

### **Requesting a Certificate From a CA**

The manager helps you create a certificate signing request (CSR) to send to your designated CA.

1. In Server Admin, select the server which has services that support SSL.
2. Click Settings.
3. Select the Certificates tab.
4. Click the Add (+) button.
5. Fill out identity information.

The common name is the fully qualified domain name of the server which will use SSL-enabled services.

6. Enter starting and ending validity dates.
7. Select a private key size (1024 bits is the default).
8. Enter a passphrase for the private key.
9. This passphrase should be more secure than a normal password.

It is recommended you use at least 20 characters, include mixed case, numbers and/or punctuation, have no characters repeat, and having no dictionary terms.

10. Click "Request Signed Certificate...."
11. Follow the onscreen directions for requesting a signed certificate from your chosen CA.

For example, you may need to do it online or enter the email address.

12. Click Send Request.
13. Click Save.
14. When the CA replies to the email, it will include it in the text of an email.
15. Make sure the Identity is open from the Certificates tab, again.
16. Click Add Signed Certificate.
17. Copy the characters from "===Begin CSR==" to "===End CSR==" into the text box.
18. Click OK.
19. Click Save.

### **To set up SSL for a website:**

1. In Server Admin, click Web in the list for the server you want.
2. Click Settings in the button bar.
3. In the Sites pane, double-click the site in the list.

4. In the Security pane, select Enable Secure Sockets Layer (SSL).

When you turn on SSL, a message notes that the port is changed to 443.

5. Type the location of the SSL log file in the SSL Log File field.

You can also click the Browse button to locate the folder you want to use.

If you are administering a remote server, file service must be running on the remote server to use the Browse button.

6. Choose the certificate you want in the pop-up menu.

The name of the certificate must match the virtual host name if the certificate is protected by a passphrase. If the names don't match, web service won't restart.

Note: For details on editing the certificate details, see the Appendix, "Certificates and Security," in the mail service administration guide.

7. If you choose Custom Configuration or want to edit a certificate, you may need to do the following:

a Click the Edit button and supply the correct information in each field for the certificate.

b If you received a ca.crt file from the certificate authority, click the Edit button and paste the text from the ca.crt file in the Certificate Authority File field.

Note: The ca.crt file may be required but not sent directly to you. This file should be available on the website of the certificate authority.

c Type a passphrase in the Private Key Passphrase field and click OK.

8. Click Save.

9. Confirm that you want to restart web service.

Server Admin allows you to enable SSL with or without saving the SSL password. If you did not save the passphrase with the SSL certificate data, the server prompts you for the passphrase upon restart, but won't accept manually entered passphrases. Use the Security pane for the site in Server Admin to save the passphrase with the SSL certificate data.