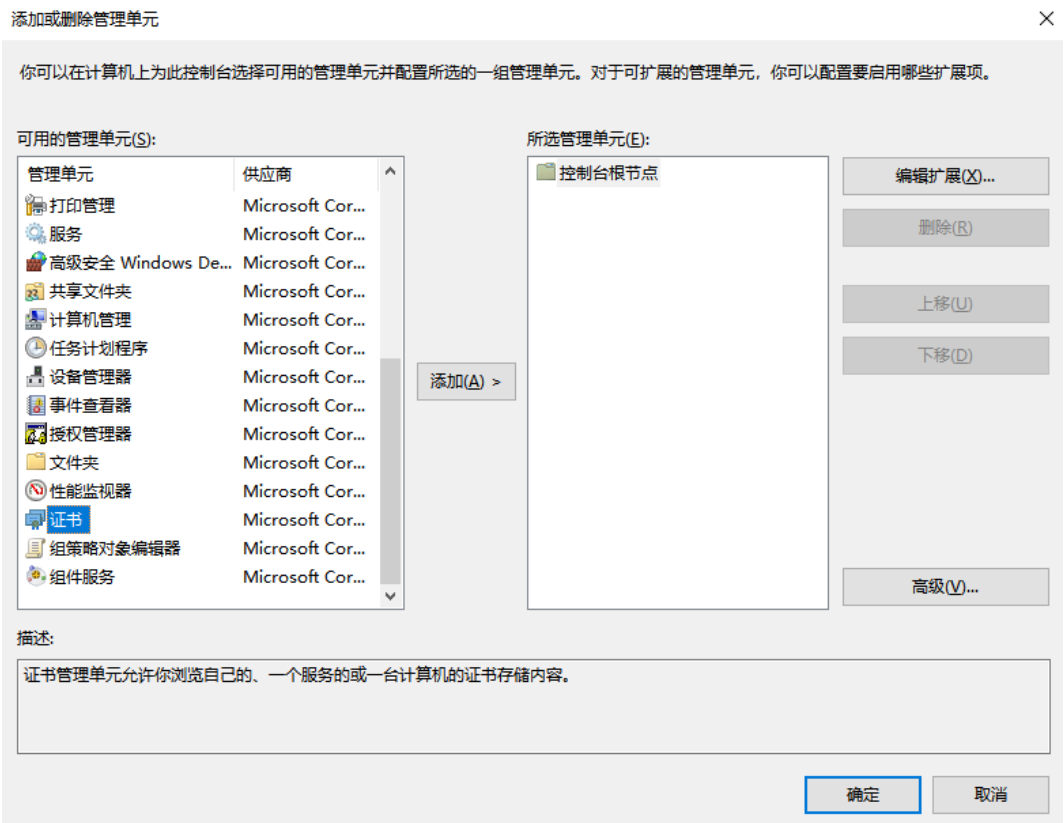
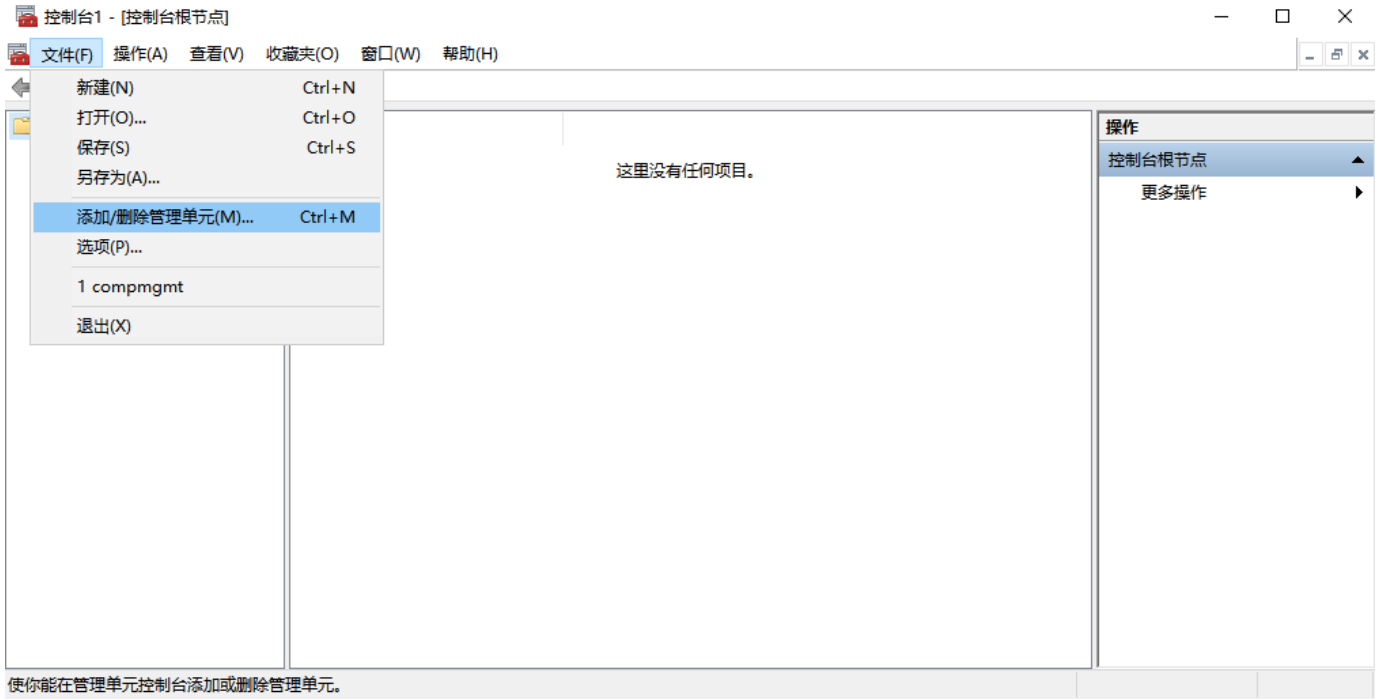
pfx格式文件包含了服务器证书（公钥）及私钥信息，可直接导入到IIS中。cer文件是中间级CA证书文件，需要导入到iis证书管理系统。

中级证书导入-安装服务器证书中级CA证书

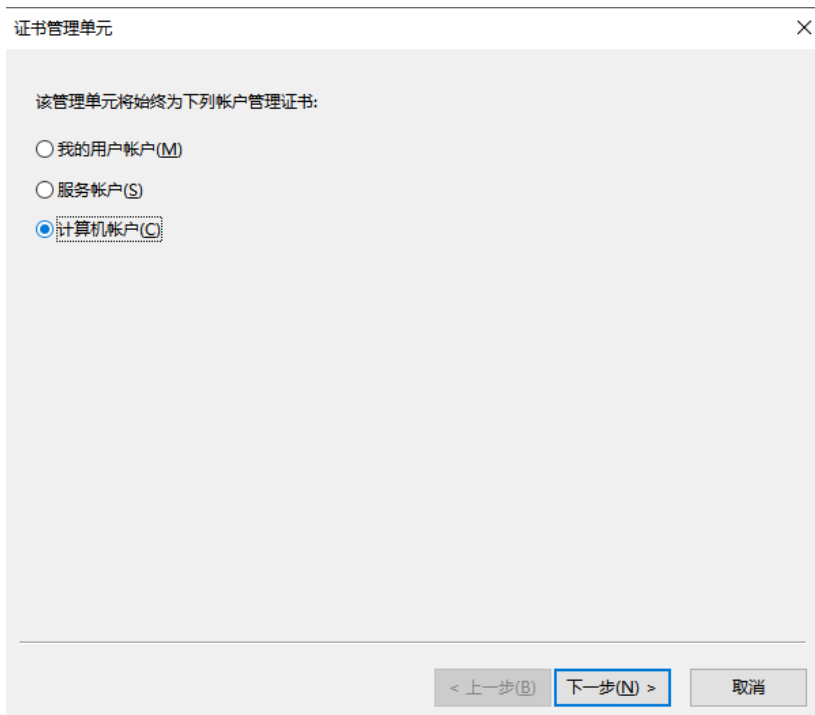
1. 点击开始菜单，在“运行”中输入“mmc”，打开控制台窗口。



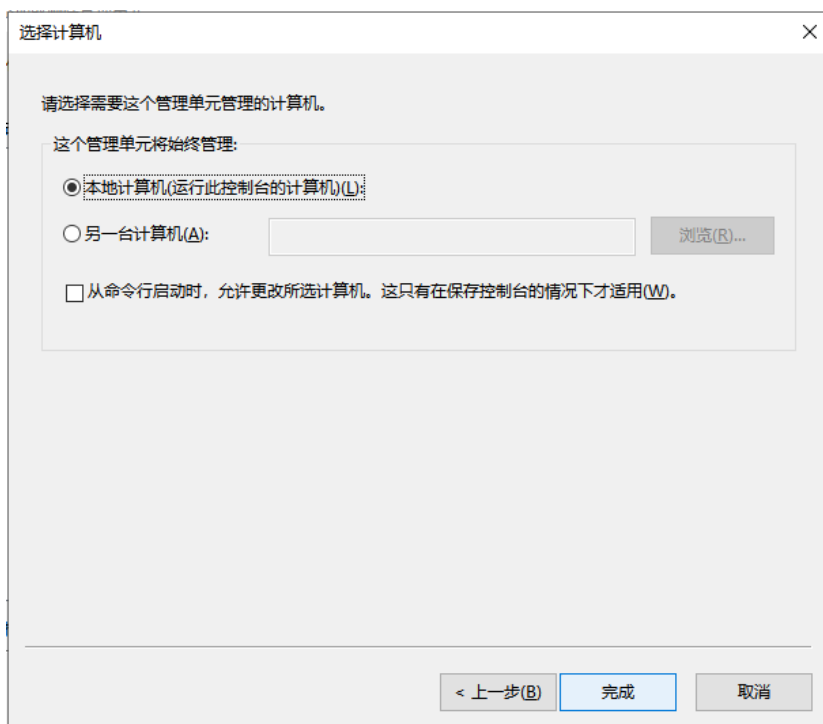
2. 点击文件 > 添加删除管理单元。



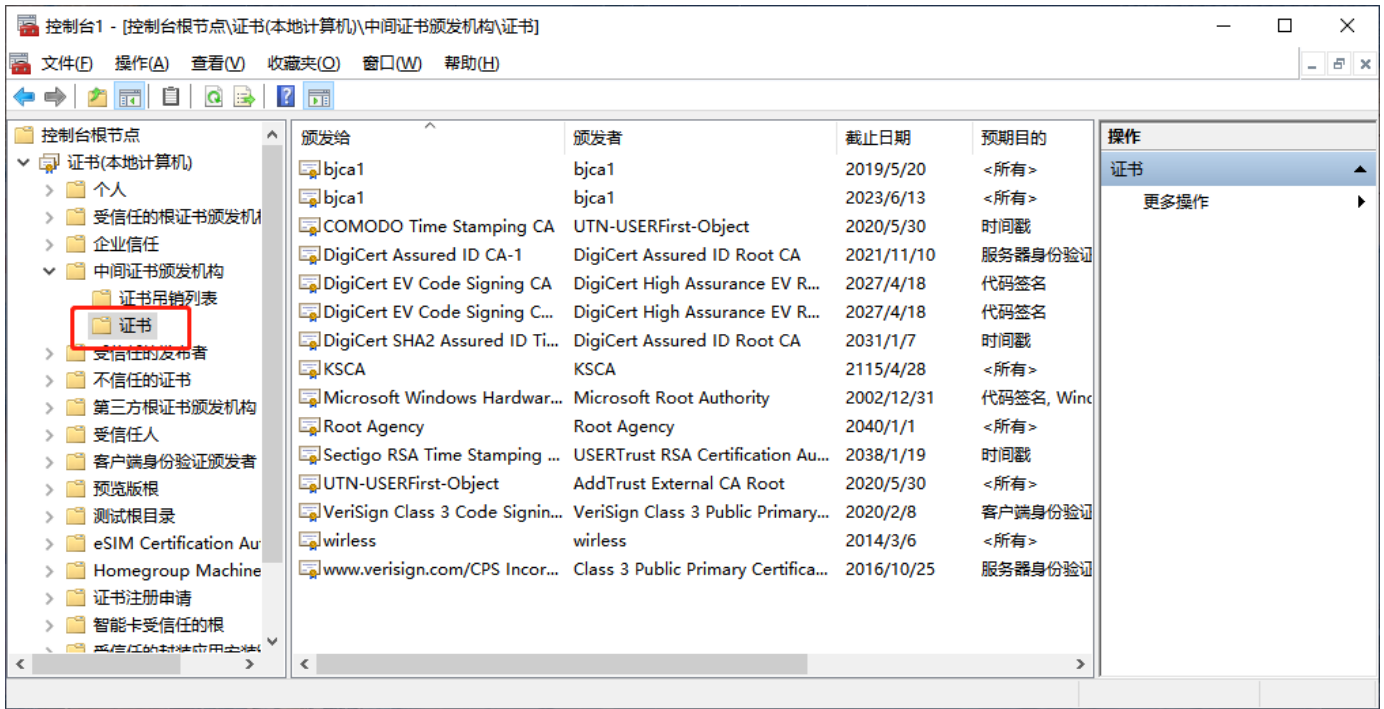
3. 找到证书，点击添加。
4. 选择计算机账户，点击下一步。



5. 点击完成。



6. 点击证书(本地计算机) > 中级证书颁发机构 > 证书。



7. 在空白处单击鼠标右键，选择所有任务 > 导入。

← 证书导入向导

欢迎使用证书导入向导

该向导可帮助你将证书、证书信任列表和证书吊销列表从磁盘复制到证书存储。

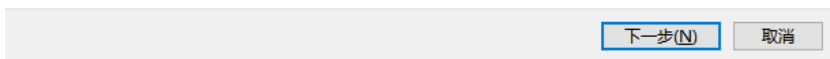
由证书颁发机构颁发的证书是对你身份的确认，它包含用来保护数据或建立安全网络连接的信息。证书存储是保存证书的系统区域。

存储位置

当前用户(C)

本地计算机(L)

单击“下一步”继续。



8. 通过证书向导导入中级证书cer文件。

← 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\Administrator\Desktop\intermediatel.cer

浏览(B)...

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)

Microsoft 系列证书存储(.SST)

下一步(N)

取消

9. 选择将所有的证书放入下列存储，点击下一步，点击完成。

×

← 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。

根据证书类型，自动选择证书存储(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

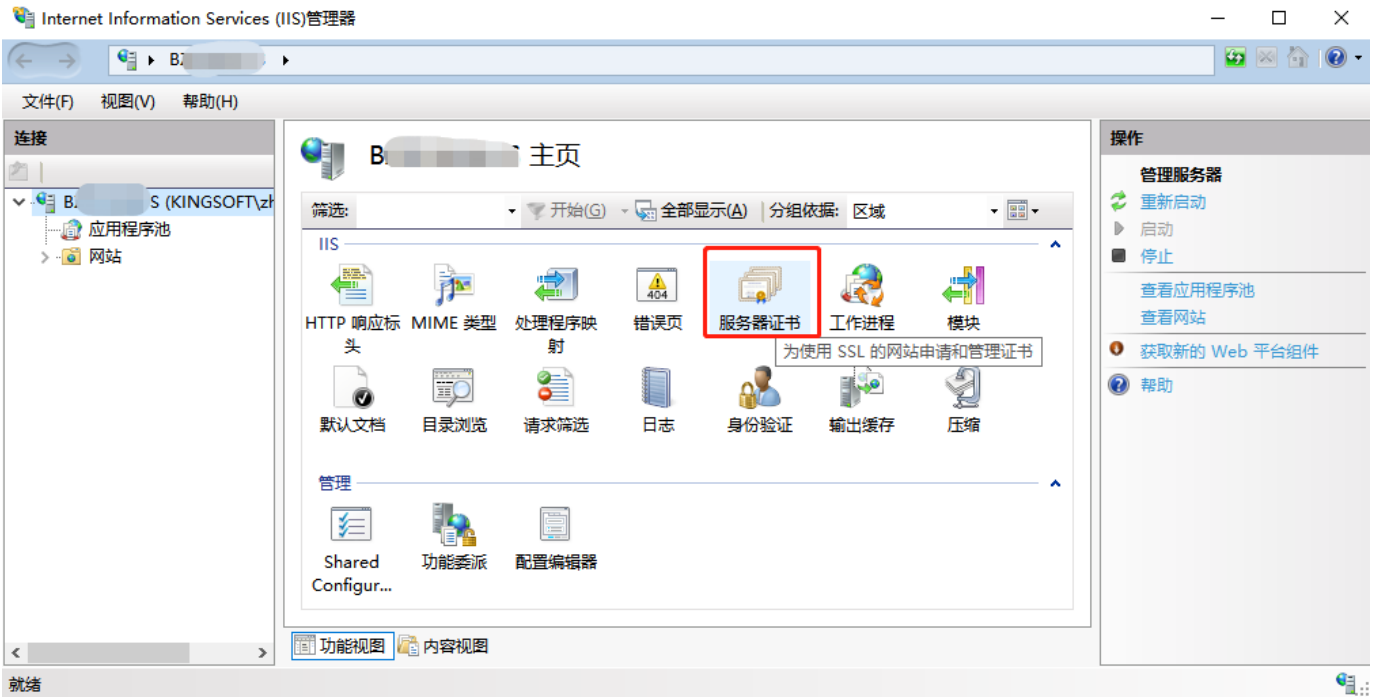
浏览(B)...

下一步(N)

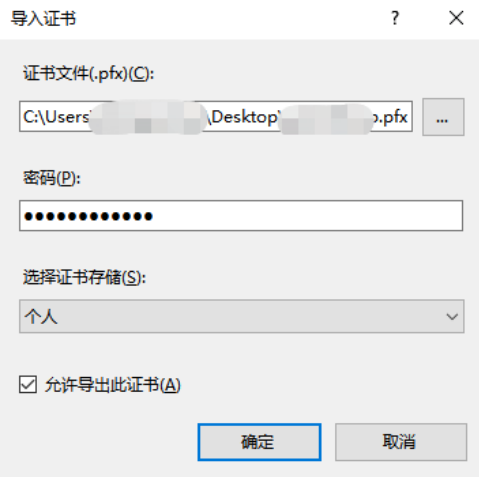
取消

导入服务器证书

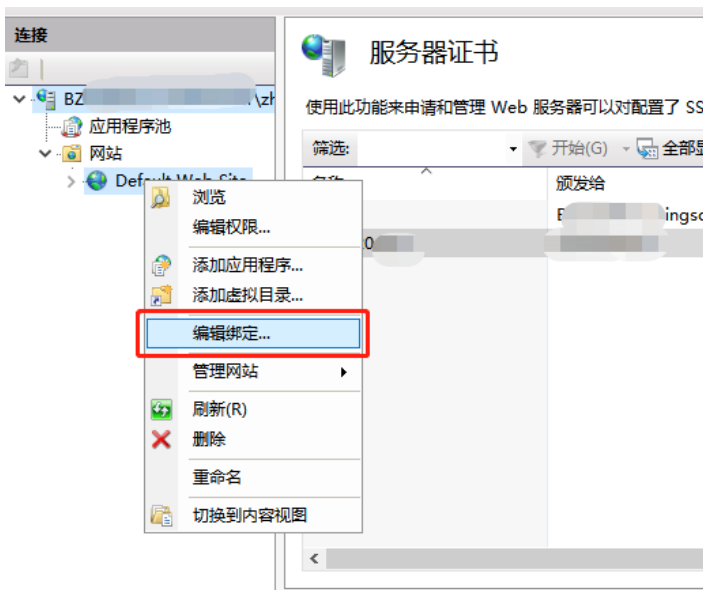
1. 打开IIS管理控制台，双击服务器证书，进入服务器证书管理界面。



2. 右击空白处选择导入证书，并输入PFX文件密码。



3. 鼠标右键单击目标站点（这里以默认站点为例），选择编辑绑定，为站点分配证书服务。



4. 在弹出的窗口中，单击添加，并填写以下信息。

5. 完成后重启IIS站点，并使用https方式访问测试站点证书安装

Apache for Linux

本文档介绍如何将证书安装到Apache for Linux服务器上，若您使用的是Apache for Linux服务器，请阅读本文档内容，完成安装操作。

前提条件

1. 证书状态为“已签发”。
2. 已获取证书文件压缩包。

安装准备

下载OpenSSL

要使Apache支持SSL，需安装OpenSSL，下载地址：<http://www.openssl.org/source/>

```
tar -zxf openssl-1.*.**.tar.gz //解压安装包
cd openssl-1.*.** //进入已经解压的安装包
./config //配置安装。推荐使用默认配置
make && make install
```

OpenSSL默认安装路径为：/usr/local/ssl

安装Apache

```
./configure --prefix=/usr/local/apache --enable-so --enable-ssl --with-ssl=/usr/local/ssl --enable-mods-shared=all
//配置安装。推荐动态编译模块
make && make install
```

动态编译Apache模块，便于模块的加载管理。Apache 将被安装到/usr/local/apache

安装服务器证书

获取服务器证书

将证书签发文件中的从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，保存为server.crt文件。

获取CA证书

将证书签发文件中的从BEGIN到END结束的两张CA证书内容（包括“-----BEGIN CERTIFICATE-----”和“-----END CERTIFICATE-----”）粘贴到同一个记事本等文本编辑器中，两张证书中间用回车换行不留空行分隔。修改文件扩展名，保存为ca.crt文件(如果只有一张CA证书，则只需要保存一张CA证书)。

配置Apache

1. 打开apache安装目录下conf目录中的httpd.conf文件，找到

```
#LoadModule ssl_module modules/mod_ssl.so
```

2. 删除行首的配置语句注释符号“#”。

- 保存退出。
- 打开apache安装目录下conf目录中的ssl.conf文件，查到“LoadModule ssl_module”如下：

```
#LoadModule ssl_module modules/mod_ssl.so
#include conf/extra/httpd_ssl.conf
```

- 删除行首的配置语句注释符号“#”。
- 保存退出。
- 打开apache安装目录下conf/extra目录中的httpd-ssl.conf（或conf目录中的ssl.conf）文件，在配置文件中的<VirtualHost *:443>……</VirtualHost>之间添加或编辑如下配置项

```
SSLProtocol all -SSLv2 -SSLv3
SSLHonorCipherOrder on
SSLCipherSuite HIGH:!RC4:!MD5:!aNULL:!eNULL:!NULL:!DH:!EDH:!EXP:+MEDIUM
SSLCertificateFile conf/server.crt      将服务器证书配置到该路径下
SSLCertificateKeyFile conf/server.key    将服务器证书私钥配置到该路径下
#SSLCertificateChainFile conf/ca.crt     删除行首的“#”号注释符，并将CA证书ca.crt配置到该路径下
```

- 保存退出。
- 重启Apache，重启方式如下：

进入Apache安装目录下的bin目录，运行如下命令

```
./apachectl -k stop
./apachectl -k start
```

- 通过https方式访问您的站点，测试站点证书的安装配置。

服务器证书的备份及恢复

在您成功的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。

服务器证书的备份

备份服务器证书私钥文件server.key，服务器证书文件server.crt，以及服务器证书CA证书文件ca.crt即可完成服务器证书的备份操作。

服务器证书的恢复

请参照服务器证书配置部分，将服务器证书密钥文件恢复到您的服务器上，并修改配置文件，恢复服务器证书的应用。

Nginx

本文档介绍如何将证书安装到Nginx服务器上。若您使用的是Nginx服务器，请阅读本文档内容，完成安装操作。

前提条件

- 证书状态为“已签发”。
- 已获取证书文件压缩包。

获取证书文件

在本地解压已下载的证书文件，解压后获得.key 和 .pem 文件。

安装服务器证书

- 复制server.key、server.pem文件到Nginx安装目录下的conf目录。
- 打开Nginx安装目录下conf目录中的nginx.conf文件，找到如下参数：

```
# HTTPS server
#
#server {
#    listen      443;
#    server_name localhost;
#    ssl         on;
#    ssl_certificate    cert.pem;
#    ssl_certificate_key    cert.key;
#    ssl_session_timeout    5m;
#    ssl_protocols    SSLv2 SSLv3 TLSv1;
#    ssl_ciphers    ALL:!ADH:!EXPORT56:RC4+RSA:+HIGH:+MEDIUM:+LOW:+SSLv2:+EXP;
#    ssl_prefer_server_ciphers    on;
#    location / {
#        root    html;
#        index    index.html index.htm;
#    }
#}
```

- 删除行首的配置语句注释符号#，并将其修改为：

```
server {
    listen      443;
    server_name localhost;
    ssl         on;
    ssl_certificate    server.pem;
```

```

ssl_certificate_key server.key;
ssl_session_timeout 5m;
ssl_protocols TLSv1 TLSv1.1 TLSv1.2;
#启用TLS1.1、TLS1.2要求OpenSSL.0.1及以上版本，openssl的版本建议使用1.0.1、1.0.2 最新版本;
ssl_ciphers HIGH:!RC4:!MD5:!aNULL:!eNULL:!NULL:!DH:!EDH:!EXP:+MEDIUM;
ssl_prefer_server_ciphers on;
location / {
    root html;
    index index.html index.htm;
}
}

```

4. 保存退出，并重启Nginx。
5. 通过https方式访问您的站点，测试站点证书的安装配置。

Tomcat

下载证书文件

从金山云证书管理控制台下载证书文件包，解压后获得.jks的文件。

JKS证书安装

配置Tomcat

复制keystore.jks文件到Tomcat安装目录下的conf目录。打开conf目录下的server.xml文件，找到并修改以下内容

```

<Connector port="8080" protocol="HTTP/1.1"
    connectionTimeout="20000"
    redirectPort="8443" />

```

修改为

```

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

```

```

<!--
    <Connector protocol="org.apache.coyote.http11.Http11Protocol"
        port="8443" SSLEnabled="true"
        maxThreads="150" scheme="https" secure="true"
        clientAuth="false" sslProtocol="TLS" />
-->

```

修改为

```

<Connector protocol="org.apache.coyote.http11.Http11Protocol"
    port="443" SSLEnabled="true"
    maxThreads="150" scheme="https" secure="true"
    keystoreFile="conf\keystore.jks" keystorePass="JKS文件密码"
    clientAuth="false" sslProtocol="TLS"
ciphers="TLS_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_AES_256_CBC_SHA,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,TLS_RSA_W
ITH_AES_128_CBC_SHA256,TLS_RSA_WITH_AES_256_CBC_SHA256"/>

```

默认的SSL访问端口号为443，如果使用其他端口号，则您需要使用https://yourdomain:port的方式来访问您的站点。

访问测试

重启Tomcat，访问https://yourdomain:port，测试证书的安装。

IIS6

本文档介绍如何将证书安装到IIS6服务器上。若您使用的是IIS6服务器，请阅读本文档内容，完成安装操作。

前提条件

1. 证书状态为“已签发”。
2. 已获取证书文件压缩包。

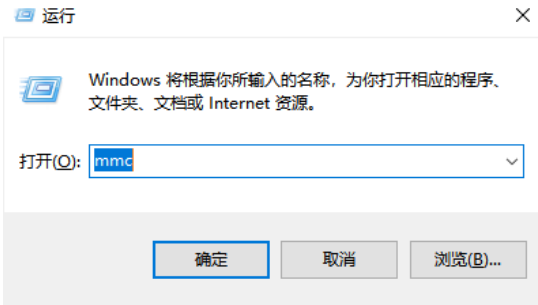
安装中级CA证书

获取服务器证书中级CA证书

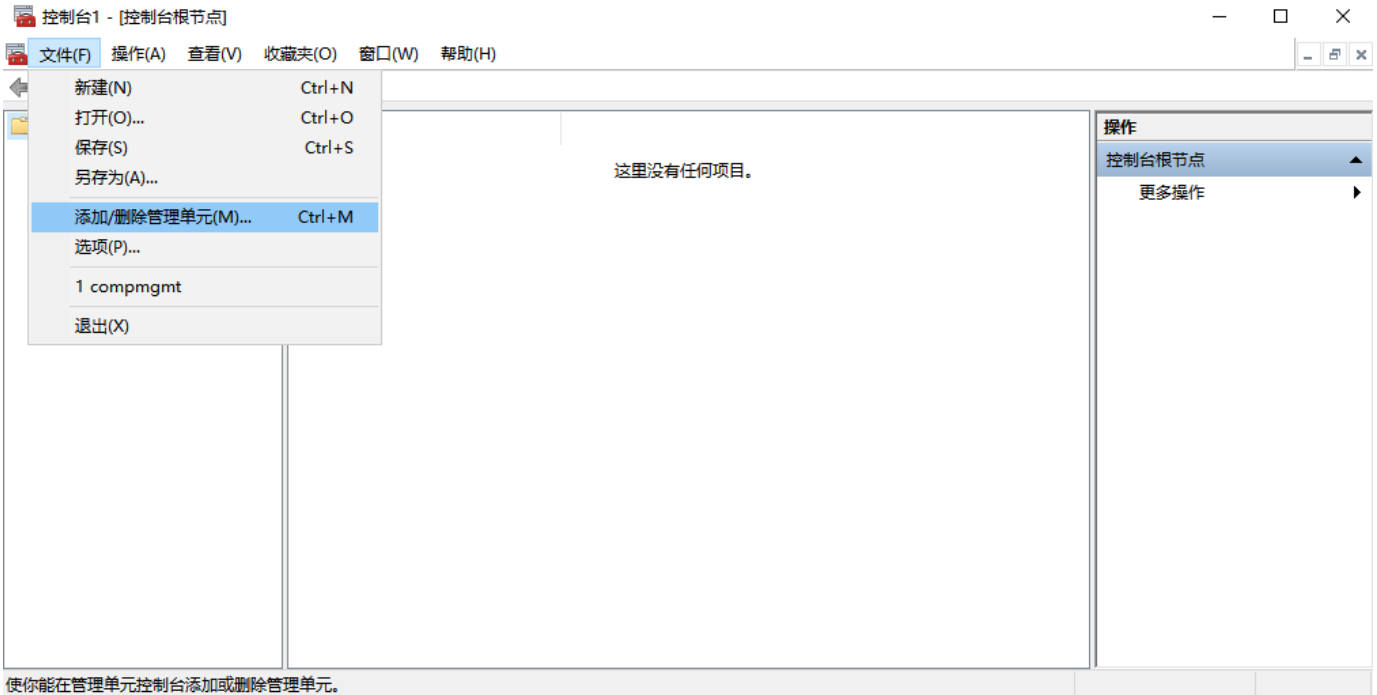
- 为保障服务器证书在客户端的兼容性，服务器证书需要安装两张中级CA证书(首先安装中间CA证书，安装成功后再安装服务器证书，请注意中级CA证书与服务器证书安装的先后顺序；不同品牌证书，可能只有一张中级证书)。
- 将pem文件使用记事本打开，将从BEGIN到 END结束的两张中级CA证书内容(包括“-----BEGIN CERTIFICATE-----”和“-----END CERTIFICATE-----”)分别粘贴到记事本等文本编辑器中，并修改文件扩展名，保存为intermediate1.cer和intermediate2.cer文件(如果只有一张中级证书，则只需保存并安装一张即可)。

安装服务器证书中级CA证书

1. 点击开始菜单，在“运行”中输入“mmc”，打开控制台窗口。

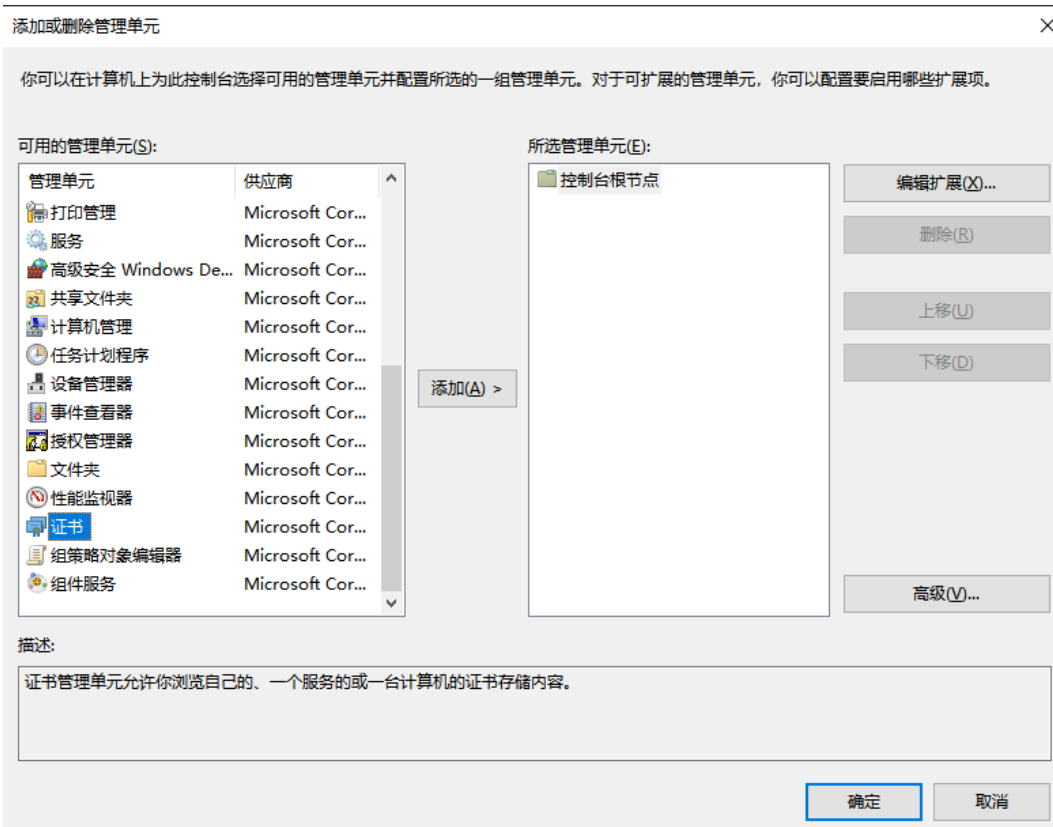


2. 点击文件 > 添加删除管理单元。

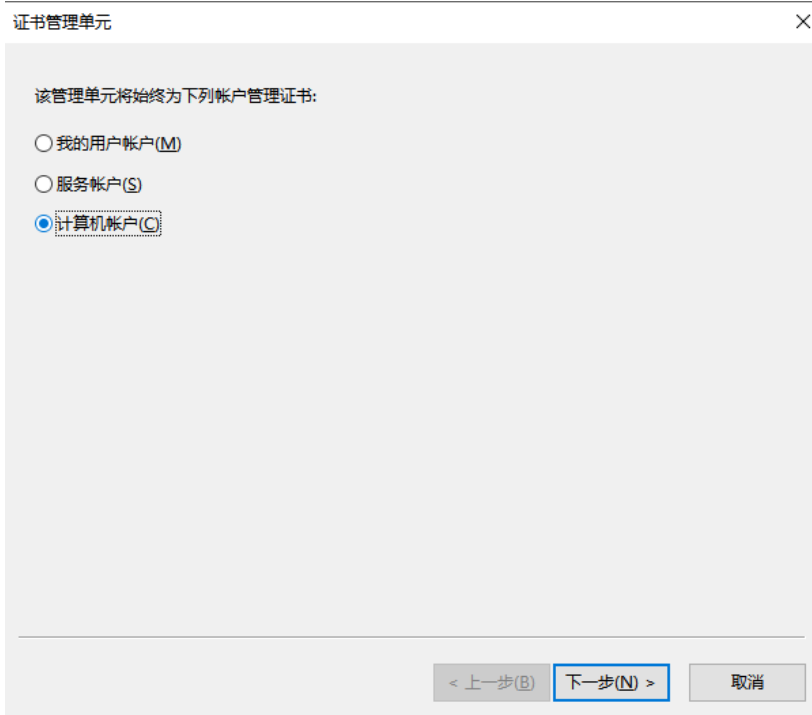


使你能在管理单元控制台添加或删除管理单元。

3. 选择证书，然后点击添加。



4. 选择计算机帐户，点击下一步。



6. 在添加的证书管理单元中，点击中级证书颁发机构 > 证书。



7. 在空白处单击鼠标右键，选择所有任务 > 导入，将两张中级CA证书intermediate1.cer和intermediate2.cer分别导入。

删除一张服务端 (EV) 根证书

在IIS上安装服务器证书，需要检查服务器上是否存在一张(EV)服务器证书根证书。如果存在，需要删除该证书，否则客户端IE7以下客户端将访问报错。

- 选择证书 > 受信任的根证书颁发机构 > 证书。检查其中是否存在名称为“VeriSign Class 3 Public Primary Certification Authority - G5”有效期 2006-11-8 到 2036-7-17的证书，如果存在，请删除该证书。
- 选择证书 > 第三方根证书颁发机构 > 证书 检查其中是否存在名称为“VeriSign Class 3 Public Primary Certification Authority - G5”有效期 2006-11-27 到 2036-7-17的证书，如果存在，请删除该证书

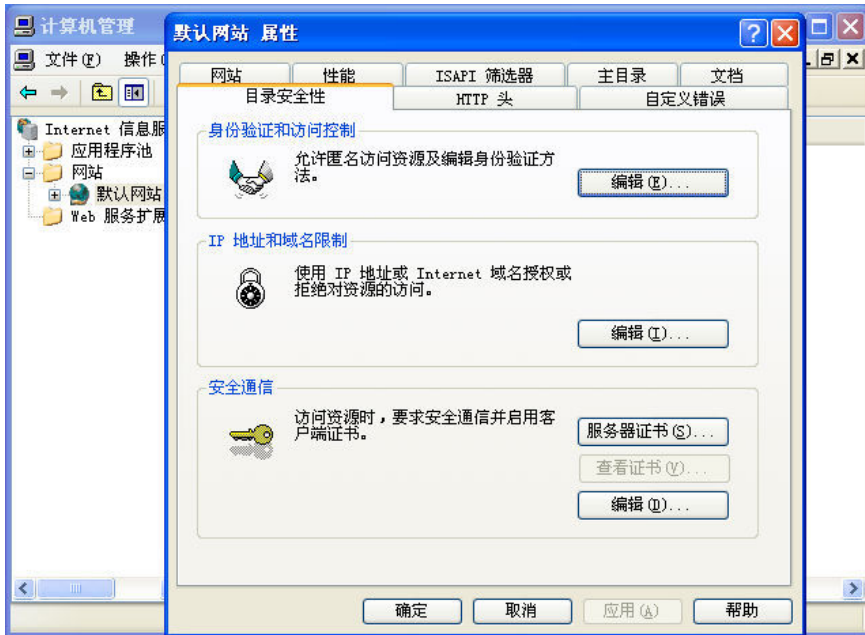
安装服务器证书

保存服务器证书

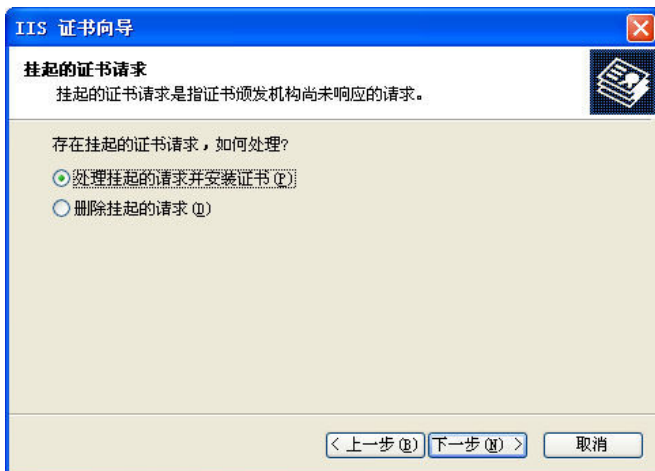
将证书签发邮件中的从BEGIN到 END结束的服务器证书内容（包括“-----BEGIN CERTIFICATE-----”和“-----END CERTIFICATE-----”）粘贴到记事本等文本编辑器中，并修改文件扩展名，保存为server.cer文件。

进入IIS控制台

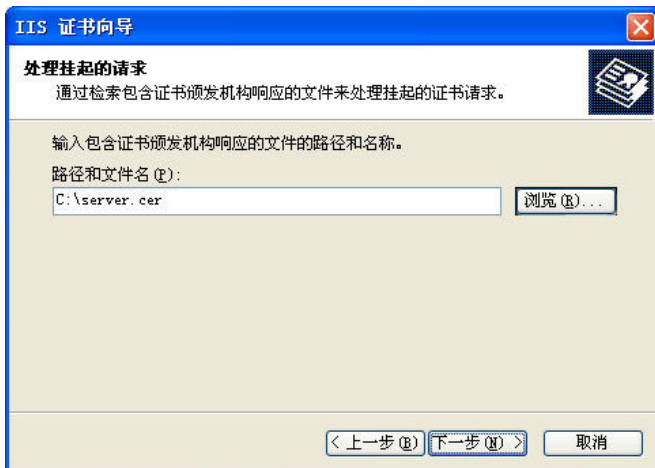
1. 进入IIS控制台，并选中需要配置服务器证书的站点，属性 > 目录安全性。



2. 选择服务器证书 > 处理挂起请求并安装证书，点击下一步。



3. 选中您的服务器证书文件，点击下一步。



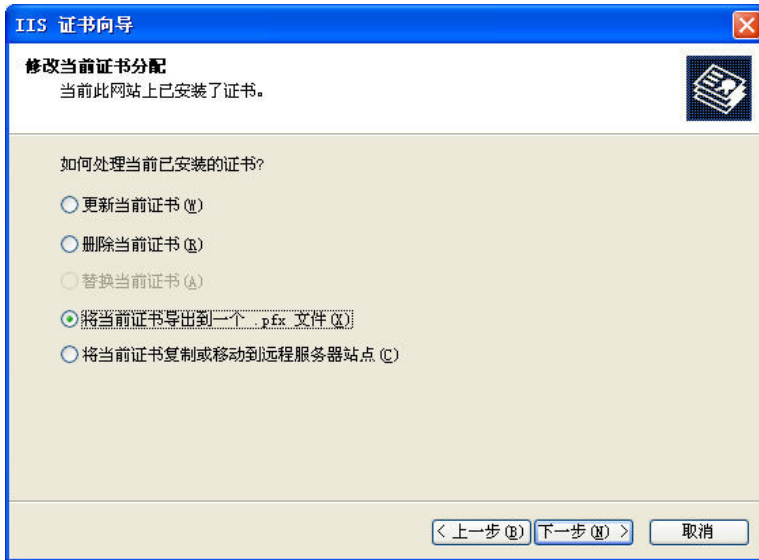
4. 配置默认的https访问端口443，重启IIS并使用https方式访问测试站点证书安装。

服务器证书的备份及恢复

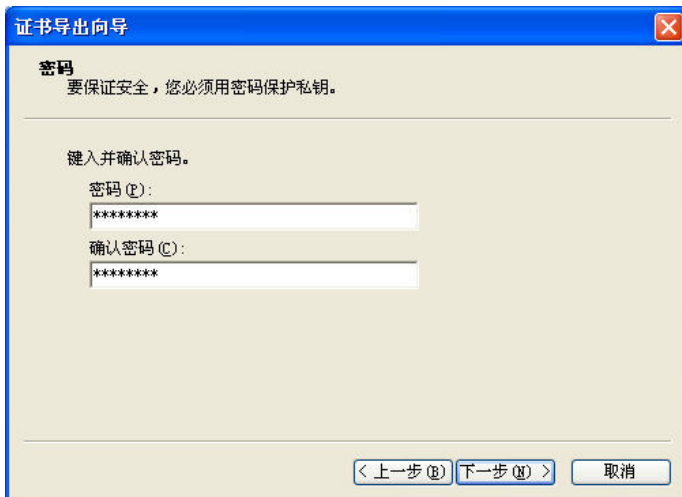
在您成功的安装和配置了服务器证书之后，请务必依据下面的操作流程，备份好您的服务器证书，以防证书丢失给您带来不便。操作流程如下：

服务器证书的备份

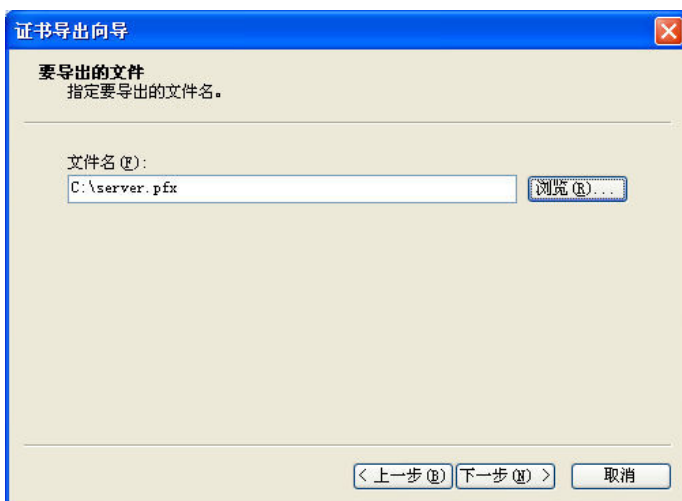
1. 进入IIS控制台，选择安装有服务器证书的站点，右键选择属性 > 目录安全性 > 服务器证书 > 将当前站点证书导出到一个.pfx文件。



2. 为导出的证书备份文件设置一个保护密码，点击下一步。

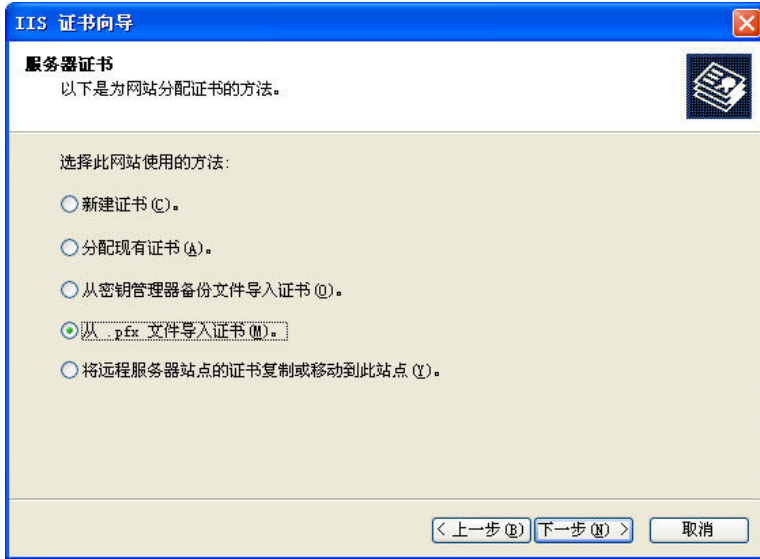


3. 设置文件导出路径，点击下一步。

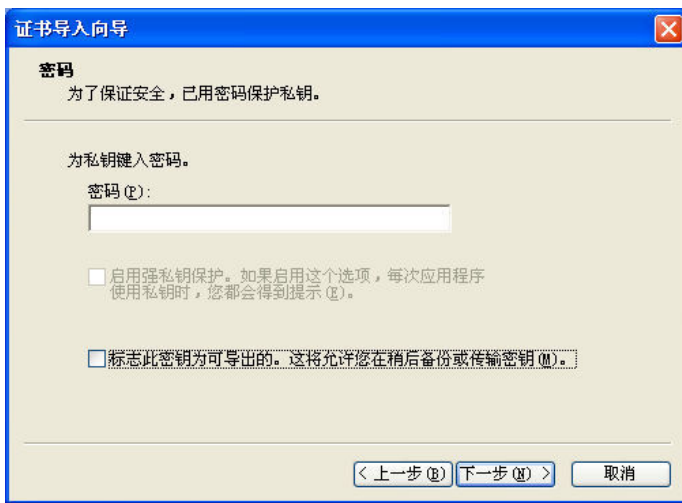


服务器证书的恢复

1. 进入IIS控制台，选择安装有服务器证书的站点，右键选择属性 > 目录安全性 > 服务器证书 > 从.pfx文件导入证书。



2. 选择您的服务器证书备份文件，并输入备份文件保护密码。



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，私钥将无法从服务器中导出。建议您将证书备份文件保存好，不勾选此选项，这将更有利于服务器证书密钥的安全。

3. 配置默认的https访问端口443，重启IIS并使用https方式访问测试站点证书安装。