

# 如何设置证书不信任

## 一、Windows

### 步骤 1：获取证书文件

下载公告附件中的恶意伪造证书

### 步骤 2：打开证书管理器

打开“运行”对话框：

按下 Win + R 键，打开“运行”窗口。

输入证书管理器命令：

在“运行”窗口中输入 certmgr.msc，然后按 Enter 键。这将打开“证书管理器”。

### 步骤 3：找到不受信任的证书区域

在“证书管理器”窗口的左侧菜单中，找到并展开\*\*“不受信任的证书”\*\*节点。

您将看到三个子文件夹：“不受信任的根证书颁发机构”、“第三方证书颁发机构”和“个人”。

### 步骤 4：导入证书

右键点击“不受信任的根证书颁发机构”：

选择“所有任务” > “导入”。这将启动证书导入向导。

在导入向导中点击“下一步”。

选择证书文件：

点击“浏览”按钮，找到您要安装的证书文件。



选择该文件后，点击“打开”。

#### **继续导入向导：**

点击“下一步”。

#### **选择存储位置：**

在“证书存储”页面，选择“将所有证书放入以下存储”并确保选中“不受信任的根证书颁发机构”，然后点击“下一步”。

#### **完成导入：**

最后，点击“完成”。您将看到一个提示，确认证书已成功导入。

## **步骤 5：验证证书**

#### **查看证书列表：**

返回“证书管理器”，在“不受信任的根证书颁发机构”中查看您刚刚导入的证书。

#### **检查证书详细信息：**

右键点击证书，选择“打开”，查看证书详细信息，确保其内容正确无误和确认已不信任该证书。

## **二、Linux**

在 Linux 系统中，通常将证书放入特定目录并更新证书存储。步骤如下：

**找到证书文件：** 获取要安装的证书（如 .crt 或 .pem 格式）。

**移动证书文件：** 使用终端命令将证书文件移动到不受信任的证书目录。

```
sudo mv /path/to/certificate.crt /etc/ssl/certs/blacklist/
```

**更新证书存储：** 运行以下命令以更新证书存储：

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