Key Manager

You can use Key Manager to create and manage SSL *key pair* files, necessary for establishing encrypted communication links with remote users. Additionally, you can also use Key Manager to generate a request for a *server certificate,* which is a digital identification file essential for activating the SSL key pair. Without installing and attaching a valid server certificate "attached" to your key pair, you cannot use your server's SSL security features.

The Server Certificate

A server certificate contains identification information about you or the organization responsible for a Web site's content. The server certificate provides a way wherein users can authenticate your Web site and establish an SSL secured communication link. You can obtain a server certificate from a mutually trusted, third-party organization, called a *certificate authority.* A certificate authority requires you to provide a detailed identification information before issuing a valid server certificate. After you receive a certificate file, you can use Key Manager to install the server certificate.

The SSL Key Pair

Using Key Manager, you create an SSL key pair, which is necessary for establishing a secure communication link. The key pair consists of a file called a *public* key and a *private* key. The key pair is used to "negotiate" a secure SSL connection with a user`s Web browser, not to encrypt transmitted information.

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 A department within your company, such as Marketing.

Common Name The domain name of the server, for example, www.microsoft.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 a .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.

Backing up SSL Key Pair Files

Your SSL key pairs are vital for ensuring that your encrypted communications remain secure. Key pairs, bound to a valid server certificate, provide a highly reliable and unique identification for your Web sites. An unauthorized individual with access to your key pair could significantly compromise your secure communications and transactions.

Because of the security importance of the SSL key pair, and in some cases, the expense related to obtaining a valid server certificate, you should take every effort to safeguard your key pair from accidental loss or theft.

To backup your SSL key pair

1. Select the key.
2. In the **Key** menu, select **Export Key**, then click **Backup File**.
3. In the **Key Manager** warning dialog box, read the warning message, then click **OK**.
4. Save your key pair file using a .txt extension.

Note

You should save your key pair file in a directory protected with appropriate Windows NT File System (NTFS) permissions that restrict unauthorized access, or on a disk that you can store in a secure location.

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.

Connect To Computer

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

Computer Type the computer name of the server you want to connect to.

Send for a Certificate

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

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.