For information about how to use Key Manager, see the section "Securing Data Transmissions with Secure Sockets Layer (SSL)" in Chapter 5, "Securing Your Site Against Intruders," of the Product Documentation.

Create a New Key

Fill in the information in this dialog box and click OK to create two files. The first file is a key file containing a key pair. The second file is a certificate request file. When your request is processed, the provider will return a certificate to you.

Key Name Assign a name to the key you are creating.

Password Specify a password to encrypt the private key.

Bits By default, Key Manager generates a key pair 1024 bits long. To specify a key that is 512 or 768 bits long, make the proper selection in this box.

Organization Preferably International Organization for Standardization (ISO)-registered top-level organization or company name.

Organizational Unit Your department within your company, such as Marketing.

Common Name The domain name of the server, for example, www.*mycompany*.com.

Country Two letter ISO Country designation, for example, US, FR, AU, UK, and so on.

State/Province Type in your the full name of your state or province, do not abbreviate. For example, Washington, Alberta, California, and so on.

Locality Type in the full name of the city where your company is located, such as Redmond or Toronto.

Request File Type the name of the request file that will be created, or accept the default. The default copies the Key Name you have designated and attaches an .req extension to it to create the request file name. For example, if you have typed security in the Key Name box, the default request file name will be security.req.

Note Do not use commas in any field. Commas are interpreted as the end of that field and will generate an invalid request without warning.

When you have filled in all the information, click OK. Retype your password when prompted and click OK. Your key will appear in the Key Manager window under the computer name

See also: For procedures and information about how to use Key Manager, see "Securing Data Transmissions with Secure Sockets Layer (SSL)" in Chapter 5, "Securing Your Site Against Intruders," in the Product Documentation.

Choose an IP Address

Select the Internet Protocol (IP) address of the server to which you want to apply the Secure Sockets Layer key, or type in the IP address.

See also: For procedures and information about how to use Key Manager, see "Securing Data Transmissions with Secure Sockets Layer (SSL)" in Chapter 5, "Securing Your Site Against Intruders," in the Product Documentation.

Connect to a Server

This dialog box lets you create a key request file and key pair for a remote server.

Server Name Type the computer name of the server you want to connect to.

See also: For procedures and information about how to use Key Manager, see "Securing Data Transmissions with Secure Sockets Layer (SSL)" in Chapter 5, "Securing Your Site Against Intruders," in the Product Documentation.

Send for a Certificate

To find out how to get a VeriSign certificate, connect to VeriSign's Web site, www.verisign.com.

See also: For procedures and information about how to use Key Manager, see "Securing Data Transmissions with Secure Sockets Layer (SSL)" in Chapter 5, "Securing Your Site Against Intruders," in the Product Documentation.

Connects to the specified server.

Disconnects from the selected server.

Records changes to a key on the specified server.

Creates a new key.

Renews a previous request for a key certificate.

Installs a new key once you have received the certificate.

Deletes the selected key.

Help not available for this topic.

Help not available for this topic.

Help not available for this topic.

Help not available for this topic.

Help not available for this topic.

Help not available for this topic.

Help not available for this topic.

Help not available for this topic.