SSL 證書 - WHM11

證書安裝指南

webnic
accelerate your business

SSL 證書 WHM 中的 CSR 創建

Web 主機管理器 (WHM) SSL 證書的 CSR 創建

如果您已擁有 SSL 證書並且只需要安裝，請參閱 WHM SSL 憑證安裝。

如何在 WHM 中生成 CSR

以下說明適用於 WHM 11.如果您使用的是 WHM 的其他版本，則會執行類似的過程，但您可能需要向網絡主機詢問具體說明。

1. 登錄 WebHost 管理控制面板

2. 在左側的菜單中點擊**生成一個 SSL 證書和簽名請求**。

3. 在**“生成新證書簽名請求”**部分中，輸入以下信息：

電子郵件-您將接收 CSR 的電子郵件地址

密碼-創建一個與證書關聯的密碼。稍後您需要記住這個密碼。

主機-. 您在生成私鑰時輸入或選擇的域。

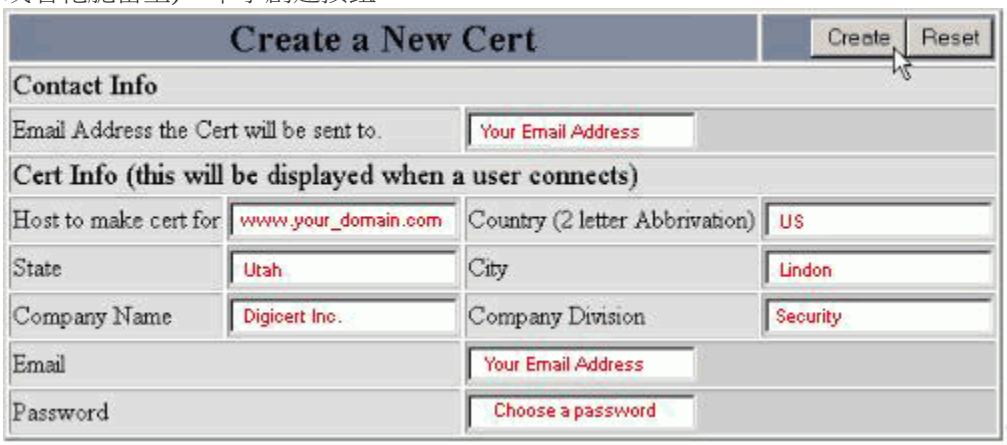
城市 -組織所在的城市。

狀態-組織所在的狀態。不要使用縮寫。

國家 -如果需要，您可以在這個列表中找到您國家的兩位數代碼。

公司名稱 –您的組織/公司的合法註冊名稱。

公司部門 -您所在部門在組織中的名稱(通常這個條目會被列出為“IT”、“Web Security”，或者乾脆留空)。單擊創建按鈕



4. 複製並粘貼整個 CSR(包括開始和結束行)到 DigiCert 訂單表單中。

5. 從 DigiCert 收到 SSL 證書後，可以安裝它。

安裝 WHM SSL 證書

在 WebHost 管理中安裝 SSL 證書

如果您尚未創建證書籤名請求(CSR)並訂購證書，請參閱 WebHost Manager (WHM) SSL 證書的 CSR 創建

安裝您的 Web 主機管理器 (WHM) SSL

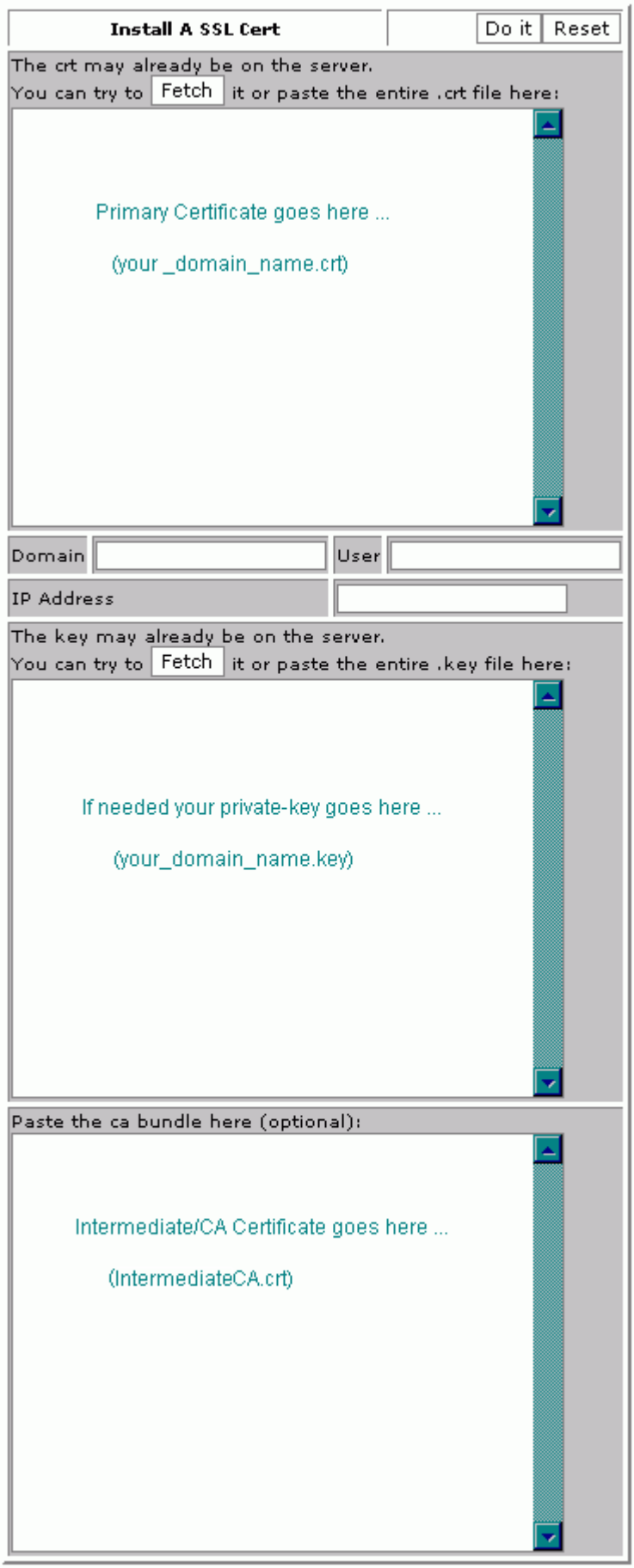
以下說明適用于 WHM11。 如果您有一個不同版本的 WHM，您將經歷類似的過程，但您可能需要向您的網路主機請求特定的指令。

1. 從憑證簽發者處下載中級和主要證書檔 到保存證書和金鑰檔的目錄。
2. 登錄到您的網路主機管理器(WHM)控制台。
3. 在左側功能表上，按一下**安裝一個 SSL 證書和設置域**。

4．在第一個框中，您需要粘貼從 DigiCert 下載的主證書（yourdomain.crt）的內容。 要訪問證書的文本版本，請使用文字編輯器將其打開。 複製和粘貼證書時，請包含 BEGIN 和 END 標記。

5．填寫所需的域/使用者/ IP 位址資訊。 域和 IP 位址可以自動填寫。 在「使用者」欄位中鍵入 WHM 使用者名。

1. 在中間框中，您需要粘貼使用 CSR 生成的正確 RSA 私密金鑰。 生成 CSR 後，此私密金鑰已發送到您的電子郵件地址。 如果伺服器識別您的證書或按一下「獲取」按鈕，則私密金鑰可以自動填寫。
2. 在底部框中，您需要粘貼中繼憑證（中間 CA.crt）的內容


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)

3. 點擊「**執行**」按鈕。 現在應該安裝 SSL 證書，並將網站配置為接受安全連線。 您或您的 Web 主機可能需要重新開機 Apache 才能正常運行。
4. **注意：如果「執行此操作」按鈕未啟動，請嘗試僅按一下私密金鑰的「獲取」按鈕。 這將啟動「執行」按鈕。 請勿按一下與證書本身對應的提取按鈕。 如果執行此操作，證書將替換為不正確自簽章憑證。

手動安裝中級證書

如果使用上述說明未正確安裝中級證書，則可能需要直接在 Apache 中安裝。 如果您無權訪問 Apache 設定檔，則需要讓您的 Web 主機或管理員按照這些說明安裝中繼憑證:

1. 找到虛擬主機檔:

   在大多數 Apache 伺服器上，虛擬網站在/ etc / HTTPd / conf / HTTPd.conf 檔中配置。 但是，此檔的位置和名稱可能因伺服器而異 - 特別是如果使用特殊介面來管理伺服器配置。 該檔的另一個常用名稱是「SSL.conf」。 如果使用文字編輯器打開檔，您將看到伺服器上的虛擬主機的配置。 虛擬主機配置可能位於檔末尾附近。

2. 確定您網站的安全虛擬主機:

   找到要保護的網站的虛擬主機配置。 它將具有正確的名稱和 IP 位址（包括埠 443）。

3. 配置 SSL 的虛擬主機:

   WHM 已經為您設置了前三個 SSL 配置行。 現在，您將通過添加下面的

   ```
   <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>
   ```

   當然，證書檔的路徑和名稱可能不同。 鍵入 SSLCertificateChainFile 的路徑時，請鍵入計畫在保存中繼憑證時使用的路徑和檔案名。 通常建議將中繼憑證保存在 WHM 已保存主證書的目錄中。

4. 將更改保存到設定檔中
5. 將中繼憑證檔保存到伺服器:

   驗證中繼憑證檔（DigiCertCA.crt）是否已保存到上面配置的路徑。

   6. 重啟 Apache。

故障排除:

1. 如果您的網站可公開訪問，SSL 證書測試工具可以說明您診斷常見問題。
2. 打開網路瀏覽器並使用 HTTPs 訪問您的網站。 最好同時使用 Internet Explorer 和 Firefox 進行測試，因為如果沒有安裝中繼憑證，Firefox 會給你一個警告。 您不應該收到任何瀏覽器警告或錯誤。 如果您立即收到有關該網站不可用的瀏覽器消息，則 Apache 可能尚未在埠 443 上偵聽。 如果您的 Web 請求需要很長時間，然後超時，則防火牆會阻止 TCP 埠 443 上的流量到達網路伺服器。

如果收到「不信任」警告，請查看證書以查看它是否是您期望的證書。 檢查「主題」，「頒發者」和「有效期」欄位。 如果證書是由 DigiCert 頒發的，那麼您的 SSLCertificateChainFile 未正確配置。