



# 如何添加自定义CA根证书到操作系统获得信任

原创 © 2017-03-15 枫叶 6278

现在很多网站和服务都使用了HTTPS进行链路加密、防止信息在传输中间节点被窃听和篡改。

HTTPS的启用都需要一个CA证书，以保证加密过程是可信的。

我们可以申请和获得一个CA机构颁发的证书，在软件调试过程中或者机构内部网可以创建自签名的CA证书，在[使用openssl创建nginx自签名证书](#)有关于自签名CA证书制作和使用的描述。

所谓“自签名”就是把自己当成一个CA证书颁发机构，只不过未得到公共证书机构的认可。这样的CA证书在部分操作系统下，可以直接配置在应用系统里使用，在浏览器里往往会进行提示，如果加入“例外”白名单中，就可以继续使用。

但在有的操作系统和一些版本中，需要将根证书配置为系统级的证书，才允许继续使用，系统就像个看大门的，需得首先过了这一关才行。尤其是因为出现证书机构颁发虚假证书问题，最近很多操作系统都加强了安全措施，对证书都加强了验证，必须进行ca证书配置才能继续访问了。

## Mac OS X

添加证书：

```
sudo security add-trusted-cert -d -r trustRoot -k /Library/Keychains/System.keychain ~/new-root-certificate.crt
```

移除证书：

```
sudo security delete-certificate -c ""
```

## Windows

添加证书：

```
certutil -addstore -f "ROOT" new-root-certificate.crt
```

移除证书：

```
certutil -delstore "ROOT" serial-number-hex
```

## Linux (Ubuntu, Debian)

添加证书：

1.复制 CA 文件到目录： /usr/local/share/ca-certificates/

2.执行：

```
sudo cp foo.crt /usr/local/share/ca-certificates/foo.crt
```

3.更新 CA 证书库：

```
sudo update-ca-certificates
```

移除证书：

1.Remove your CA.

2.Update the CA store:

```
sudo update-ca-certificates --fresh
```

Restart Kerio Connect to reload the certificates in the 32-bit versions or Debian 7.

## Linux (CentOs 6)

添加证书:

1.安装 ca-certificates package:

```
yum install ca-certificates
```

2.启用dynamic CA configuration feature:

```
update-ca-trust force-enable
```

3.Add it as a new file to /etc/pki/ca-trust/source/anchors/:

```
cp foo.crt /etc/pki/ca-trust/source/anchors/
```

4.执行:

```
update-ca-trust extract
```

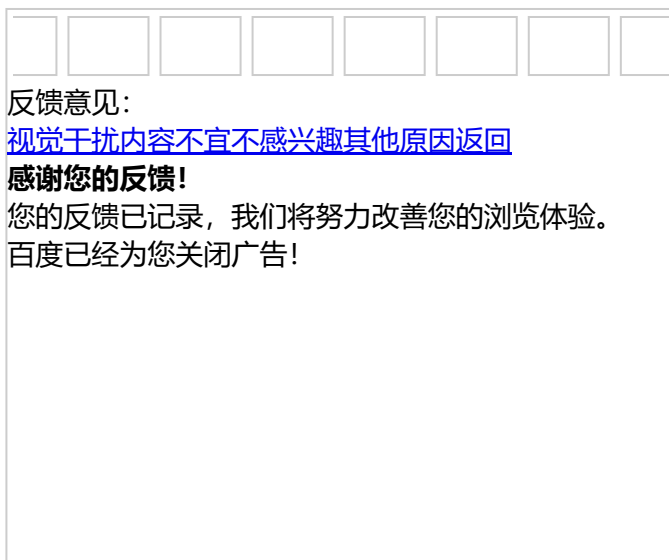
Restart Kerio Connect to reload the certificates in the 32-bit version.

## Linux (CentOs 5)

添加证书:

Append your trusted certificate to file /etc/pki/tls/certs/ca-bundle.crt

```
cat foo.crt >> /etc/pki/tls/certs/ca-bundle.crt
```



文章链接: <https://www.qiansw.com/add-the-ca-root-certificate-to-the-operating-system-for-trust.html>

码字不易，转载请注明本文出处及文章链接。

[ssl](#) [https](#) [证书](#) [ca](#)

---

上一篇: [为 mongodb 副本集增加密码认证](#)

下一篇: [LiteIDE 第三方库不能自动补全的解决办法](#)

---

### 👍 推荐阅读

[腾讯云通知用户重颁发赛门铁克 SSL 证书](#)

[配置Nginx使其支持iOS要求的ATS](#)

[使用openssl创建nginx自签名证书](#)

[Mozilla 做出不再信任沃通 CA 的决定](#)

## 苹果要求2017年开始应用内必须使用HTTPS



沙发等待中..... 2017-03-15 18:11

这篇文章还没有人留言，快来抢沙发吧。

👤 您的大名 (\*必填)

✉ Email (选填,接收回复)

🌐 您的网站 (选填)

✍ 评论内容 (\*必填)

留下足迹