服务名称：Digicert 单域名 DV SSL 数字证书

下单须知：在您下单后，在云平台的后台消息中心中会收到关于本订单的消息。

文档发布者：ZeroSSL

购买产品后系统会发送一份邮件到购买时预留邮箱，用户也可以直接联系 ZeroSSL 官方客服 www.zerossl.com.cn

1、需要准备材料：域名、申请人邮箱。
2、配合操作，根据要求配合解析域名。
3、拿到 SSL 证书文件根据教程安装部署。

Nginx 安装教程

解压后应包含两个文件:

```
yourdomain.com.crt　（服务器证书）

yourdomain.com.key （私钥文件）如果为空请将生成 CSR 时保存的私钥内容粘贴在文件中
```

环境检测，检测命令如下（测试 nginx 是否支持 SSL）

```
nginx –V
```

如果有输入 —with–http_ssl_module 表示已编译 openssl，支持安装 ssl

如果没有安装请下载 nginx 源码重新编译

```
./configure ––with–http_stub_status_module ––with–http_ssl_module

make && make install
```

配置 Nginx

```
server {

listen 80;

listen 443 ssl;

server_name www.zerossl.com.cn;

ssl_protocols TLSv1.2 TLSv1.1 TLSv1;
```

```
ssl_certificate /etc/ssl/yourdomain.com.crt;

ssl_certificate_key /etc/ssl/yourdomain.com.key;

ssl_prefer_server_ciphers on;

#自动跳转到 HTTPS (可选)

if ($server_port = 80) {

rewrite ^(.*)$ https://$host$1 permanent;

}

location / {

root /home/web/;

index index.php;

}

}
```

以上配置仅供参考，其他参数请根据生产环境需要添加。

安装后重启 nginx 使其生效

```
centos6

service nginx restart

centos7
```

```
systemctl restart nginx
```

问题排查：

如果使用 CDN（加速器），需要在 CDN 上面安装证书，国内免费加速的都不支持 https（已知阿里云 cdn 支持）

检查 443 端口是否启动 使用下面命令 **netstat –apnt | grep 443** （如果没有启动检查配置文件或者端口是否冲突）

443 端口如果已经启动,但不能访问，请检查防火墙（或者安全狗），允许 443 端口.

linux iptables 使用下面命令:

```
iptables –A INPUT –p tcp –m tcp ––dport https –j ACCEPT
```

Apache 安装教程

在我们网站购买的客户，下载 Apache 格式的证书

解压后应包含三个文件:

```
yourdomain.com.crt　（服务器证书）

yourdomain.com.key （私钥文件）如果为空请将生成 CSR 时保存的私钥内容粘贴在文件中

yourdomain.com.ca-bundle（根证书链）
```

下面介绍如何安装 Apache. 首要条件就是 apache 已经安装了 mod_ssl.so 模块 。

检测方法使用以下命令:

```
httpd -M | grep mod_ssl
```

如果有显示 mod_ssl.so 表示已经安装了 apache 模块。

CentOS/Redhat 安装 mod_ssl.so

```
yum install mod_ssl
```

Debian/Ubuntu

```
sudo a2enmod ssl

sudo service apache2 restart
```

Apache SSL 配置

```
Listen 443（如果配置已经存在就不要加）

LoadModule ssl_module modules/mod_ssl.so (如果配置已经存在就不要加)

NameVirtualHost *:443 (非必须，配置多个 SSL 站点会需要)

<VirtualHost *:443>

ServerName www.zerossl.com.cn

ServerAlias www.zerossl.com.cn

DocumentRoot /var/www/html

SSLEngine on

SSLProtocol all -SSLv2 -SSLv3

SSLCertificateFile /etc/ssl/server.crt

SSLCertificateKeyFile /etc/ssl/server.key

SSLCertificateChainFile /etc/ssl/server.ca-bundle

</VirtualHost>
```

以上只是 SSL 配置范例，尽量不要直接应用于生产环境，请根据 80 端口的站点配置修改。
证书可以放在其他位置，没有强制要求
ServerName 和 ServerAlias 需要修改

配置完成重启 Apache 使其生效.

```
service httpd restart
```

使用 https://yourdomain.com 测试是否可以访问。

问题排查：

如果使用 CDN（加速器），需要在 CDN 上面安装证书，国内免费加速的都不支持 https（已知阿里云 cdn 支持）

检查 443 端口是否启动　使用下面命令 netstat –apnt | grep 443　（如果没有启动检查配置文件或者端口是否冲突）

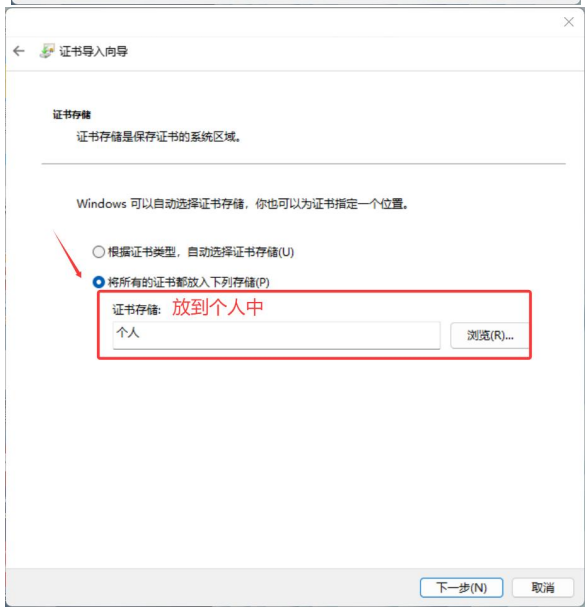
443 端口如果已经启动,但不能访问，请检查防火墙（或者安全狗），允许 443 端口.

linux iptables 使用下面命令:

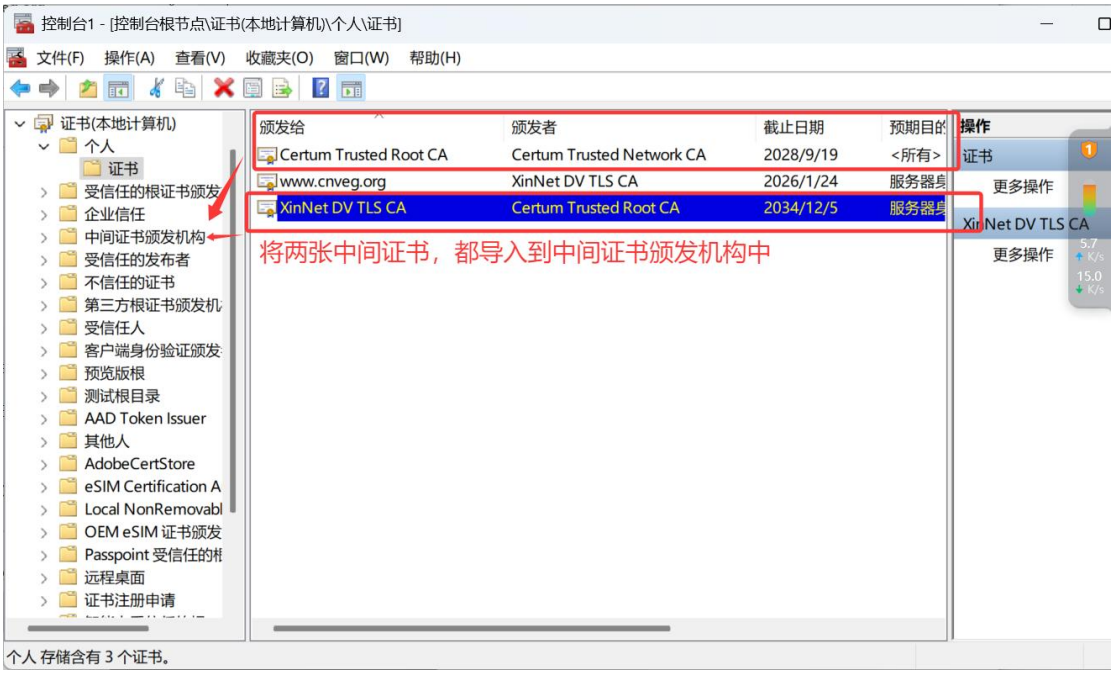
```
iptables –A INPUT –p tcp –m tcp ––dport https –j ACCEPT
```

IIS 服务器 SSL 证书的部署

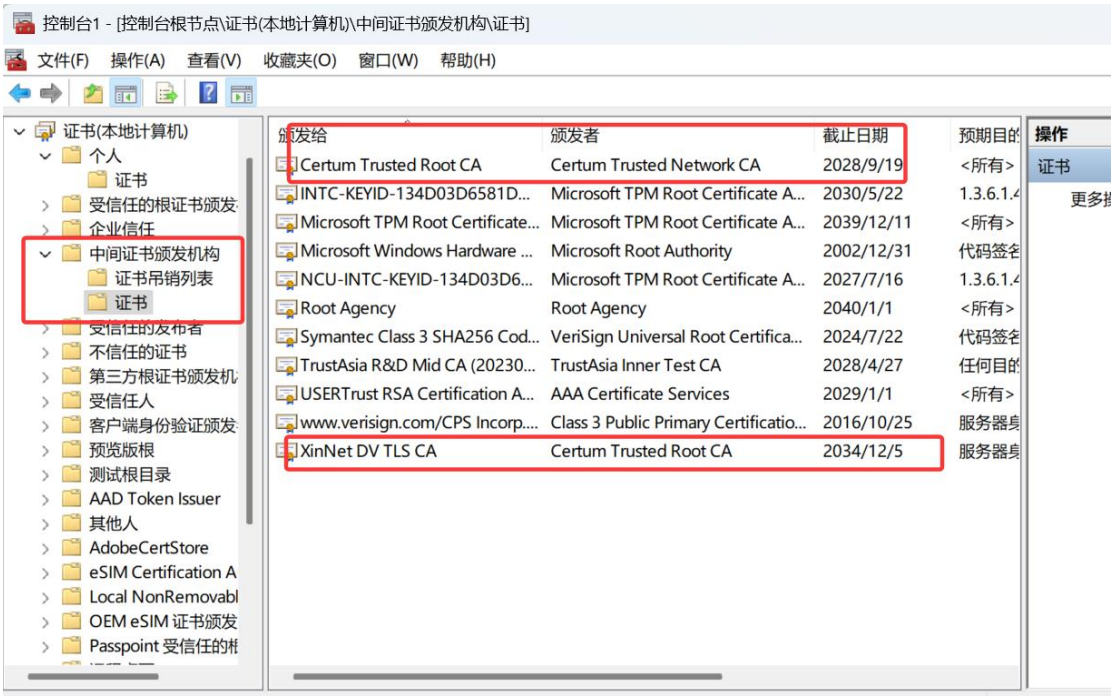
1、 IIS 服务器的证书格式为 pfx，在证书申请完成之后，选择对应的格式进行下载，下载完成之后，双击证书进行导入到本地计算机的个人单元中。



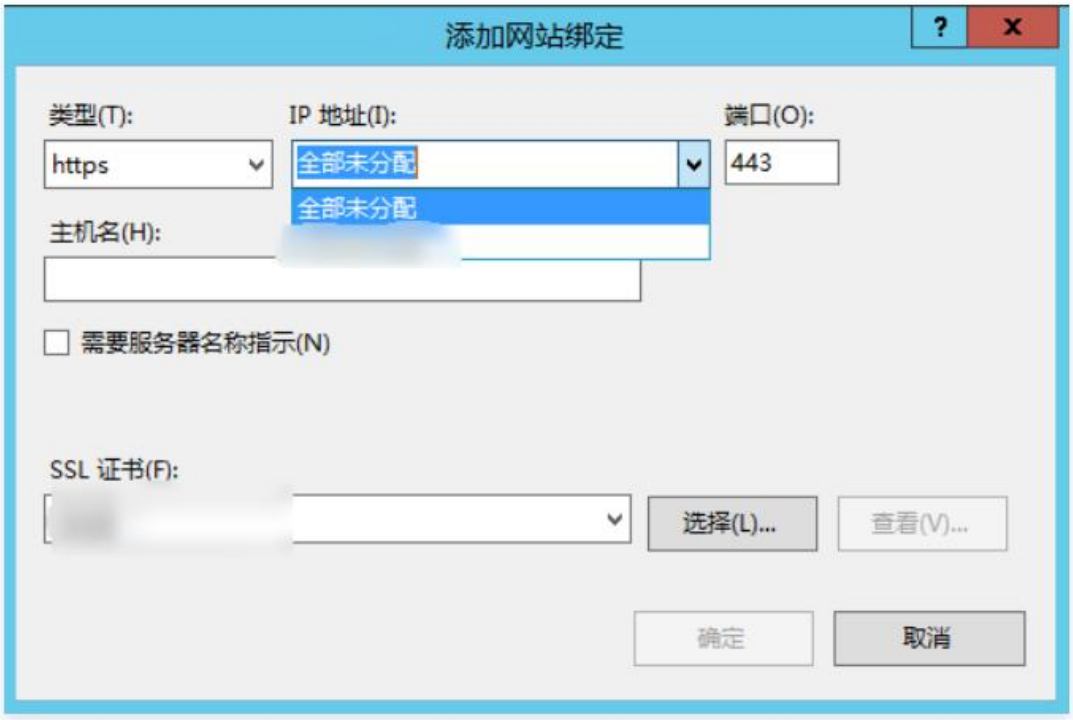
2、 在搜索框中输入 mmc 打开管理控制台，点击添加单元之后点击证书选择本地计算机进行添加，然后点击个人，将中间证书和交叉证书导入到中间证书颁发机构中。



检查中间证书颁发机构中，包含这两张证书即可



3、 3、导入证书之后，点击 iis 管理器中要安装证书的网站，导入证书将证书与网站进行绑定。



注：如果检查证书链显示完整，实际部分设备无法校验，请查看是否以及将两张中间证书都导入了，可使用 zerossl.com.cn 进行检测，如显示第三张证书缺少，则单独导入该交叉证书。

1、将交叉证书的证书内容保存为后缀为 cer 或 crt 的文件进行使用。

certum-cross.cer

Certum Trusted Root CA 》Certum Trusted Network CA

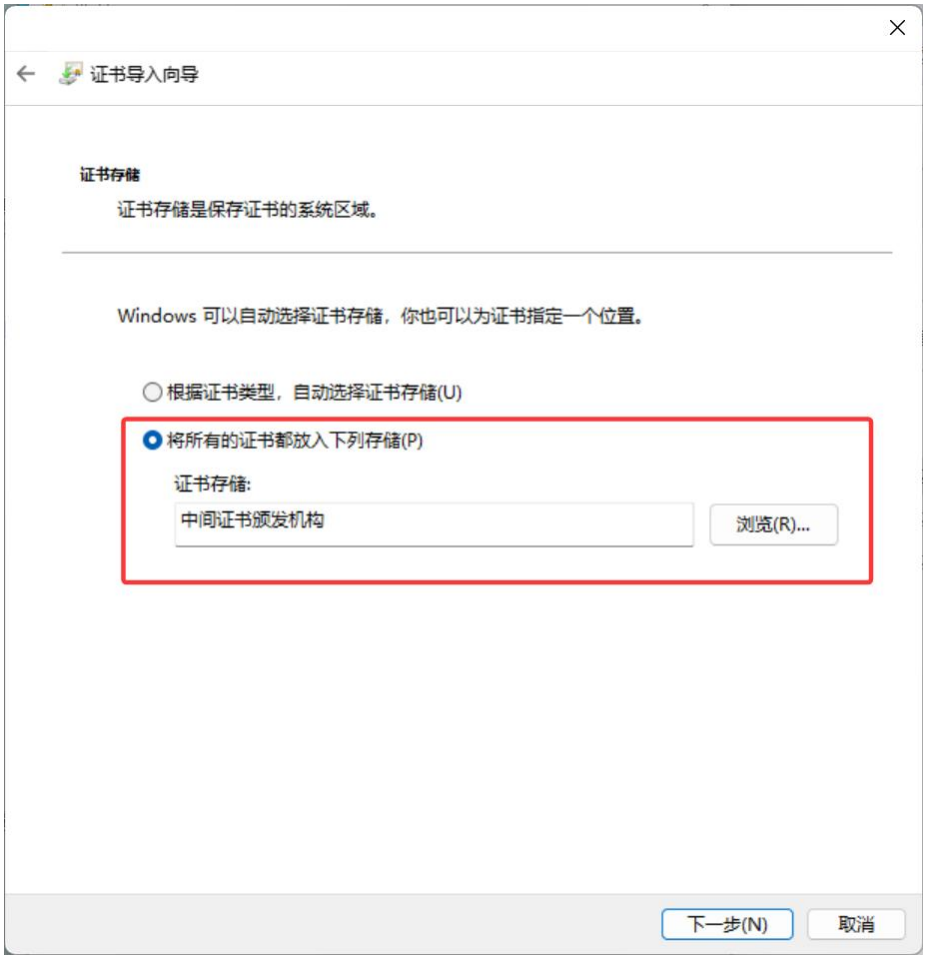
使用者：CN = Certum Trusted Root CA
颁发者：CN = Certum Trusted Network CA

证书内容：

-----BEGIN CERTIFICATE-----
MIIFxDCCBKygAwIBAgIRANjgdEtYJJGfvQiEffcgIPowDQYJKoZIhvcNAQENBQAw
fjELMAkGA1UEBhMCUEwxIjAgBgNVBAoTGVVuaXpldG8gVGVjaG5vbG9naWVzIFMu
QS4xJzAlBgNVBAsTHkNlcnR1bSBDZXJ0aWZpY2F0aW9uIEF1dGhvcml0eTEiMCAG
A1UEAxMZQ2VydHVtIFRydXN0ZWQgTmV0d29yayBDQTAeFw0yMzA5MTkxMDAwMDBa
Fw0yODA5MTkxMDAwMDBaMHoxCzAJBgNVBAYTAlBMMSEwHwYDVQQKExhBc3NlY28g
RGF0YSBTeXN0ZW1zIFMuQS4xJzAlBgNVBAsTHkNlcnR1bSBDZXJ0aWZpY2F0aW9u

IEF1dGhvcml0eTEfMB0GA1UEAxMWQ2VydHVtIFRydXN0ZWQgUm9vdCBDQTCCAiIw
DQYJKoZIhvcNAQEBBQADggIPADCCAgoCggIBANEtjru3NuptN5GfTpOnBeQpAyXO
HIL3fJmfQQbN7aO6wNsJLMF83yl+S2Uvk6fUAWsDKBij2J0FwSrYRfGR3t870IAC
jM84D+qnXHgRpMHIhVwl09Oy5yXPEVSXqzXAHnYc7wBTnzncFKUsIiWzcnL8jbPl
PggeFCo3C4g8yrD0yMKhrrzBvilnVeL8rVlc/r1XLLCQjcLtN7Z8mYi11QOaPRUN
PTqoqEXwlU4lWR3NmGm708wyyY3vgf6tfYm7umATymWVZ6DzGfYDVtRq0yfioa2D
8EoSInccBXPiGXFCwOx1RpqQWOBqjiulRjAEjhmyF+O+qbp/VvEkA9eyISh2DjYw
THnVQZqaqLg1ugw68kQbIIj3xSXXPcbjPkPdh/7E6vVTPkxl/ztKy3haaxdfDcfD
T06aKqLtV00i4kaaPw+RNCR9VeOMlTfTGvAJKyzSyY20DQCrZyko2AH1GQS2Hb52
/nJcxIXK0oBB3wWoo9WEkE8L8+A/mxnSN4k/8ntSHIz24fc8B5eMDqJZgQyykD3T
41lG7Q+pp96Aa1qqB7YZy7xX85chegyxK3Q+69qnZy1MxJieNgl2Zmb8Gj/qSFQc
vjC9gFC/fLXOAPYMYdnnJAPg4wGBDr3YhTSIvbI2qHtcCOVEgIxv+C/VIcodHND7
xLWH0TpOx3a1NUi1AgMBAAGjggE/MIIBOzAPBgNVHRMBAf8EBTADAQH/MB0GA1Ud
DgQWBBSM+xx1vALTn04uSNn5YFSqxLNP+jAfBgNVHSMEGDAWgBQIds3LB/8k9sXN
7buQvOKEN0Z19zAOBgNVHQ8BAf8EBAMCAQYwLwYDVR0fBCgwJjAkoCKgIIYeaHR0
cDovL2NybC5jZXJ0dW0ucGwvY3RuY2EuY3JsMGsGCCsGAQUFBwEBBF8wXTAoBggr
BgEFBQcwAYYcaHR0cDovL3N1YmNhLm9jc3AtY2VydHVtLmNvbTAxBggrBgEFBQcw
AoYlaHR0cDovL3JlcG9zaXRvcnkuY2VydHVtLnBsL2N0bmNhLmNlcjA6BgNVHSAE
MzAxMC8GBFUdIAAwJzAlBggrBgEFBQcCARYZaHR0cHM6Ly93d3cuY2VydHVtLnBs
L0NQUzANBgkqhkiG9w0BAQ0FAAOCAQEAKPpdjKpRGqa+eIZpwndaFy+p4H1FT2wf
9JOJdmyjSkJ4wlUp+xbL6v7D6/6xYO8IcvyWyR1sdqef8HK49mYK9jDjk+ypq7IO
h8R9VbhSuS6KxY3X5lVV6vmYZ6QE4G8IuK9ktvGSVS4uNabf+/r+Gq9oiysCwsck
AsjwXbYN2gsKAWxXGC1vAqIOlB3tJaL29UVh2nKdl0eD7EsFwbk0vo/U5pQ/Yi8u
JJb/OSiK1XXUJ7S8wmURNWK2hIzHSnP9xotjmUJMVMb8Igj8jntZNc9U3lNuzG6R
F2kSR3FCgnCJ9AebGFZwEc7QDTCuohG6Lmb6D3Dtopv/LvqypxAmQQ==
-----END CERTIFICATE-----

2、双击该证书，安装到当前用户（不确定的话，当前用户和本地计算机都导入下）的中间证书颁发机构中去。



3、重新导入并绑定 iis 需要的证书。