SSL 证书 - WHM11

证书安装指南

webnic
accelerate your business

SSL 证书 WHM 中的 CSR 创建

WebHost Manager (WHM) SSL 证书的 CSR 创建

如果您已拥有 SSL 证书并且只需要安装，请参阅 WHM SSL 证书安装。

如何在 WHM 中生成 CSR

以下说明适用于 WHM 11.如果您使用的是 WHM 的其他版本，则会执行类似的过程，但您可能需要向网络主机询问具体说明。

1. 登录 WebHost 管理控制面板
2. 在左侧的菜单中点击**生成一个 SSL 证书和签名请求。**
3. 在“**生成新证书签名请求”**部分中，输入以下信息：

   电子邮件-您将接收 CSR 的电子邮件地址

   密码-创建一个与证书关联的密码。稍后您需要记住这个密码。

   主机-. 您在生成私钥时输入或选择的域。

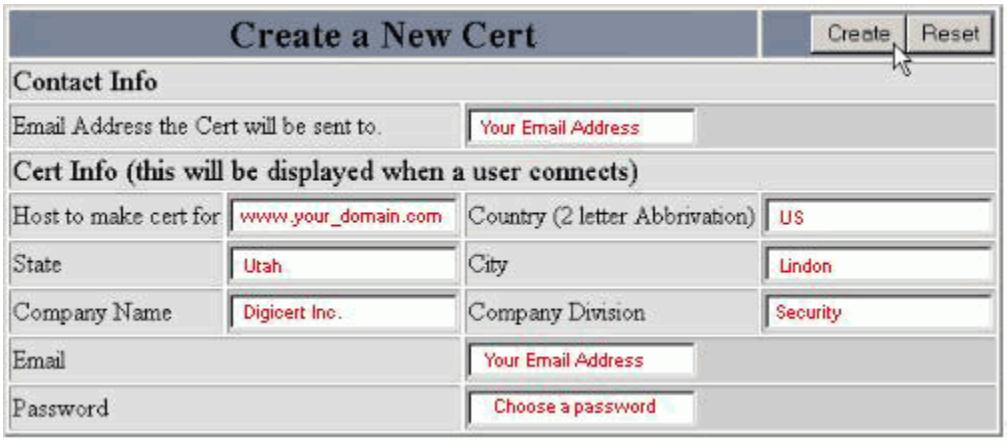
   城市 -组织所在的城市。

   状态-组织所在的状态。不要使用缩写。

   国家 -如果需要，您可以在这个列表中找到您国家的两位数代码。

   公司名称 –您的组织/公司的合法注册名称。

   公司部门 -您所在部门在组织中的名称(通常这个条目会被列出为“IT”、“Web Security”，或者干脆留空)。单击创建按钮



4. 复制并粘贴整个 CSR(包括开始和结束行)到 DigiCert 订单表单中。
5. 从 DigiCert 收到 SSL 证书后，可以安装它。

安装 WHM SSL 证书

在 WebHost 管理中安装 SSL 证书

如果您尚未创建证书签名请求(CSR)并订购证书，请参阅 WebHost Manager (WHM) SSL 证书的 CSR 创建

安装您的 WebHost Manager(WHM) SSL 证书

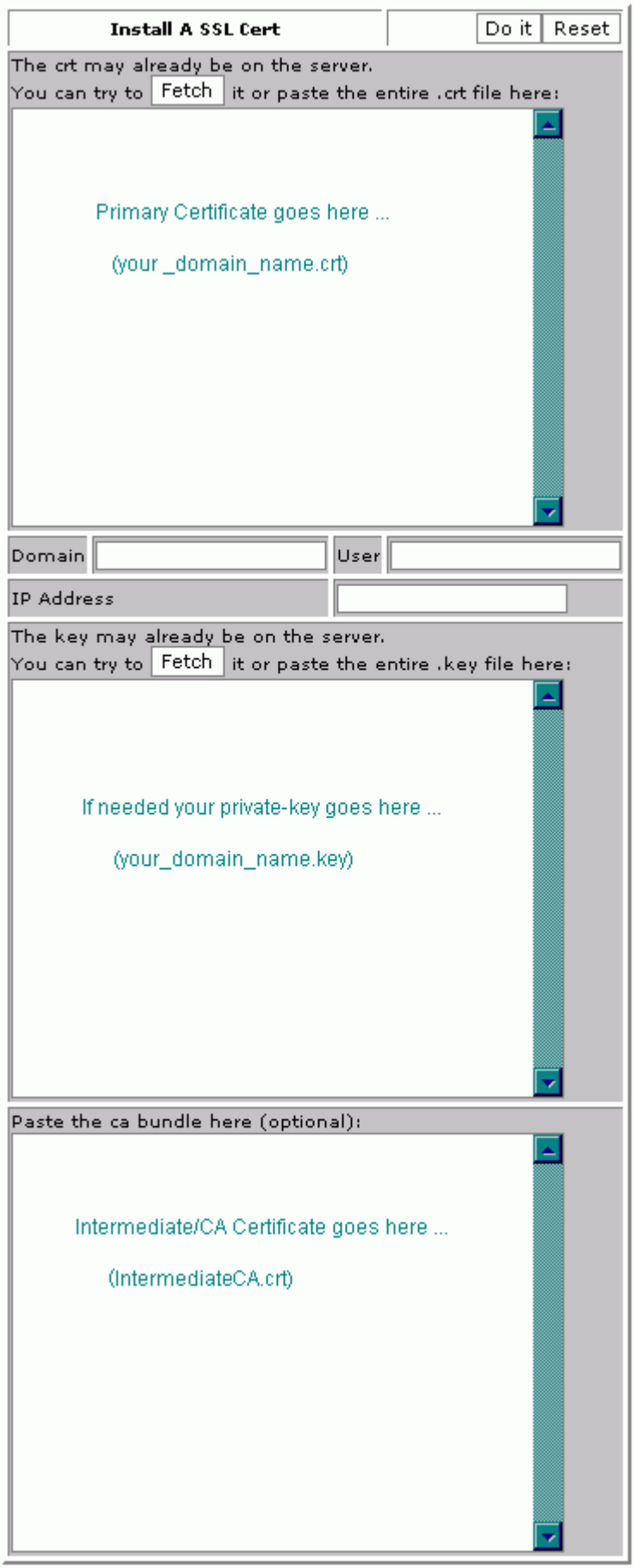
以下说明适用于 WHM11。如果您有一个不同版本的 WHM，您将经历类似的过程，但您可能需要向您的网络主机请求特定的指令。

1. 从证书颁发者处下载中级和主要证书文件 到保存证书和密钥文件的目录。
2. 登录到您的网络主机管理器(WHM)控制面板。
3. 在左侧菜单上，单击**安装一个 SSL 证书和设置域**。

4．在第一个框中，您需要粘贴从 DigiCert 下载的主证书（yourdomain.crt）的内容。要访问证书的文本版本，请使用文本编辑器将其打开。复制和粘贴证书时，请包含 BEGIN 和 END 标记。

5．填写所需的域/用户/ IP 地址信息。域和 IP 地址可以自动填写。在“用户”字段中键入 WHM 用户名。

6. 在中间框中，您需要粘贴使用 CSR 生成的正确 RSA 私钥。生成 CSR 后，此私钥已发送到您的电子邮件地址。如果服务器识别您的证书或单击“获取”按钮，则私钥可以自动填写。
7. 在底部框中，您需要粘贴中间证书（中间 CA.crt）的内容


Install A SSL Cert
Do it
Reset
The crt may already be on the server.
You can try to
Fetch
it or paste the entire .crt file here:
Primary Certificate goes here ...
(your _domain_name.crt)
Domain
User
IP Address
The key may already be on the server.
You can try to
Fetch
it or paste the entire .key file here:
If needed your private-key goes here ...
(your_domain_name.key)
Paste the ca bundle here (optional):
Intermediate/CA Certificate goes here ...
(IntermediateCA.crt)

8. 点击“ **执行”** 按钮。现在应该安装 SSL 证书，并将网站配置为接受安全连接。您或您的 Web 主机可能需要重新启动 Apache 才能正常运行。

9. **注意：如果“执行此操作”按钮未激活，请尝试仅单击私钥的“获取”按钮。这将激活“执行”按钮。请勿单击与证书本身对应的提取按钮。如果执行此操作，证书将替换为无效的自签名证书。

手动安装中级证书

如果使用上述说明未正确安装中级证书，则可能需要直接在 Apache 中安装。如果您无权访问 Apache 配置文件，则需要让您的 Web 主机或管理员按照这些说明安装中间证书：

1. 找到虚拟主机文件：

   在大多数 Apache 服务器上，虚拟站点在/ etc / httpd / conf / httpd.conf 文件中配置。但是，此文件的位置和名称可能因服务器而异 - 特别是如果使用特殊界面来管理服务器配置。该文件的另一个常用名称是“ SSL.conf ”。如果使用文本编辑器打开文件，您将看到服务器上的虚拟主机的配置。虚拟主机配置可能位于文件末尾附近。

2. 确定您站点的安全虚拟主机:

   找到要保护的站点的虚拟主机配置。它将具有正确的名称和 IP 地址（包括端口 443 ）。

3. 配置 SSL 的虚拟主机：

   WHM 已经为您设置了前三个 SSL 配置行。现在，您将通过添加下面的“ SSLCertificateChainFile ”行来编辑虚拟主机配置（此行以粗体显示）。

   ```
   <VirtualHost 192.168.0.1:443>
   DocumentRoot /var/www/html2
   ServerName www.yourdomain.com
   SSLEngine on
   SSLCertificateFile /etc/ssl/crt/your_domain_name.crt
   SSLCertificateKeyFile /etc/ssl/crt/your_private.key
   SSLCertificateChainFile /etc/ssl/crt/intermediateCA.crt
   </VirtualHost>
   ```

   当然，证书文件的路径和名称可能不同。键入 SSLCertificateChainFile 的路径时，请键入计划在保存中间证书时使用的路径和文件名。通常建议将中间证书保存在 WHM 已保存主证书的目录中。

4. 将更改保存到配置文件中

5. Save the Intermediate Certificate file to the Server: 将中级证书文件保存到服务器：

   验证中间证书文件（DigiCertCA.crt）是否已保存到上面配置的路径。

6. 重启 Apache。

故障排除：

1. 如果您的网站可公开访问，SSL 证书测试工具可以帮助您诊断常见问题。
2. 打开网络浏览器并使用 https 访问您的网站。最好同时使用 Internet Explorer 和 Firefox 进行测试，因为如果没有安装中间证书，Firefox 会给你一个警告。您不应该收到任何浏览器警告或错误。如果您立即收到有关该站点不可用的浏览器消息，则 Apache 可能尚未在端口 443 上侦听。如果您的 Web 请求需要很长时间，然后超时，则防火墙会阻止 TCP 端口 443 上的流量到达网络服务器。

如果收到“不信任”警告，请查看证书以查看它是否是您期望的证书。检查“主题”，“颁发者”和“有效期”字段。如果证书是由 DigiCert 颁发的，那么您的 SSLCertificateChainFile 未正确配置。