

# SSL 证书 – F5

## 证书安装指南

请选择您的版本

[BIG-IP F5 v 9.x 和 10.x SSL 安装指南](#)

[F5 BIG-IP v11 SSL 安装指南](#)

## BIG-IP F5 v 9.x 和 10.x SSL 安装指南

### 步骤 1: 获取 Intermediate CA 证书

1. [通过此链接下载 Intermediate CA 证书](#)。

选择和你的 SSL 证书适合的 Intermediate CA 证书。

2. 复制 Intermediate CA 并粘贴至 Notepad 或其他 TXT 文本编辑器，并把文件存档为 intermediate.crt.
3. 把文件储存至此: /config/bigconfig/ssl.crt/intermediate.crt

### 步骤 2: 安装 Intermediate CA 证书

1. 登入 Configuration Utility。
2. 点击 Local Traffic。
3. 点击 SSL Certificates。
4. 点击 Import。
5. 在 Import Type 菜单，选择 Certificate。
6. 点击 Create New 选项。
7. 为证书创建别名。
8. 点击 Browse 然后找到已储存的 Intermediate.crt。
9. 点击 Open。
10. 点击 Import。

### 步骤 3: 获取 SSL 证书

1. SSL 证书将会通过邮件发给用户。用户也可通过登入用户中心获取 SSL 证书。
2. 请把电邮中的正文复制并粘贴到 Vi 或 Notepad 等 TXT 文本编辑器。

证书正文的例子：

```
-----BEGIN CERTIFICATE-----
```

```
[加密数据]
```

```
-----END CERTIFICATE-----
```

3. 把证书存档为 filename.crt 文档。

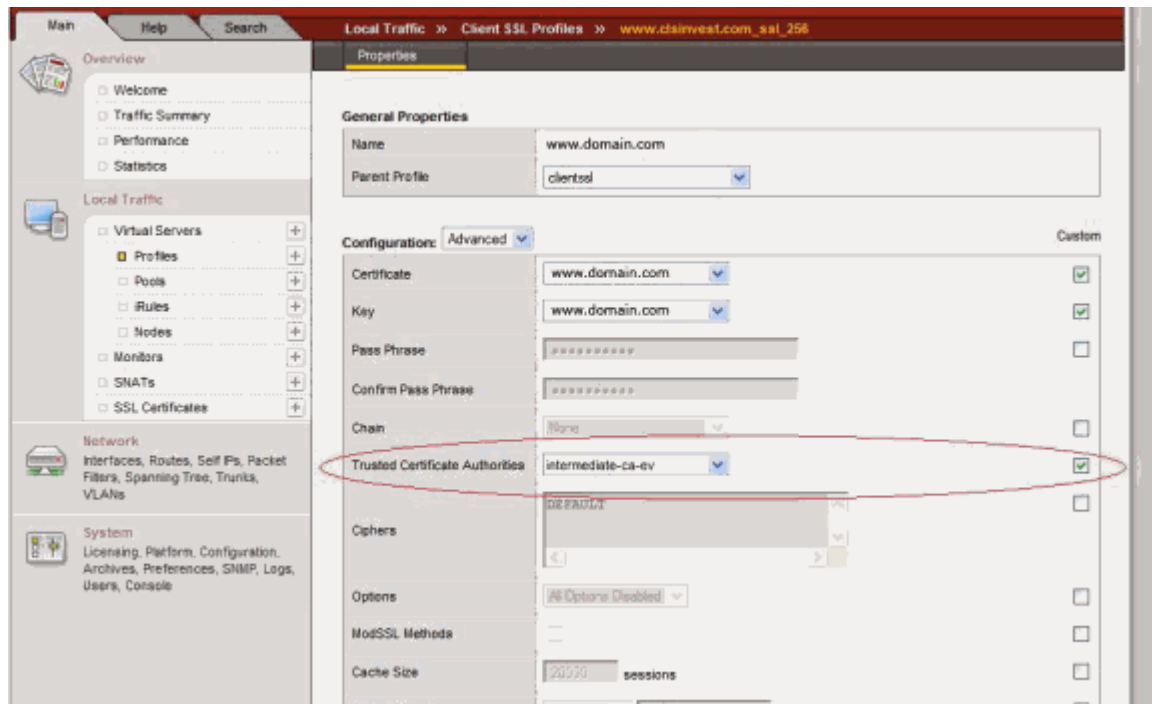
### 步骤 4: 安装 SSL 证书

1. 在导航栏中，点击 Proxies。
2. 在 Proxies 视窗，点击 Install SSL Certificate Request 选项。
3. 在 Certificate Name 文本框，输入主机的完整域名并加入.crt 扩展。
4. 把证书正文复制至 Install SSL Certificate 视窗。
5. 点击 Write Certificate File 安装证书。证书完成安装后可进行下一步。

### 步骤 5: 配置服务器

1. 登入 Configuration utility。
2. 点击 Local Traffic。
3. 点击 Profiles。
4. 在 SSL menu，选择主机名称。

5. 选择要设置的主机 SSL。
6. 从 Configuration 菜单选择 **Advanced**。
7. 选择适当的证书链。
8. 点击更新。



9. 要检验您的证书是否已正确安装，请使用 Symantec 的[证书检查工具](#)。

## F5 BIG-IP v11 SSL 安装指南

### 步骤 1: 获取 SSL 证书

1. SSL 证书将会通过邮件发给用户。用户也可通过登入用户中心获取 SSL 证书。
2. 请把电邮中的正文复制并粘贴到 Vi 或 Notepad 等 TXT 文本编辑器。

证书正文的例子：

-----BEGIN CERTIFICATE-----

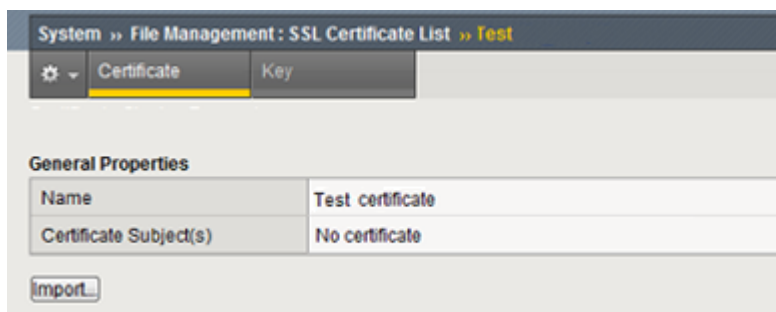
[加密数据]

-----END CERTIFICATE-----

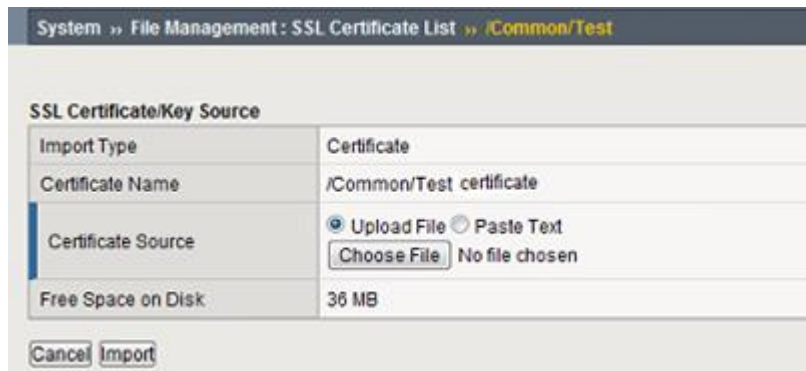
3. 把证书存档为 filename.pem 文档。

### 步骤 2: 安装 SSL 证书

1. 在左侧控制面板中，点击 File Management。
2. 选择 SSL Certificate List。
3. 从列表中，点击 pending request。
4. 点击 Import。



5. 选择 Upload File。
6. 点击 Choose File。
7. 找到证书文件然后点击 OK。
8. 点击 Import。



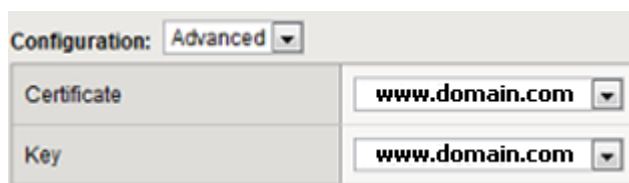
System » File Management : SSL Certificate List » /Common/Test

SSL Certificate/Key Source

Import Type	Certificate
Certificate Name	/Common/Test certificate
Certificate Source	<input checked="" type="radio"/> Upload File <input type="radio"/> Paste Text <input type="button" value="Choose File"/> No file chosen
Free Space on Disk	36 MB

### 步骤 3: 分配 SSL 证书

1. 在 Configuration 选项下，选择 Advance。
2. 从列表中选择证书和密钥。



Configuration:

Certificate	<input type="text" value="www.domain.com"/>
Key	<input type="text" value="www.domain.com"/>

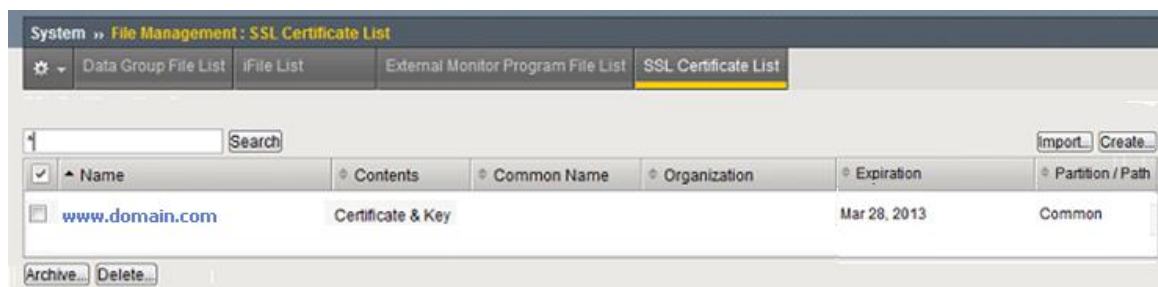
3. 点击 Submit 以确认更新。

#### 步骤 4: 下载 Intermediate CA 证书

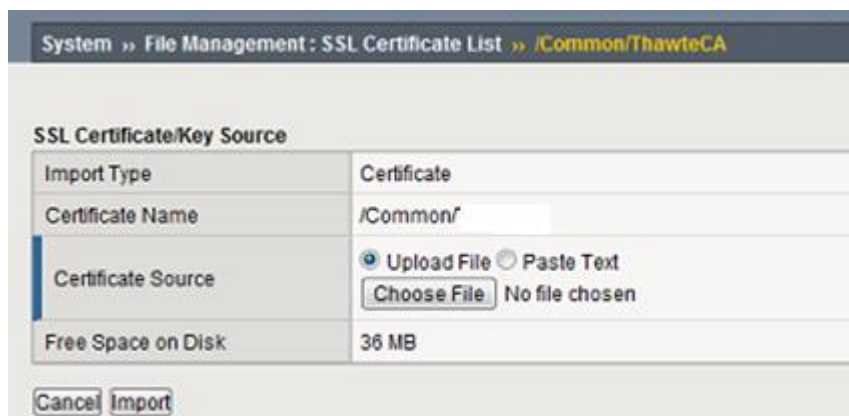
4. [通过此链接下载 Intermediate CA 证书](#)。

选择和你的 SSL 证书适合的 Intermediate CA 证书。

5. 复制 Intermediate CA 并粘贴至 Notepad 或其他 TXT 文本编辑器，并把文件存档为 intermediate.pem.
6. 在左侧的控制面板中，点击 File Management.
7. 选择 SSL Certificate List.



8. 点击 Import.
9. 点击 Choose File.



10. 选择 Intermediate.pem 文件然后点击 OK.
11. 点击 Import.



## 步骤 5: 更新 SSL 配置

1. 在左侧的控制面板，点击 Profiles。
2. 选择 SSL。
3. 选择 Client。
4. 从列表中，选择你的网页的 SSL 配置。

## 步骤 6: 指定 CA Bundle

1. 在 Configuration 下，选择 Advanced。
2. 在 Chain 的列表中，选择 CA Bundle。



3. 点击 Submit。
4. 要检验您的证书是否已正确安装，请使用 Symantec 的[证书检查工具](#)。