

## How to: Install an SSL certificate

---

### Introduction

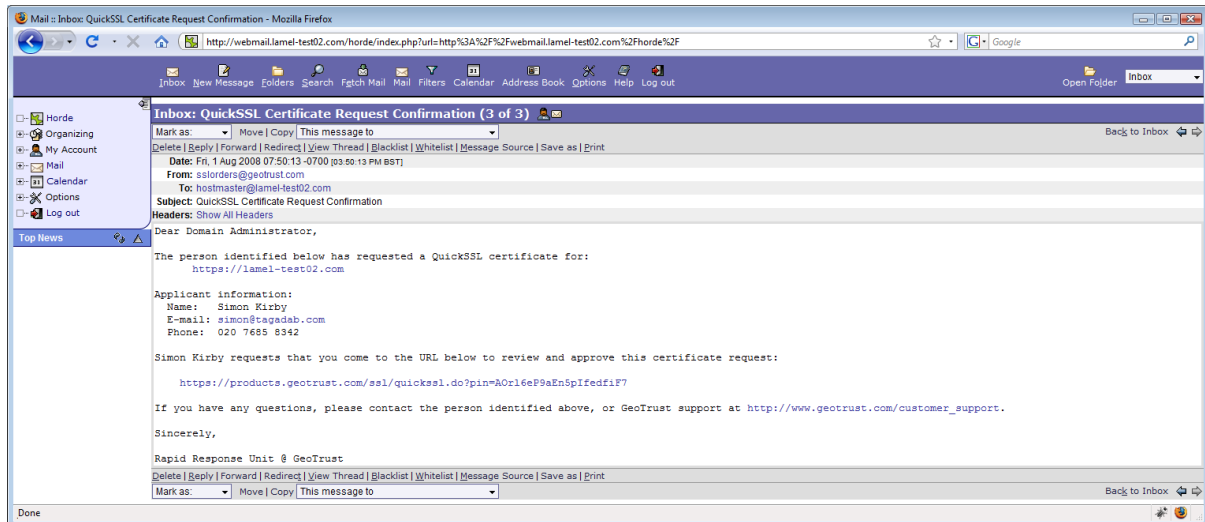
This document will talk you through the process of installing an SSL certificate on your server. Once you have approved the request for your certificate and your Control Panel has all of the certificate details, you will need to follow instructions specific to your web server. You'll be able to find the instructions you need by referring to the contents section of this document.

### Table of Contents

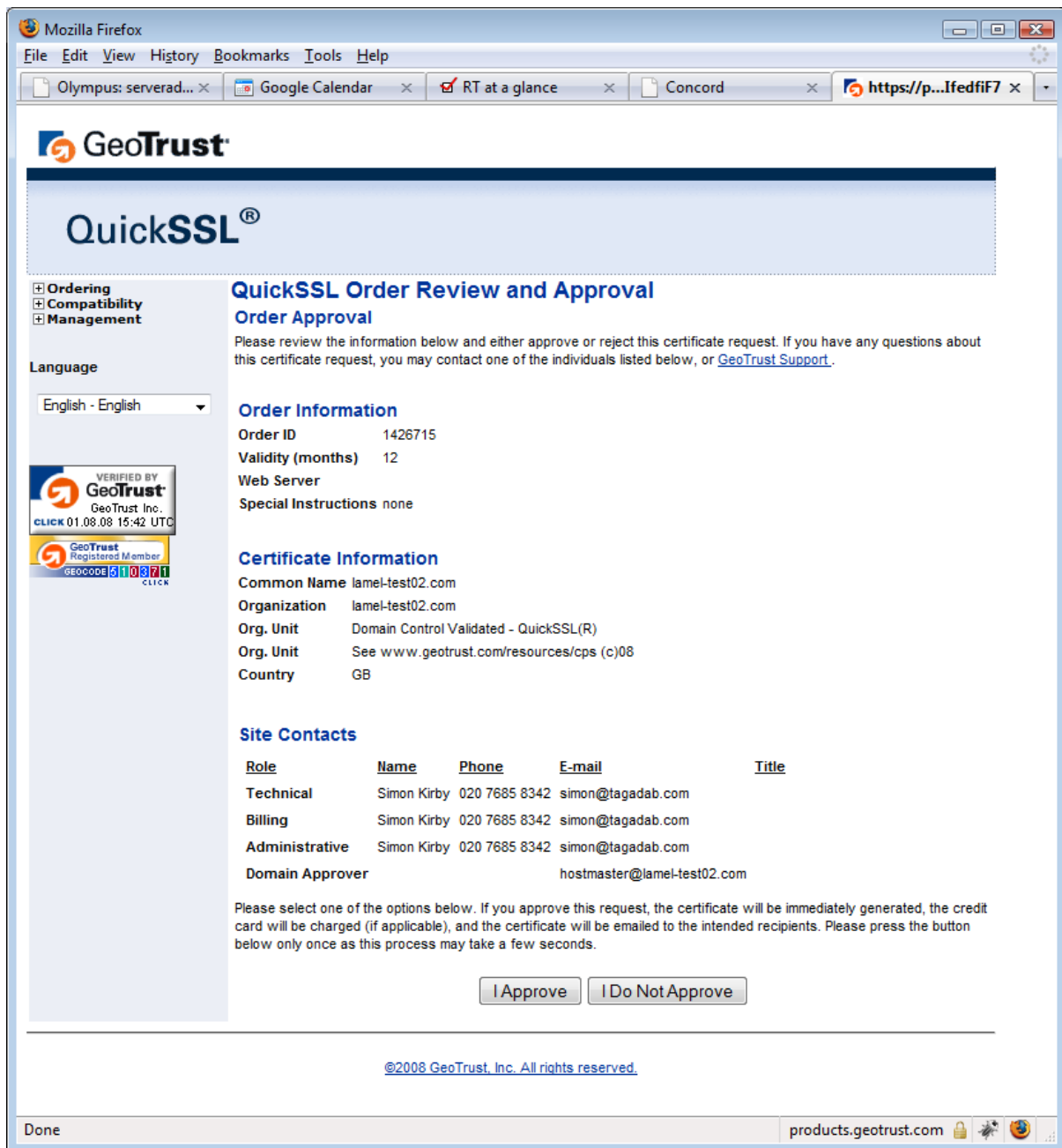
How to: Install an SSL certificate.....	1
Introduction .....	1
Table of Contents.....	1
Approving the SSL certificate request.....	2
Installing a SSL certificate in Apache for Linux.....	6
Installing a SSL certificate in IIS for Windows .....	8
Converting your Certificate and Private Key to .p12 format .....	8
Installing the .p12 Certificate .....	9
Importing the .p12 Certificate .....	12
Installing the .p12 certificate in IIS.....	14
Installing a SSL certificate using the Plesk Control Panel.....	19

## Approving the SSL certificate request

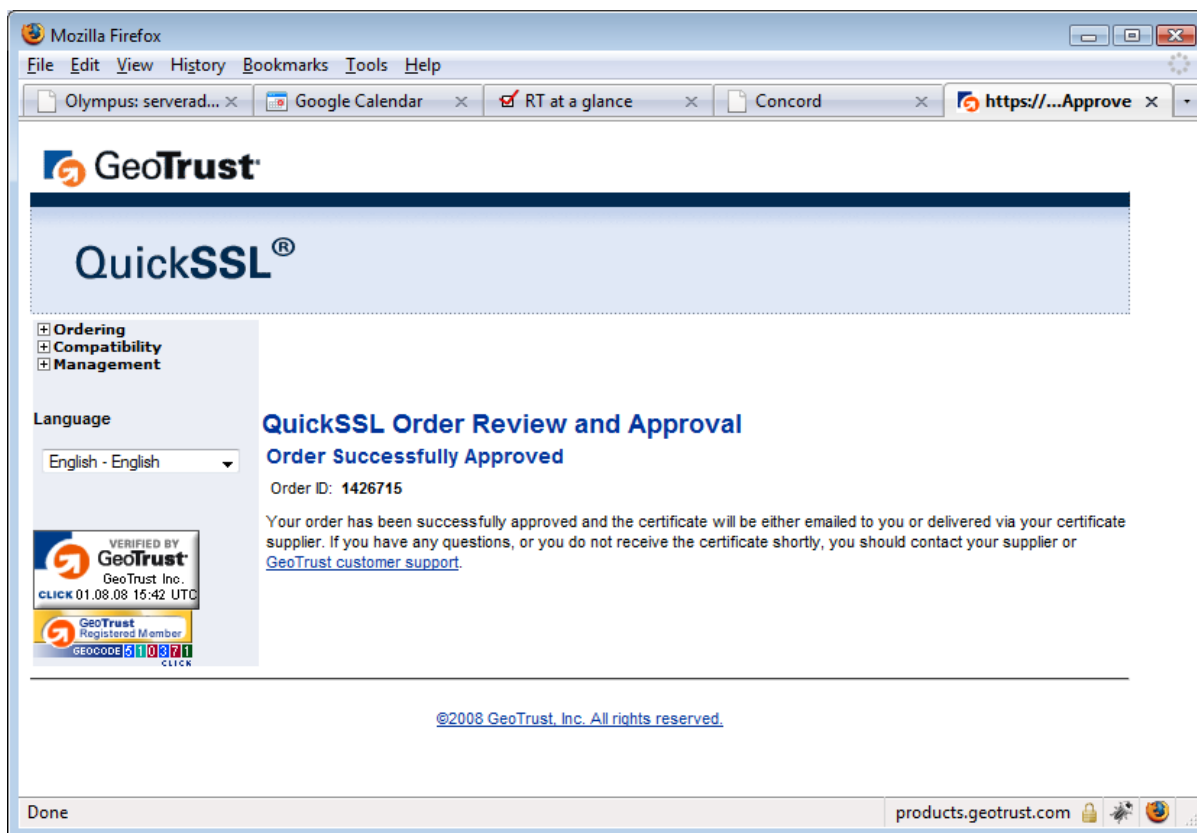
After you have ordered an SSL certificate, the 'Approver E-mail Address' you specified during the order process will receive an approval request e-mail (see our article on ordering SSL certificates at: [http://www.tagadab.com/support\\_pdf/ssl\\_01.pdf](http://www.tagadab.com/support_pdf/ssl_01.pdf)). The text of the approver e-mail will look similar to that in the screen shot below:



Click the approval link provided to be taken to the issuing authorities' website.



Your SSL certificate approval screen will look similar to the above. Click the 'I Approve' button and your certificate will be generated and sent to us. If your approval has been processed correctly you will see the screen below.



After you have approved your certificate, we will be sent the certificate file and will then manually upload it to your Customer Control Panel. This can take up to one working day but will usually be much sooner. If you still don't have your full certificate one working day after approving it, please e-mail [hostmaster@tagadab.com](mailto:hostmaster@tagadab.com) and request an update.

When your certificate has been fully provisioned, you will see it with a 'live' status in your control panel:



The screenshot shows a web browser window titled "Service Groups - Opera" with the URL [https://control-panel.tagadab.com/control\\_panel/service\\_groups?type=ssl\\_certs](https://control-panel.tagadab.com/control_panel/service_groups?type=ssl_certs). The page features the Tagadab logo and navigation menu: Home, Dedicated Servers, Hosting, Domains, SSL Certs, Support. A user is logged in as Nick Amoki. The "Your Services" section contains text about SSL certificates and a "here" link. A table lists one certificate for lamel-test02.com with status "live" and expiry date "02-08-2009". A "View" link is provided for this certificate. A padlock icon with an 'X' is also visible.

Certificate	Status	Expiry date	View
lamel-test02.com	live	02-08-2009	<a href="#">View</a>

© 2008 Tagadab

Click the 'view' link to see both the Certificate and Private Key that make up your certificate. You can click the appropriate 'download' link to download the certificate in .crt format, and the private key in .key format. Once you have these files, you are all set to install your certificate on your web server.

## Installing a SSL certificate in Apache for Linux

Follow the steps below to install your SSL certificate for your website.

1. Save the certificate and private key files as **<your domainname>.cert** and **<your domainname>.key** respectively. Note: The examples below use the following naming conventions: "Your Private Key" = "**domainname.key**"; "Your Web Server Certificate" = "**domainname.cert**"

2. Copy the certificate to the Apache server directory in which you plan to store your certificates (this can be any folder which Apache has permissions for, but is usually: /usr/local/apache/conf/ssl.crt/ or /etc/httpd/conf/ssl.crt/ for certificates and /usr/local/apache/conf/ssl.key/ or /etc/httpd/conf/ssl.key/ for private keys).

3. Open the Apache httpd.conf file in a text editor (NOTE Ubuntu users should instead open the apache2.conf file). Locate the SSL VirtualHost associated with your certificate. Verify that you have the following 2 directives within this virtual host. Please add them if they are not present:

```
SSLCertificateFile /usr/local/apache/conf/ssl.crt/domainname.crt (or the path to your cert)
SSLCertificateKeyFile /usr/local/apache/conf/ssl.key/domainname.key (or the path to your key)
```

Note that some instances of Apache will store Virtual Host information in a ssl.conf file. If your httpd.conf contains no Virtual Host information then you will need to locate and amend the ssl.conf as above.

4. Save the changes and exit the editor.

5. Start or Restart your apache web server.

### Additional information

Your httpd.conf should contain some or all of the following directives (for an IP based site). Those directives marked in bold are SSL related. Those directives marked in italics should only be used for troubleshooting.

```
<VirtualHost 192.168.1.1:443>
DocumentRoot /var/www/html
ServerName 192.168.1.98
ServerAdmin someone@your.domain
ErrorLog /etc/httpd/logs/ssl_error_log
TransferLog /etc/httpd/logs/ssl_access_log
SSLEngine On
SSLCertificateFile /etc/httpd/conf/ssl.crt/domainname.crt
SSLCertificateKeyFile /etc/httpd/conf/ssl.key/domainname.key
SSLSessionCache dbm:/var/cache/httpd/ssl_cache
SSLSessionCacheTimeout 300
SetEnvIf User-Agent ".MSIE.*" nokeepalive ssl-unclean-shutdown downgrade-1.0 force-response-
```

## 1.0

</VirtualHost>

SSLSessionCache & SSLSessionCacheTimeout prevent known issues with Mac Internet Explorer compatibility with Apache. You are only advised to add these directives if you are experiencing Mac compatibility issues.

SetEnvIf User-Agent fixes the Intermittant Server Errors associated with some versions of Windows Internet Explorer. You are only advised to add this directive if you are experiencing compatibility issues with old versions of Internet Explorer.

For more information about configuring Apache, please review [http://httpd.apache.org/docs-2.0/mod/mod\\_ssl.html](http://httpd.apache.org/docs-2.0/mod/mod_ssl.html)

6. Test your certificate by using a browser to connect to your server. Use the https protocol directive (e.g. https://your server/) to indicate you wish to use secure HTTP. The padlock icon on your browser will be displayed in the locked position if your certificates are installed correctly and the server is properly configured for SSL.

## Installing a SSL certificate in IIS for Windows

To install your certificate on a Windows Server you will need to first convert it into a compatible format (the .p12 format). Once you have the .p12 file you will be able to import it into IIS in the usual way.

## Converting your Certificate and Private Key to .p12 format

You can convert PEM files to .p12 files using openssl. This can either be done on a Linux server running Apache (with mod SSL) or you can install openssl on your Windows server (or any Windows machine) and convert the file there.

To install openssl on a Windows machine, browse to:

<http://www.slproweb.com/products/Win32OpenSSL.html>

You want to download and run the [Visual C++ 2008 Redistributables](#) and [Win32 OpenSSL v0.9.8i Light](#) packages (see screenshot below).

The screenshot shows a web browser window displaying the 'Win32 OpenSSL' website. The browser's address bar shows 'Shining Light Productions - Win32 OpenSSL - Mozilla Firefox'. The website has a yellow header with the 'Shining Light Productions' logo and navigation links for 'Home', 'Products', 'Support', and 'About'. The main content area is divided into several sections:

- Win32 OpenSSL:** A paragraph describing the installation project and a 'LEGAL NOTICE'.
- System Requirements:** A table comparing minimum and recommended system requirements.
- Win32 OpenSSL Screenshot:** A placeholder for a screenshot of the installer.
- Download these packages:** A callout box pointing to a table of download links.

The 'Sponsors & Donators' sidebar on the right lists 'Businesses' (DTH Software, Custom Billing Software) and 'Individuals' (Bryon Eldridge, Martin Balk, Ehsan F., Daya Puls, Art Kominos, Kenneth Brobst).

File	Size	Description
<a href="#">Win32 OpenSSL v0.9.8i Light</a>	1MB Installer	Installs the most commonly used essentials of Win32 OpenSSL v0.9.8i (Recommended for most users by the creators of OpenSSL). Note that this is a default build of OpenSSL and is subject to local and state laws. More information can be found in the legal agreement of the installation.
<a href="#">Visual C++ 2008 Redistributables</a>	1.7MB Installer	Having problems with error messages when trying to run OpenSSL? This will likely fix the problem. Only works with Windows 2000 and later. Although there is a "newer version" of this installer, this is the <b>correct</b> version to install.

Feel free to donate to the author of the site – if it weren't for him you'd probably have to compile the package from binaries!

You will now need to obtain your certificate in PEM format from your Control Panel. Browse to <http://control-panel.tagadab.com>, login and click the 'SSL' link at the top of the page. View the certificate you wish to install and on that certificate's page click the 'Download Private Key and Certificate' link. This will then prompt you to download both the private key and the certificate in the same .pem file. Save it as '<your domainname.pem>' and copy it to the folder where openSSL installed on your server.

Next, open a command prompt (start -> run -> cmd), navigate to the folder where openSSL and your PEM file are located, and run the following command:

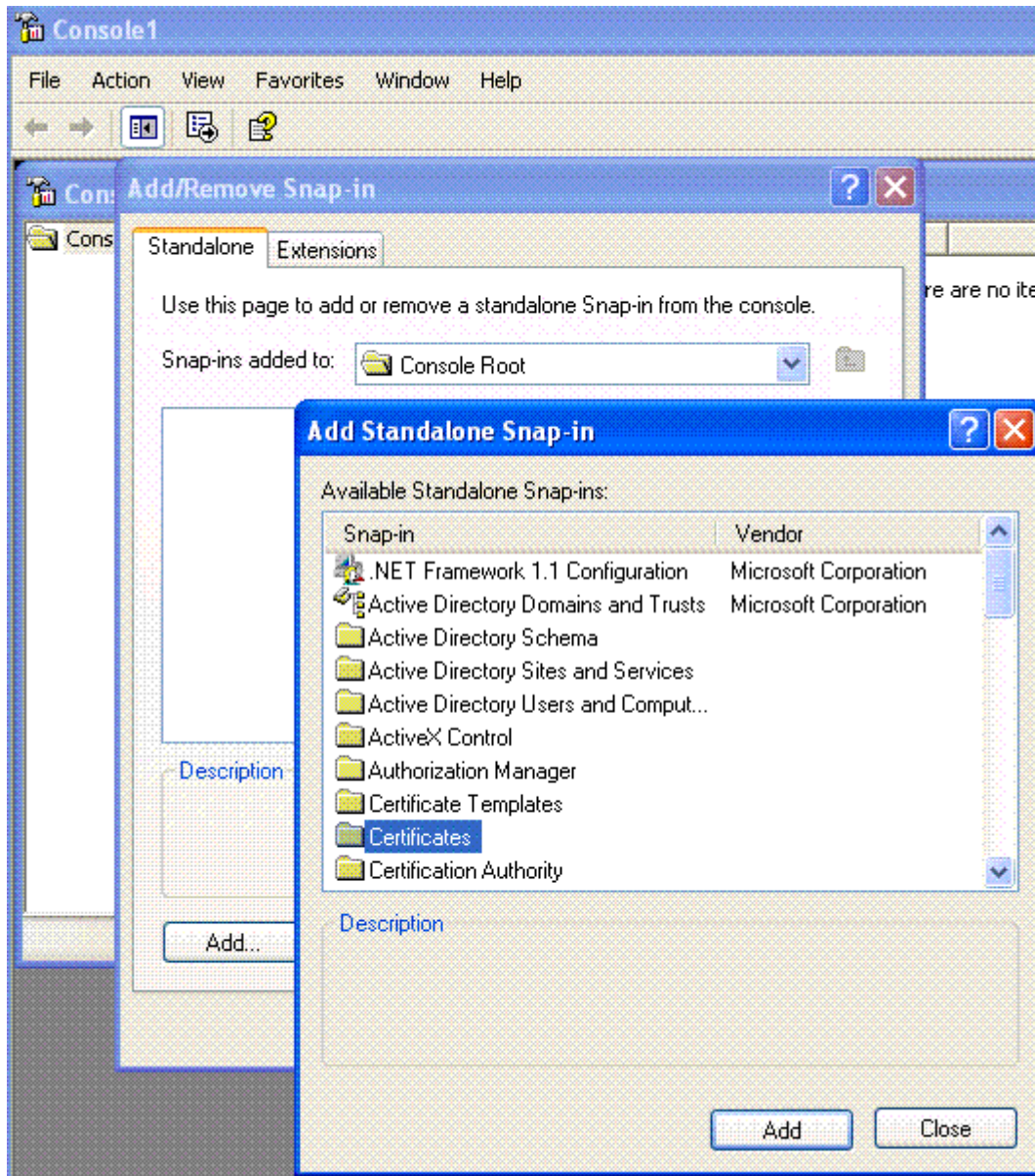
```
openssl pkcs12 -export -passout pass:"<enter a good password>" -in <your domain name>.pem  
-out <your domain name>.p12 -name "<your domain name>"
```

This will create a file of the form <your domain name>.p12 in the folder where SSL is installed. You will now be able to install this certificate using the Certificate and IIS snap-ins for the MMC.

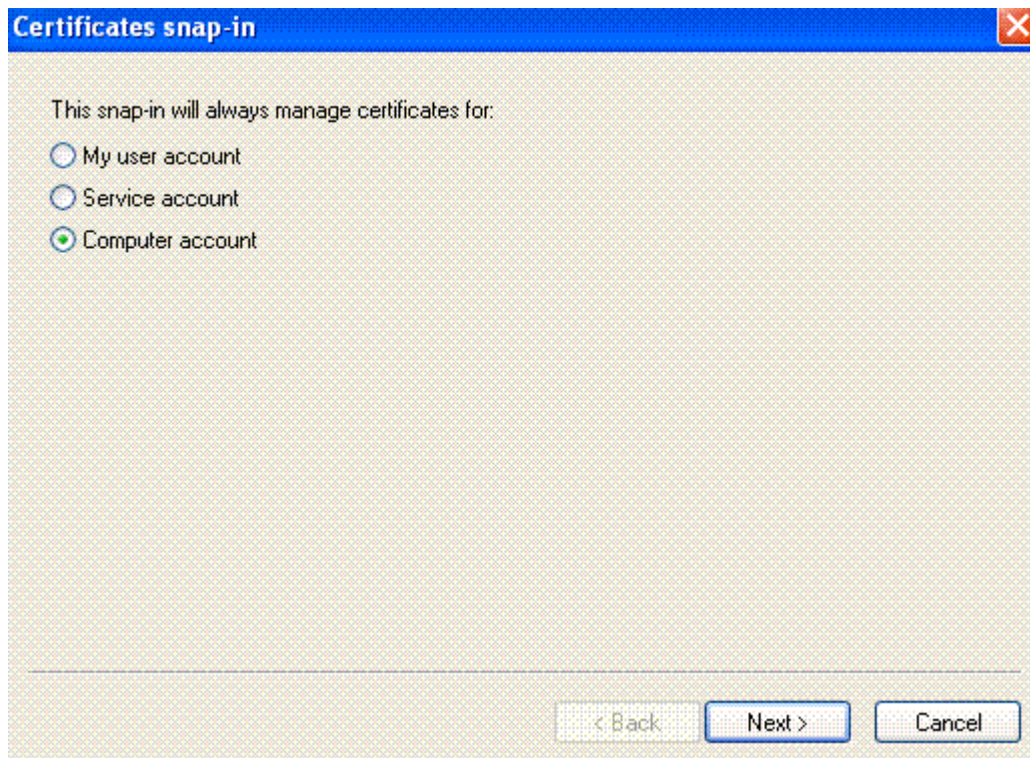
### **Installing the .p12 Certificate**

Now you have the certificate in .p12 format you can install it. To do this first open the MMC and add the Certificate snap-in:

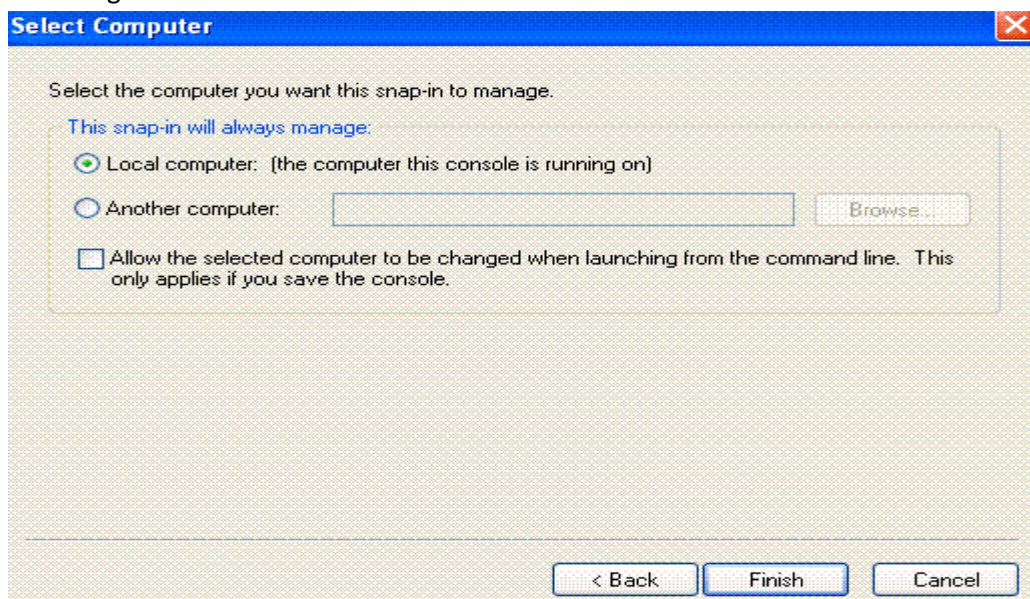
1. Go to 'Start' -> 'Run' and enter 'mmc'. Hit enter.
2. This will start the MMC. Go to the 'File' menu and select 'add/remove snap-in'.
3. Click 'Add' and select 'Certificates' from the list of snap-ins.
4. Click 'Add' to be taken to the snap-in configuration window.



- At the snap-in configuration window, select the radio button for 'Computer Account' and click the 'Next' button.



- Finally specify the computer for which you want to manage certificates. Select either local computer (for the computer you are working on) or specify the remote computer you want to manage. Then click 'Finish'.

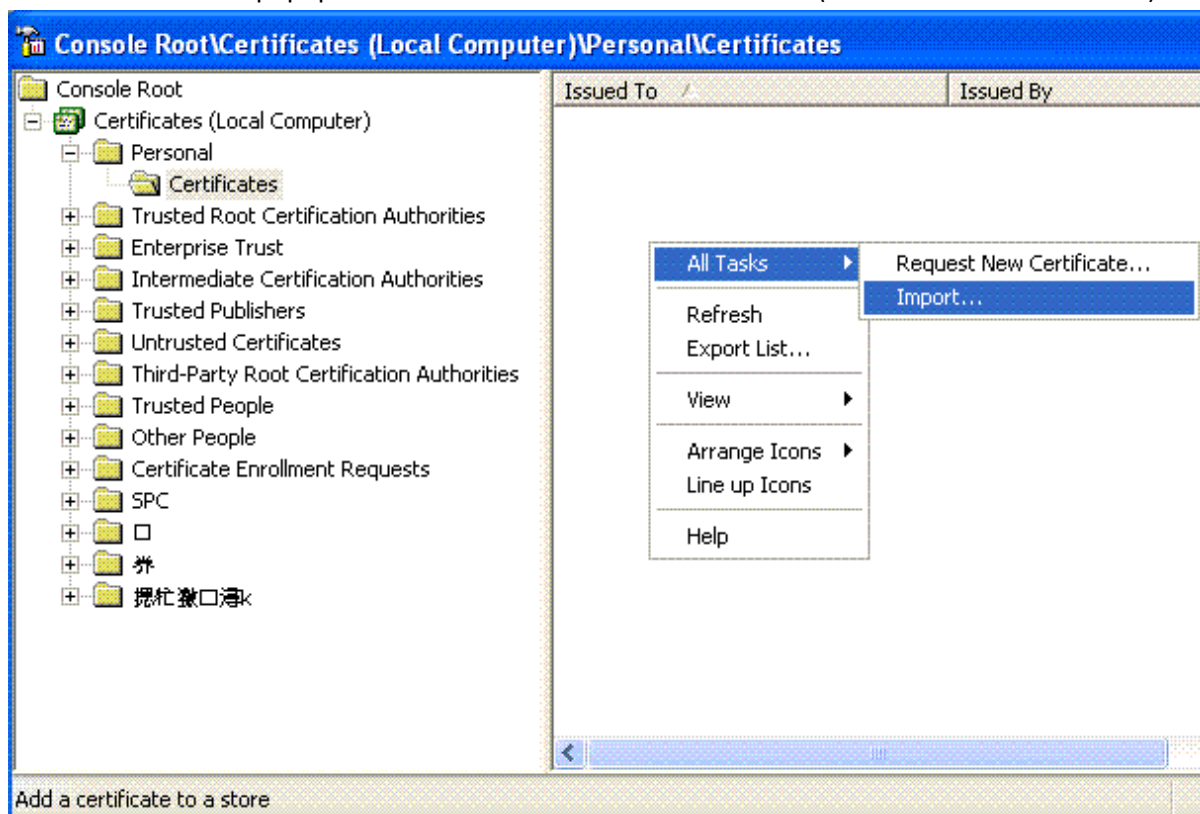


- Now you've created a Certificates management console, you can save it's settings to make using it easier in future by going to 'File'->'Save' or 'Save As'

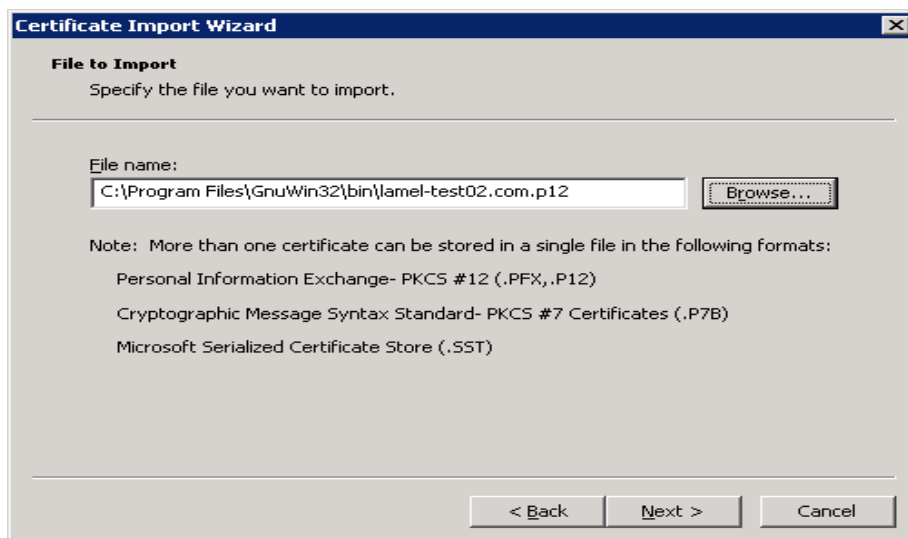
## Importing the .p12 Certificate

Now you have setup the Certificates snap-in, you need to import your .p12 certificate. To do this:

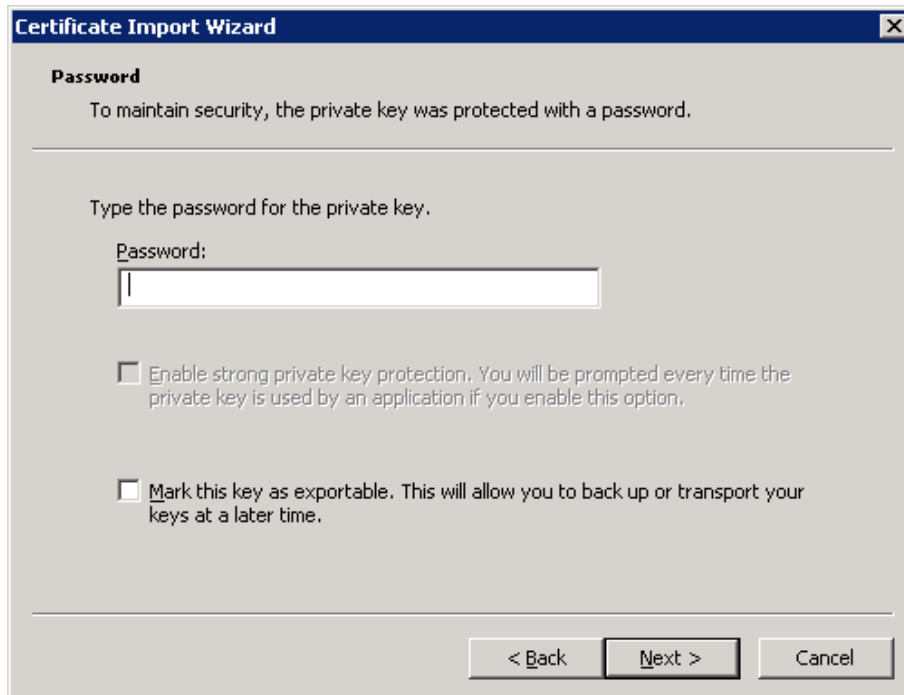
1. Expand the 'Personal' folder and right-click on 'Certificates'. Select 'All Tasks' -> 'Import...' from the popup menu (see below).



2. This will take you to the certificate Import wizard. Click 'Next' at the first window to see:



3. Click the 'Browse' button to locate your certificate. NOTE: Make sure that you set the file type to 'Personal Information Exchange (\*.pfx, \*.p12)' or you won't see your certificate. Once you have selected your certificate, click 'Next'.



**Certificate Import Wizard**

**Password**

To maintain security, the private key was protected with a password.

---

Type the password for the private key.

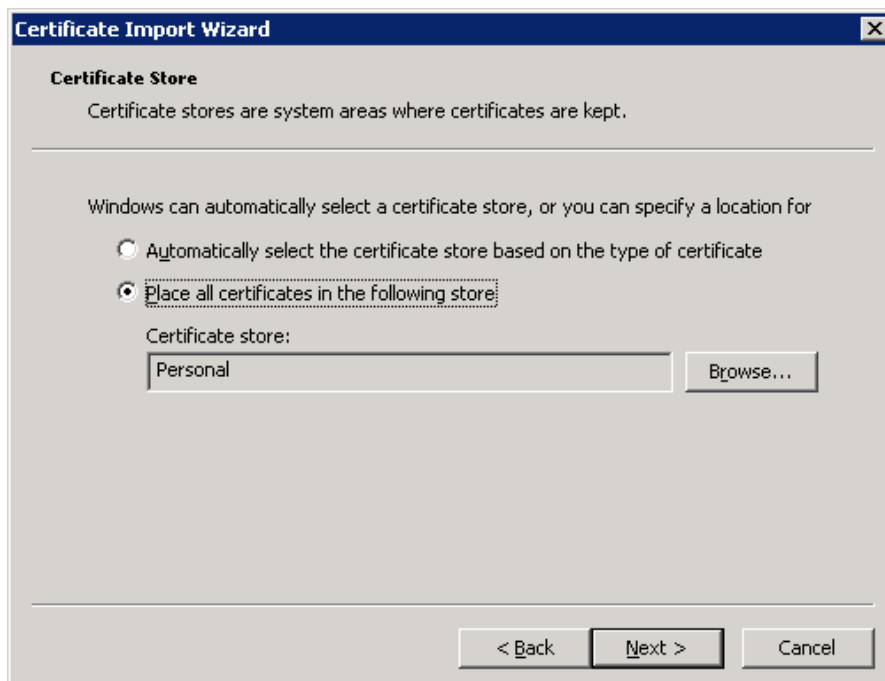
Password:

  
 Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option.

Mark this key as exportable. This will allow you to back up or transport your keys at a later time.

< Back   Next >   Cancel

4. At the window above, enter the password you specified when creating your .p12 certificate, mark the key as exportable and click 'Next'.



**Certificate Import Wizard**

**Certificate Store**

Certificate stores are system areas where certificates are kept.

---

Windows can automatically select a certificate store, or you can specify a location for

Automatically select the certificate store based on the type of certificate

Place all certificates in the following store:

Certificate store:

   Browse...

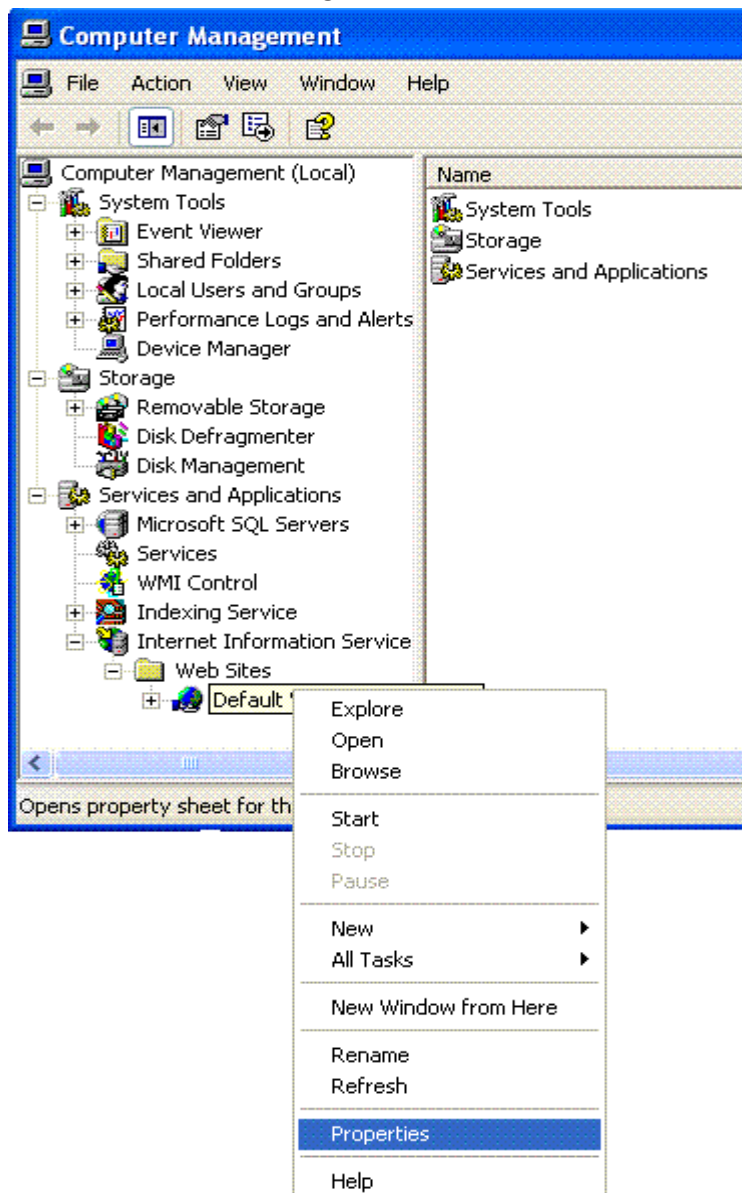
< Back   Next >   Cancel

5. At the window above, select the location in which you want to store the certificate (the default certificate store, 'Personal', is fine) and click 'Next'.
6. You will then see a screen confirming the details you have entered. Click 'Finish' to complete the process.

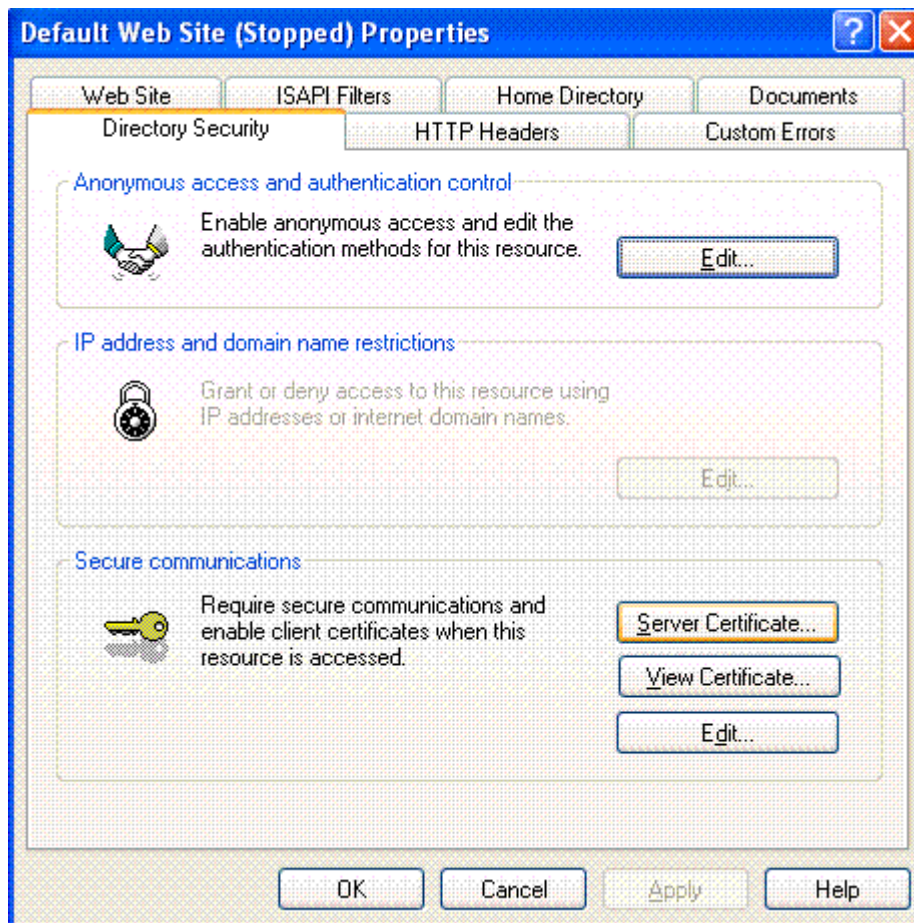
## Installing the .p12 certificate in IIS

The final stage in this process is the installation of the certificate in IIS for your website. Start up the IIS manager ('Start' -> 'Administrative Tools' -> 'Internet Information Services (IIS) Manager') and follow the steps below:

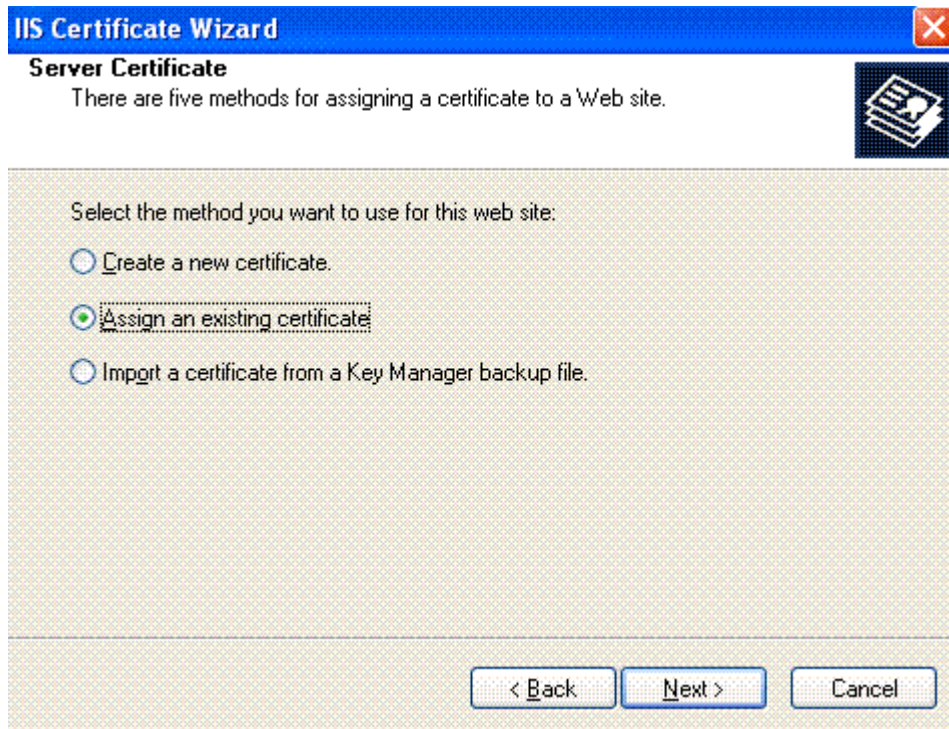
1. Select the website for which you want to install the SSL certificate from the folder tree on the left, right-click it and select 'properties'.



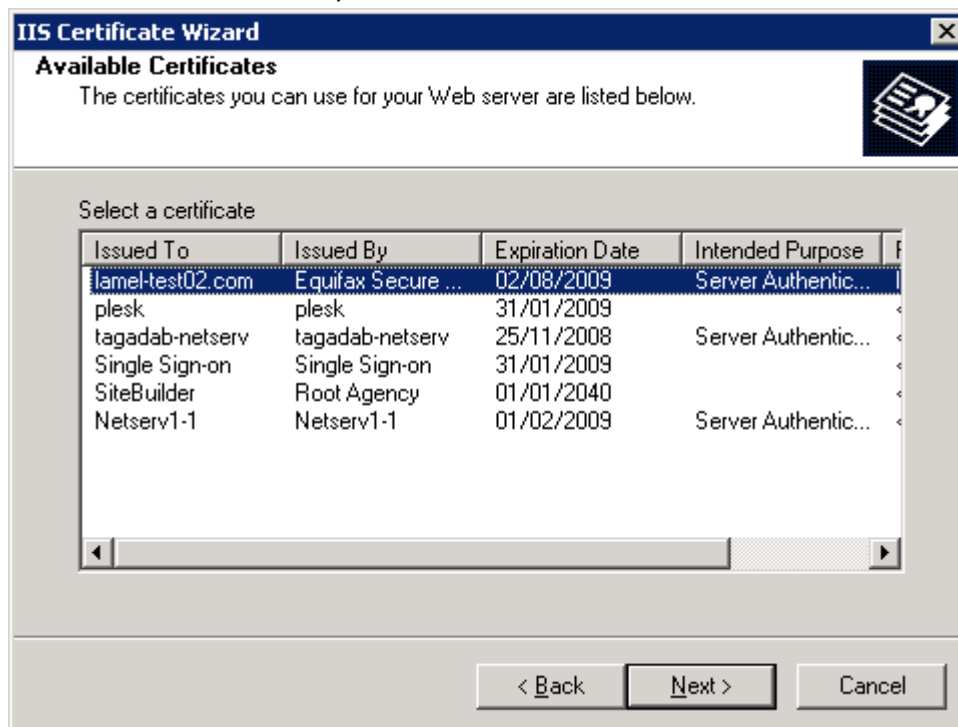
2. At the 'Properties' window, select the 'Directory Security' tab and click the 'Server Certificate' button.



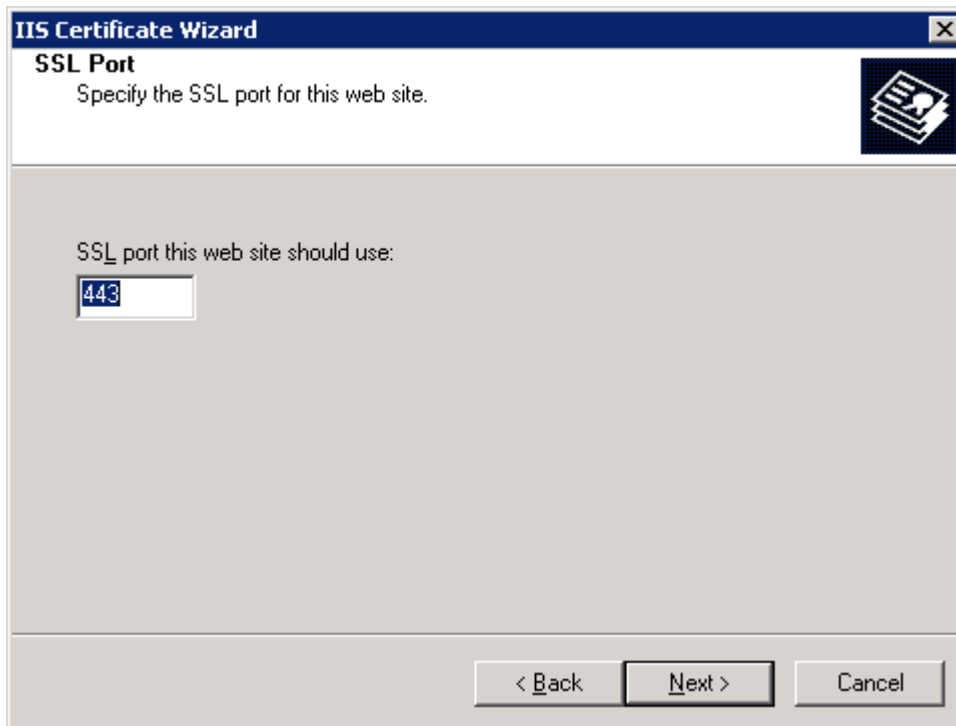
- This will start the Certificate Wizard. Click 'Next', select the 'Assign an existing certificate' radio button on the next screen and click 'Next' again.



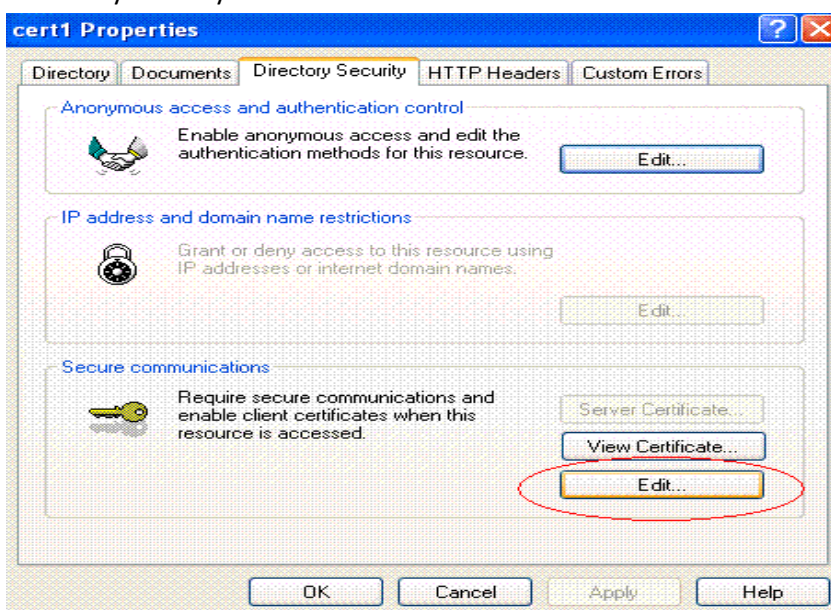
- Select the certificate you wish to install from the list and click 'Next'.



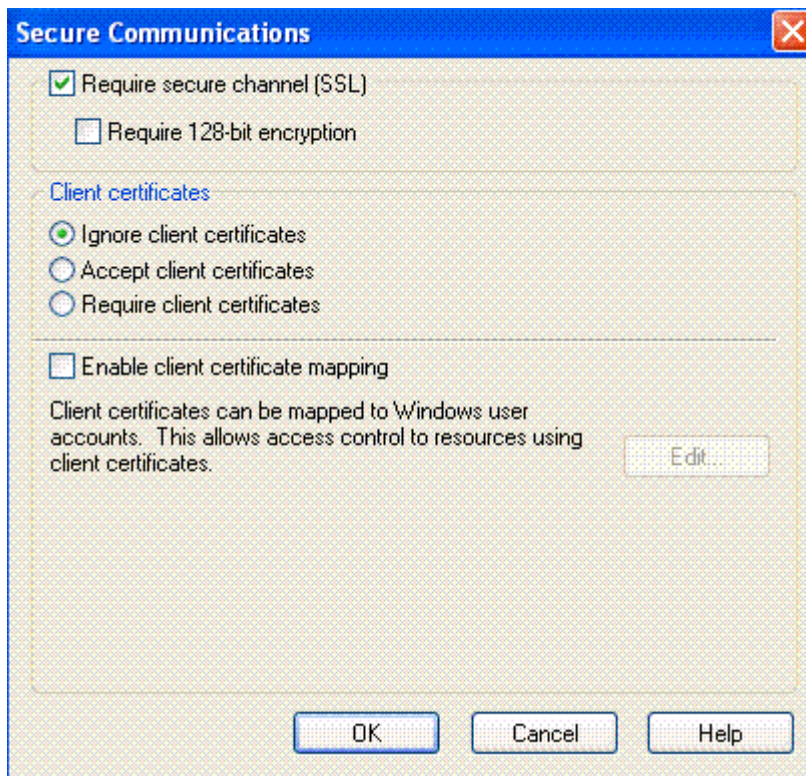
- Specify the port you wish the certificate to use. 443 is the default but if you have an application that requires a different port then enter the port number here.



- You will then be presented with the Certificate details. Check that all the details are correct and then click 'Next' and 'Finish' to complete the Wizard.
- Back in the IIS manager, right-click the folder in your website you'd like to secure (this can be any sub-folder or the root folder of the website) and select 'Properties'. Again, select the 'Directory Security' tab and this time click the 'Edit' button.



8. Check the 'Require secure channel (SSL)' checkbox. Optionally, you can also force clients to use 128-bit encryption. Unless you will require visitors to this part of your site to have their own certificates, leave the radio button for 'Ignore Client Certificates' selected. Click the okay button to finish installing your certificate!



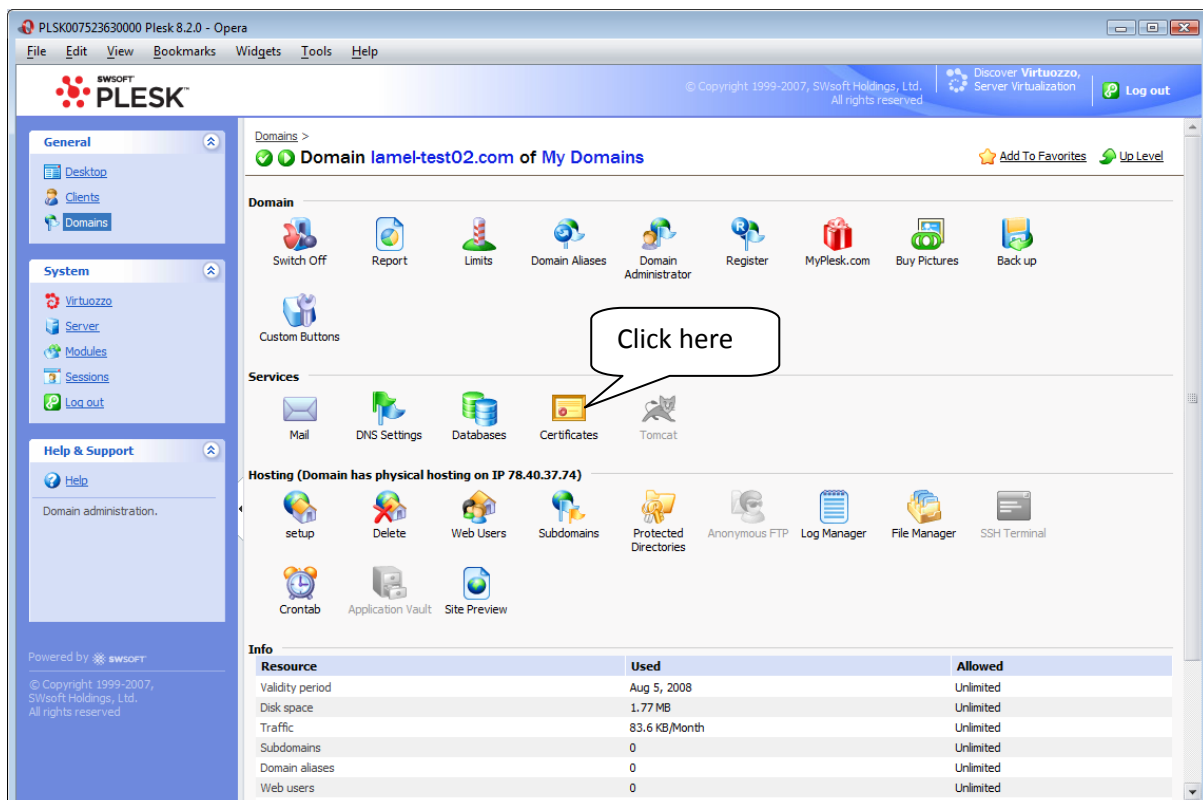
The directory you selected should now be protected by the certificate. To test this, browse to 'https://www.<your domain.tld>/<your secure directory>'. If you specified a port other than 443 for your certificate, remember to append it to the end of the URL. You should see in your browser that you are at a secure web page (typically they display padlocks and related graphics) and you should have the option of viewing the certificate in your browser.

## Installing a SSL certificate using the Plesk Control Panel

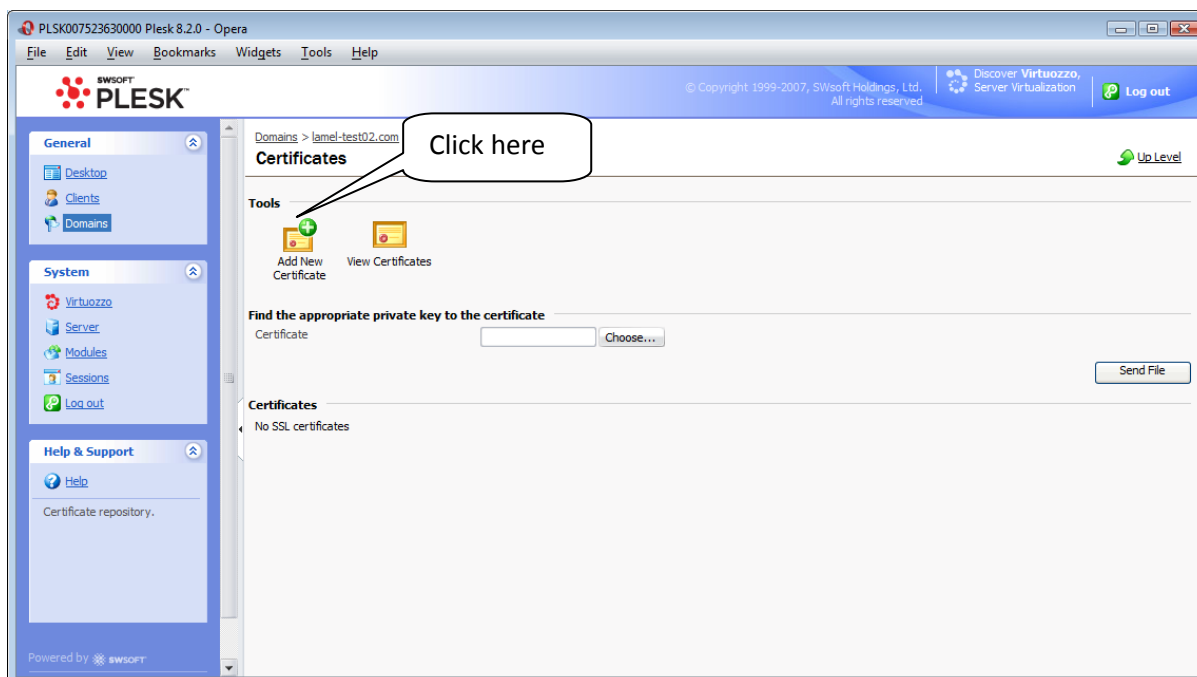
Whether you have Plesk for Linux, Plesk MSDE for Windows or Plesk MSSQL for Windows the installation process for an SSL certificate is the same (at least for the single domain certificates we're concerned with here). This guide has been written for version 8.2 of Plesk. Before we go through the steps in the Plesk GUI, you will need to have downloaded your Private Key and your Certificate from your Tagadab control panel. Instructions for how to do this are in the 'Approving the SSL Certificate Request' section at the beginning of this document.

You will also need to have an exclusive IP address assigned to the domain in Plesk. If you don't have more than one IP address, you can e-mail [dedicated@tagadab.com](mailto:dedicated@tagadab.com) and we will provide up to 4 additional address at no extra charge. Once you have these allocated you will need to add the IP addresses in Plesk and associate one of them exclusively to your domain. Consult the Plesk help documentation if you need guidance on this.

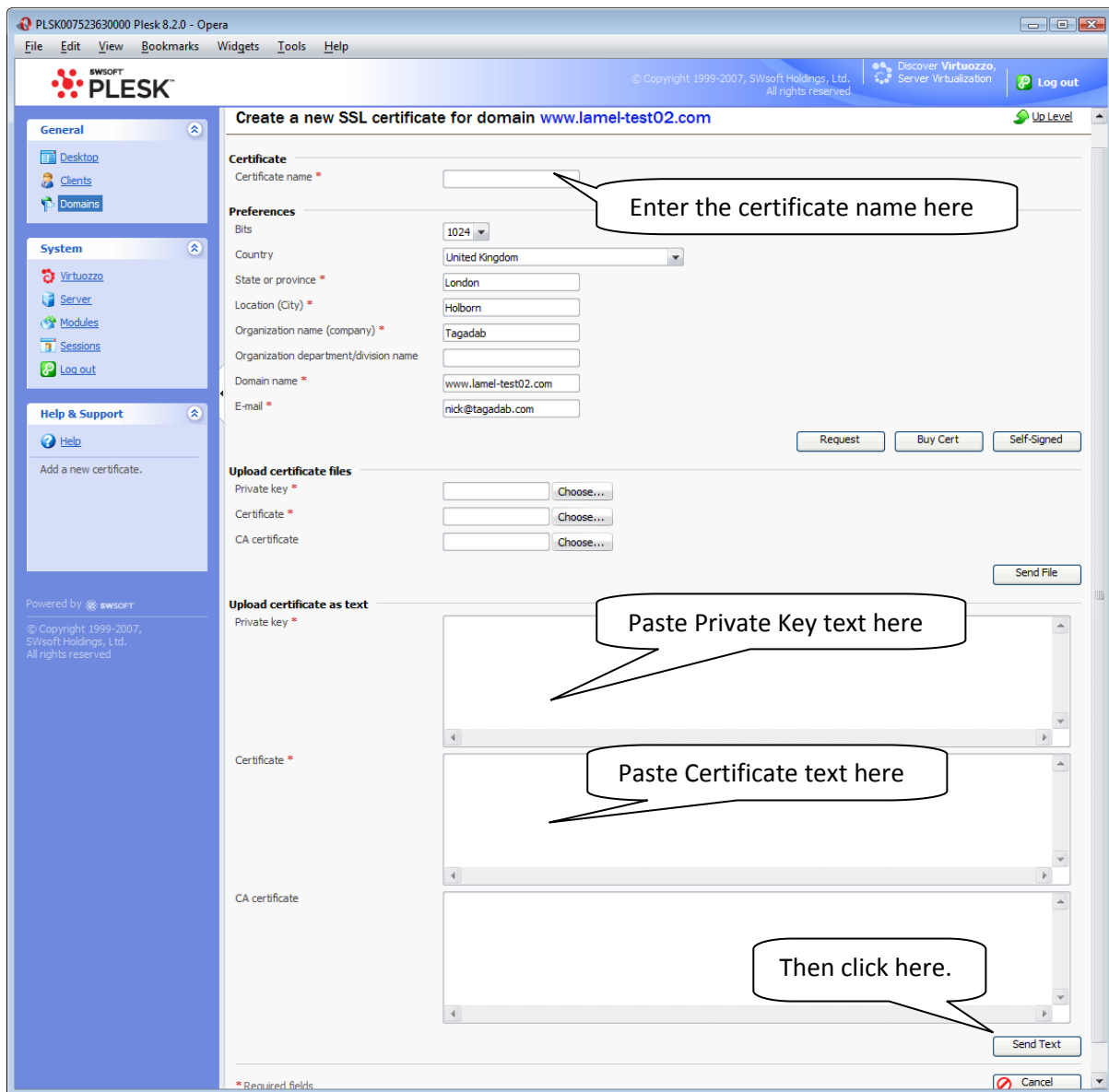
Once you have the text for both Key and Certificate, login to your Plesk control panel and navigate to the Domain page of the domain for which you are installing the certificate. It will look similar to this:



Click the 'Certificates' icon to load the Certificates page.



Click the 'Add New Certificate' icon to navigate to the Certificate creation page.



Here you will want to initially ignore all the fields except three. First, enter the certificate name at the top of the page. Then, paste the text of your private key into the 'Private Key' field of the 'Upload certificate as text' section and paste the text of your certificate into the 'Certificate' field of the same section. You can leave the 'CA certificate' blank. When pasting the text of the key and certificate ensure that in both cases you paste in the entire text, including the beginning and ending '-----Begin Certificate-----'. Also make sure that you don't paste any whitespace into the fields.

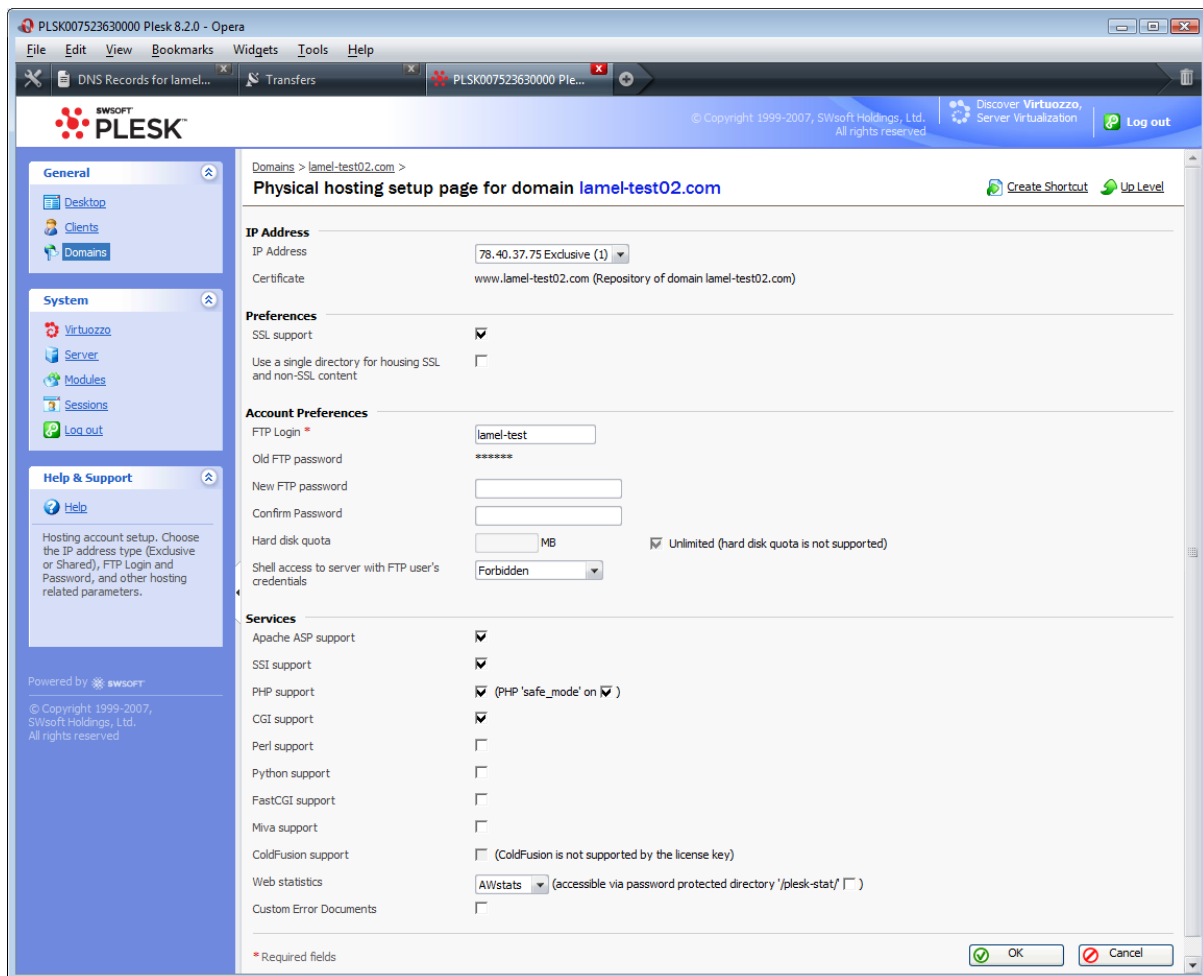
Once you're sure that you have pasted key and certificate correctly, click the 'Send Text' button. The page will update to complete the relevant remaining fields and you'll be taken back to the certificates page where you'll see your certificate listed. Your certificate is now installed, but we need to activate it for your domain. To do this, navigate back to your domain page and instead of clicking the 'Certificates' link, this time click the 'Setup' link in the Hosting section (see below).

The screenshot shows the Plesk 8.2.0 interface in a browser window. The main content area is titled 'Domain label-test02.com of My Domains'. It features several sections: 'Domain' with icons for Switch Off, Report, Limits, Domain Aliases, Domain Administrator, Register, MyPlesk.com, Buy Pictures, and Back up; 'Services' with icons for Mail, DNS Settings, Databases, and Tomcat; 'Hosting (Domain has physical host...)' with icons for setup, Delete, Web Users, Subdomains, Protected Directories, Anonymous FTP, Log Manager, File Manager, and SSH Terminal; and 'Info' with a table of resource usage.

A callout box with the text 'Click here' points to the 'setup' icon in the 'Hosting' section.

Resource	Used	Allowed
Validity period	Aug 5, 2008	Unlimited
Disk space	0 B	Unlimited
Traffic	0 B/Month	Unlimited
Subdomains	0	Unlimited
Domain aliases	0	Unlimited
Web users	0	Unlimited
Mailboxes	0	Unlimited
Redirects	0	Unlimited
Mail groups	0	Unlimited
Autoresponders	0	Unlimited
Mailing lists	0	Unlimited
Databases	0	Unlimited
Java applications	0	Unlimited

On the hosting setup page you will be able to select the Certificate you just installed for this domain. Select it and save the changes and you will see the certificate listed for the domain, as below.



Your SSL certificate is now properly configured. To test it, browse to the URL secured by your certificate and use your browser to check the certificate details.

If you have any problems with this, please e-mail [dedicated@tagadab.com](mailto:dedicated@tagadab.com) or call 0845 045 1101 between 9am and 6pm Monday to Friday.