How to create a certificate signing request (CSR) and install the certificate on a Mac OS X Tiger Server

Certificate Manager helps you create a CSR to send to your designated CA.

To request a signed certificate

1. Open Server Admin.

2. In the Computers & Services list, select the server you are requesting a certificate for.

3. Click Settings.

4. Click Certificates.

5. Click the Add (+) button.

6. Fill out identity information.

The common name is the fully qualified domain name of the server which uses SSL enabled services.

7. Enter starting and ending validity dates.

8. Select a private key size (2048-bit is recommended).

9. Enter a passphrase for the private key and click Save.

This passphrase should be more secure than a normal password. You should use at least 20 characters, including mixed case, numbers, and punctuation. Do not repeat characters and do not use words contained in the dictionary.

10. Click Request Signed Certificate.

11. Follow the onscreen directions for requesting a signed certificate from Entrust.

12. Click Send Request.

13. Click Done.

14. When Entrust completes the order the signed certificate is included in a link on the completed email.

15. Click Add Signed Certificate.

16. From your Entrust pickup link, copy the characters from ==Begin Certificate== to ==End Certificate== into the text box.

17. Click OK.

18. Click Save.

When the certificate is implemented for the server, you have to tell which Web site will use this certificate. Go in Server Admin > ConnectToYourServer > Web > Settings > Sites (this is the path for Tiger server). Then choose your site from the list and click the edit button, then go to the Security tab. Check the Enable Secure Sockets Layer (SSL) checkbox and select the certificate from the drop-down list. Click Save, then reset your Web server and you are done.

TN 6803 - Why does nothing happen when I try to install certificate in Mac OS X Server?

PROBLEM

Why does nothing happen when I attempt to install my Certificate into Mac OS X 10.4 server?

EXPLANATION

This happens when there is a corrupted key chain. The certificate cannot be installed but the Operating System does not log an error

SOLUTION

This is actually a work-around. What you will be doing is removing any traces left over from a previous certificate then creating a new keychain and installing the certificate. The steps are as follows:

1. Launch Server Admin

1.1. Stop any services that use the SSL certificate (Web, Mail, Etc.)

1.2. Delete the old certificate from the Computer's Settings->Certificates pane.

1.3. Quit Server Admin

2. Run Keychain Access (/Applications/Utilities)

2.1. Click the "Show Keychains" button in the bottom-left corner

2.2. Select the "System" Keychain

2.3. Delete the old certificate items (e.g. www.hostname.com), there will be a "certificate", "private key" and possibly a "public key" kind of items to delete.

2.4. Quit Keychain Access

3. Launch Server Admin again

3.1. Go to the Computer's Settings->Certificates pane again.

3.2. Import the new certificate using the CRT file and the private KEY file.

3.3. If an error occurs, try steps 1 & 2 again.

3.4. Quit Server Admin again

4. Run Keychain Access again

4.1. Select the "System" Keychain

4.2. Highlight the new Certificate type for your hostname, look at the top and verify the dates. This tells you that you got the right certificate imported.

4.3. Quit Keychain Access

5. Launch Serve Admin

5.1. Select your SSL enabled services and verify that they still have the certificate selected.

5.2. Launch your SSL enabled services

5.3. Check to make sure they work properly. Specifically, Run Safari, go to your SSL page and click the Lock in the top-right corner. Verify the dates are correct.

5.4. If an error occurs, try all the steps again, but try including a reboot of the machine between steps 2.4 and 3.