

SSL Quick Start Guide

The world of Secure Sockets Layer (SSL) certificates can be a bit confusing, so this document was assembled to help guide users of LoadMasters through the various processes involving certificates that you may encounter.

SSL Acceleration Network Architecture

Traditionally, if a site wanted to incorporate SSL, they would install SSL certificates they received from a certificate authority (such as Verisign) on their server software (usually Microsoft's Internet Information Server (IIS) or Apache). There are a few issues with running SSL from the web servers, however. SSL requires intense cryptographic functions, and those functions can eat up a significant portion of the available CPU power available on the server. Also, if a load balancer is utilized, the load balancer can't perform cookie persistence or content switching, since the traffic the load balancer sees is encrypted.

Putting a LoadMaster in front of these web servers and terminating the SSL session, thus sending the traffic as regular HTTP to the servers relieves the servers of the CPU-intensive cryptographic functions. Using a LoadMaster also allows the ability to do cookie persistence, since the LoadMaster will see the unencrypted traffic and will be able to make persistence decisions based on cookies. One of the primary components of this process is the SSL certificate. SSL certificates can be self-signed or they can be issued by a CA (Certificate Authority).

This guide covers several common SSL related scenarios, such as how to import an existing Microsoft IIS SSL certificate into the LoadMaster, and how to install an intermediate certificate.

Generating a Certificate Signing Request (CSR) from LoadMaster

When setting up a new secure web site (SSL), you have two basic choices: Run a self-signed certificate or obtain a certificate from a CA (Certificate Authority). If you're going to run a public site, it's usually best to get a certificate from a CA, otherwise your users will likely be presented with a dialog box saying the certificate cannot be verified.

Most Internet users would probably not know what that message means, so it's a good idea to get a certificate from a CA if your site is going to be trafficked by the public Internet. The first step in getting a CA certificate is to choose a CA. The LoadMaster will work with just about any CA out there, although it's a good idea to pick a well-known CA with a lot of browser support, such as Verisign or Thawt. Some CAs may not have support for them built into the popular Internet browsers such as Firefox and Internet Explorer (IE).

Once you've selected a CA, the next step is to generate what's known as a CSR, or Certificate Signing Request from LoadMaster. This can be done directly using the LoadMaster WUI.

Login to the LoadMaster WUI and select the "Generate CSR" sub-menu from the "Certificates" main menu.



Enter all of the appropriate information and click the "Create" button to generate the CSR file and the key file. LoadMaster will generate the CSR information and also the private key information. You should copy the certificate request information and the key information and store it in two separate files using an ASCII text editor of choice.

All Fields are optional except "Common Name"

2 Letter Country Code (ex. US):	<input type="text"/>
State/Province (Entire Name - New York, not NY):	<input type="text"/>
City:	<input type="text"/>
Company:	<input type="text"/>
Organization (e.g., Marketing, Finance, Sales):	<input type="text"/>
Common Name: (The fully qualified domain name for your web server)	<input type="text"/>
Email Address:	<input type="text"/>

Make sure to keep the key information very secure. You can now submit the CSR information to your CA for them to generate the certificate. Once the certificate is delivered from your CA you can install it into LoadMaster

Installing a Certificate

If you have received a certificate from a CA, you can install it directly into the LoadMaster. When requesting the certificate, you will want to make sure that they provide it to you as an Apache-modSSL certificate. This should be in the form of a text file which you can then copy and paste into the web interface of the LoadMaster.

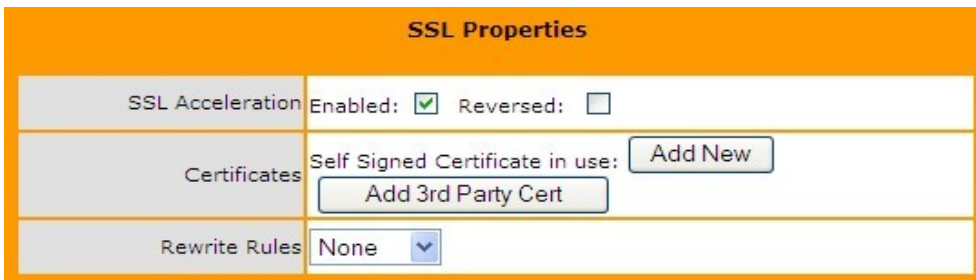
Login to LoadMaster WUI and select Modify button for the Virtual Service that requires the SSL certificate.



Within the Virtual Service enable the “SSL Acceleration” option located in the SSL Properties panel. (Accept any warning dialogs that are generated due to a temporary SSL certificate.)



Once you confirm the dialog you will see a set of options that allow you to configure additional SSL options. To install the certificate select the “Add New” button.



Copy and paste in your private key file and your new certificate file, and click submit.



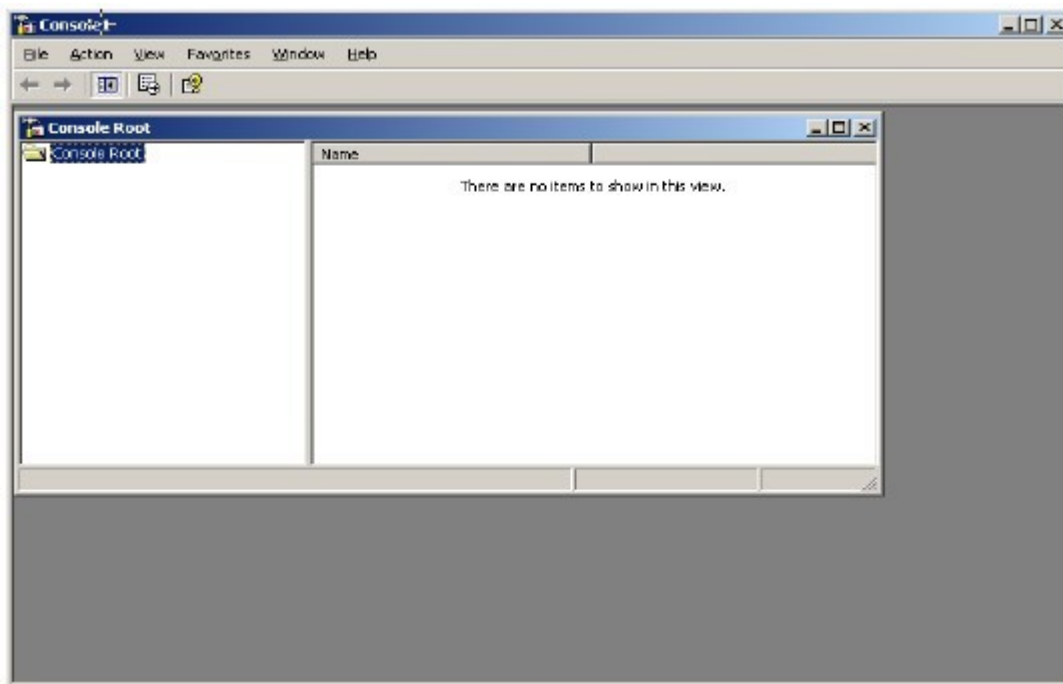
Migrating SSL from Microsoft Internet Information Server to LoadMaster

When putting a LoadMaster in a situation where a Microsoft IIS server was previously performing SSL, you'll need to import your IIS certificate into the LoadMaster. You can migrate this SSL certificate from Microsoft Internet Information Server (IIS) to the LoadMaster by completing two simple tasks.

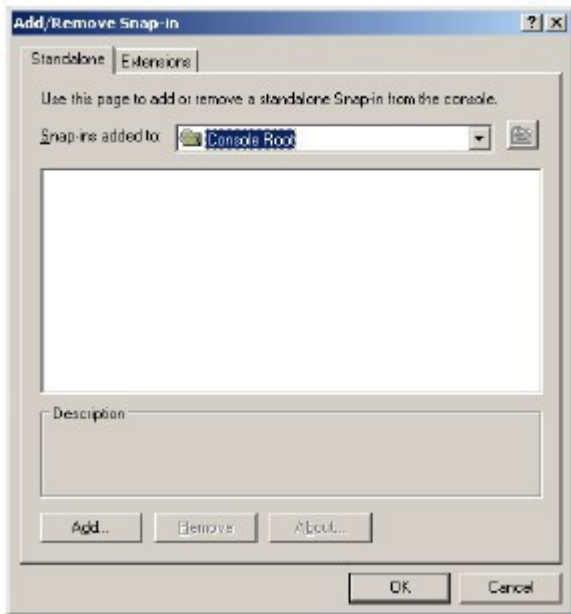
1. The first task is to export the SSL certificate from the IIS using Microsoft exports tools; you want to make sure to export the file as Personal Information Exchange File (PFX).
2. The the PFX will be converted to a LoadMaster friendly format
3. The second step is to import the converted file into LoadMaster using the LoadMaster WUI.

Exporting IIS Certificate

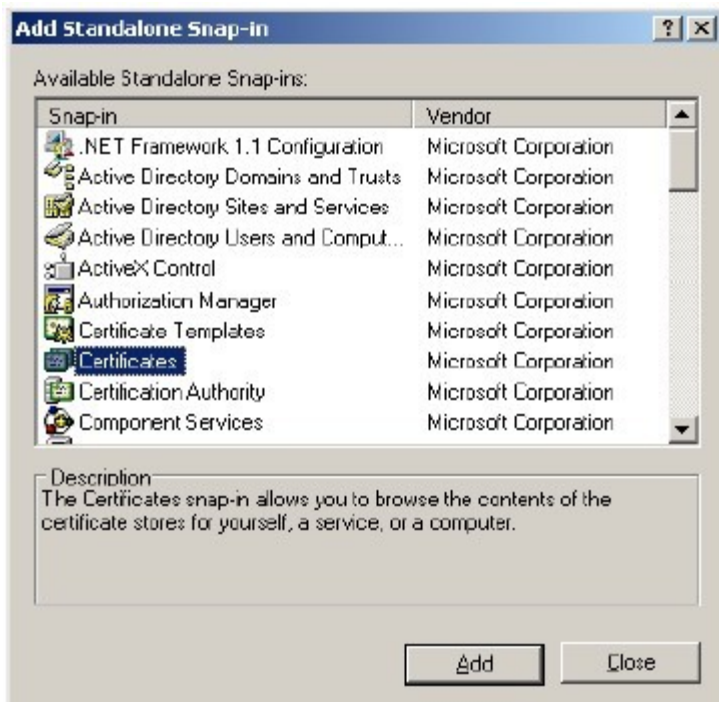
The first step is to get the certificate out of IIS, To do that, run mmc.exe from a command-line window.



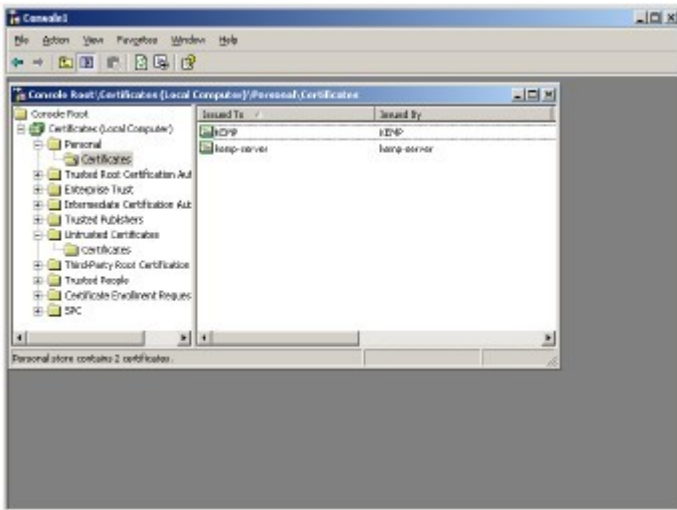
From there, go to File -> Add/Remove Snap-in.



Click the "Add..." button at the bottom.



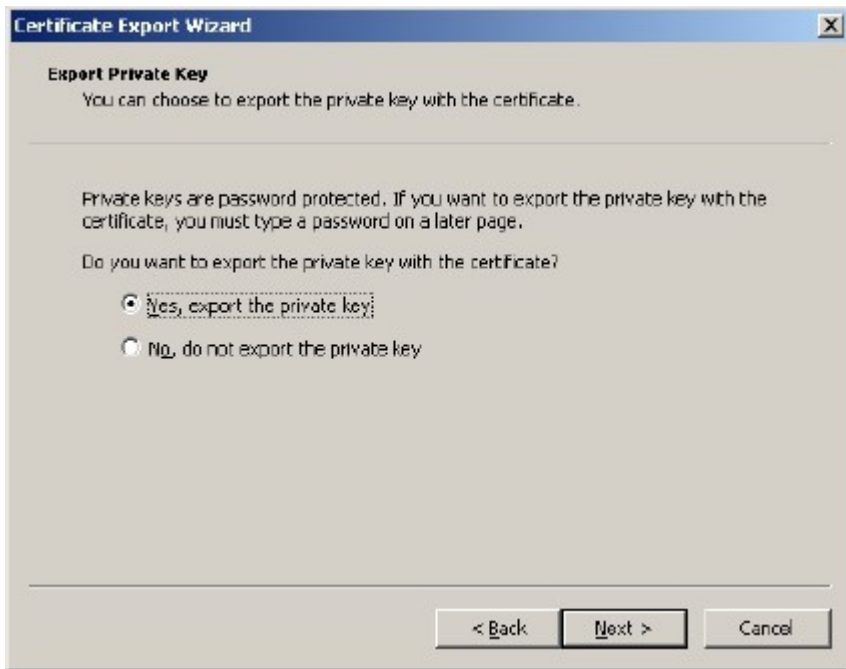
Select "Certificates" and click "Add". You'll be returned to the main Console window. Expand the "Certificates (Local Computer)" view, select "Personal", and expand that view as well.



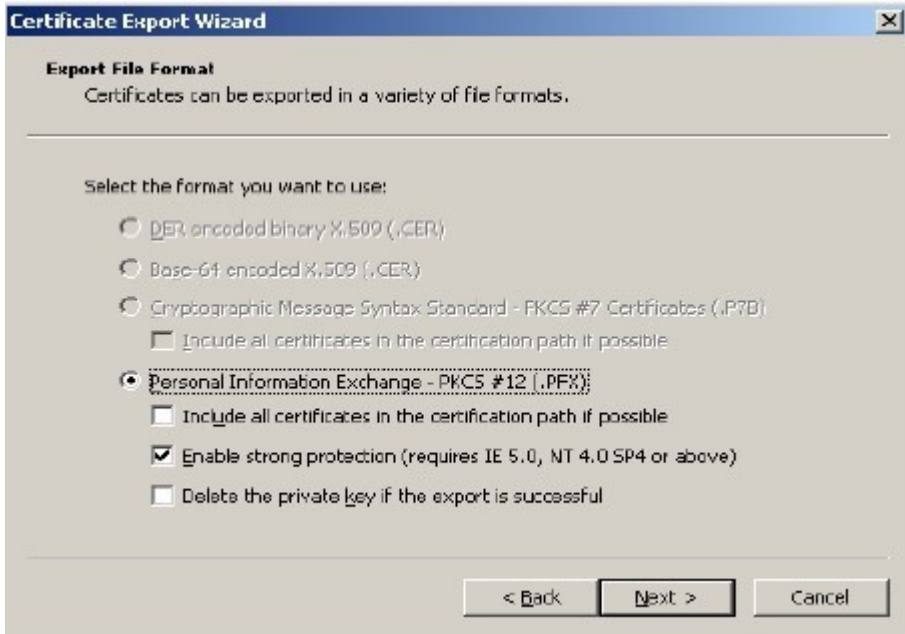
Right-mouse click on the certificate you wish to export, and select "All tasks" -> 'Export'. This will start up the Certificate Export Wizard.



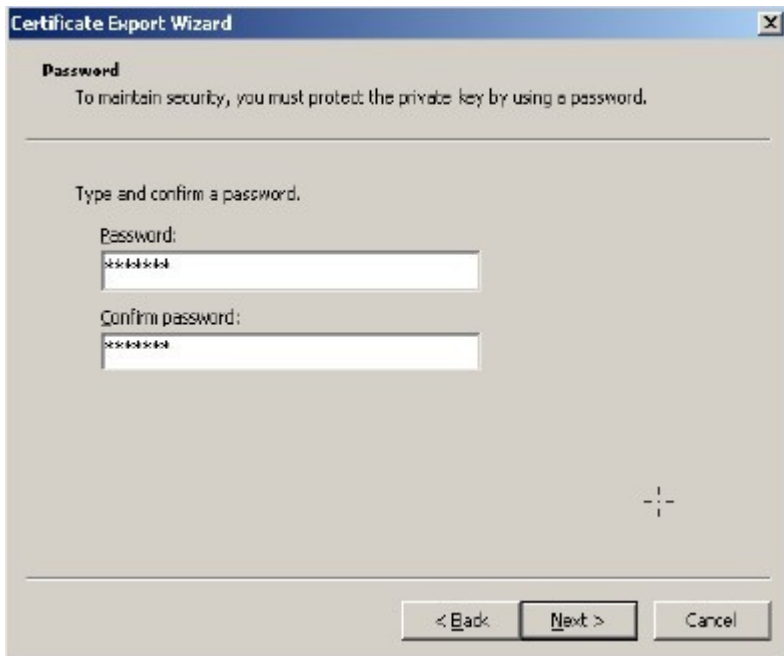
In the first screen, select “Yes” for whether to export the private key. You will definitely need this.



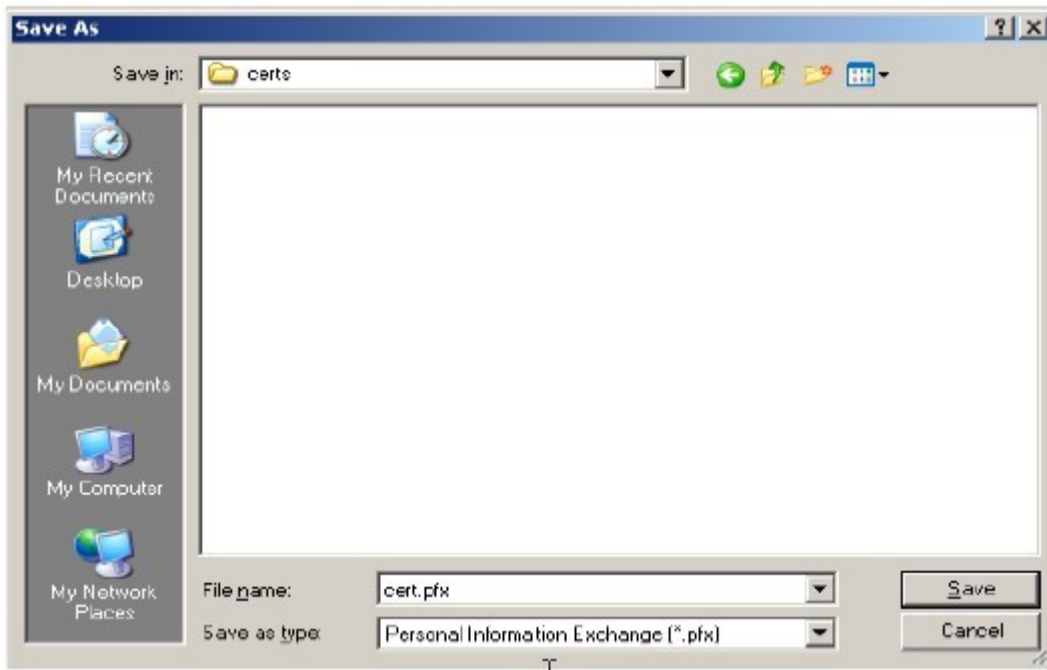
Select the PKCS #12 format, and select “Enable strong protection”.



You will be required to set a password. Select a password you can remember. You will need this password in a future step.



The wizard will now ask you where to put the PFX file. Place it someplace appropriate. Remember that this contains your private key, so don't put it in a place that could be easily accessed by unauthorized personnel. You've now completed the exporting process.



Convert PFX for LoadMaster Import

To convert the PFX file into a format the LoadMaster can understand you will need a utility built on OpenSSL. These utilities are included with virtually every Linux system. Windows binaries can be found here <http://www.slproweb.com/products/Win32OpenSSL.html> We will convert the PFX file for LoadMaster using Win32 OpenSSL v0.9.8g Light from Shining Light Productions

Download the Windows installer file and complete the installation.

Place the PFX file in the directory you install the OpenSSL, such as in the C:\OpenSSL\bin directory.

Run the following command:

```
openssl pkcs12 -in [your file].pfx -nocerts -out key.pem
```

In this example, the file name is test.pfx.

```
C:\OpenSSL\bin>openssl pkcs12 -in test.pfx -nocerts -nodes -out key.pem
```

You'll then be asked to enter the password, which should match the password used during the IIS export process. You will also be asked for a passphrase. Enter a passphrase and make sure to write it down, you will need it for a subsequent step.

You will now have a new file called "key.pem". There is one more step required for the key file. The PEM file has some extraneous information that should be stripped out. To remove the information run the following command:

```
C:\OpenSSL\bin>openssl rsa -in key.pem -out server.key
```

You will be prompted for a passphrase. Make sure it's the same one you set in the previous task.

You'll now have a new file called "server.key". This is only one of the two files that will be imported into the LoadMaster. Be careful with your key files, as they are the private keys that protect the integrity of your website.

You've now successfully separated the key from the PFX file. The next step is to separate the certificate from the PFX file and convert it into a PEM format so that it can be used with the LoadMaster.

Run the following command:

```
openssl pkcs12 -in [your file].pfx -clcerts -nokeys -out cert.pem
```

Example:

```
C:\OpenSSL\bin>openssl pkcs12 -in test.pfx -clcerts -nokeys -out cert.pem
```

You'll then be asked to enter the password, which should match the password used during the IIS export process.

You will then have a file called "cert.pem", this will be your certificate file that you load into the LoadMaster.

The files have been successfully exported and converted. You can now import the key and certificate information into LoadMaster using the WUI

Import SSL Certificate into LoadMaster

Importing a PFX file into LoadMaster can be accomplished in only a few steps.

Login to LoadMaster WUI and select Modify button for the Virtual Service that requires the SSL certificate.



Within the Virtual Service enable the “SSL Acceleration” option located in the SSL Properties panel. (Accept any warning dialogs that are generated due to a temporary SSL certificate.)



Once you confirm the dialog you will see a set of options that allow you to configure additional SSL options. To install the IIS based key and certificate select the “Add New” button.



Now to install the key and certificate file simply open each of the files you created using a ASCII text file editor of choice and then copy the corresponding contents into the appropriate text box and enter the passphrase you used during the conversion process. (Make sure to copy everything in the control tags == only, this includes the control tags.)

**Copy and Paste the entire bodies of both the Signed Certificate and Key files
for 10.0.1.36:443 below:**

Signed
Public
Certificate:

Private
Key:

Private
Key Pass
Phrase:

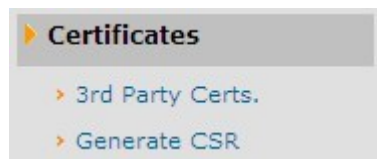
Intermediate Certificates (3rd Party)

Some certificate authorities require what's known as an intermediate certificate, in addition to the primary SSL certificate. Verisign is one such CA that uses intermediate certificates.

The first step with intermediate certificates is of course to have the site certificate (non-intermediate) certificate already installed onto your virtual service.

The next item you'll need is the actual intermediate certificate. You can obtain these through the CA that you obtained your certificate from. For instance, Verisign's intermediate certificate can be found here <http://www.verisign.com/support/verisign-intermediate-ca/index.html>

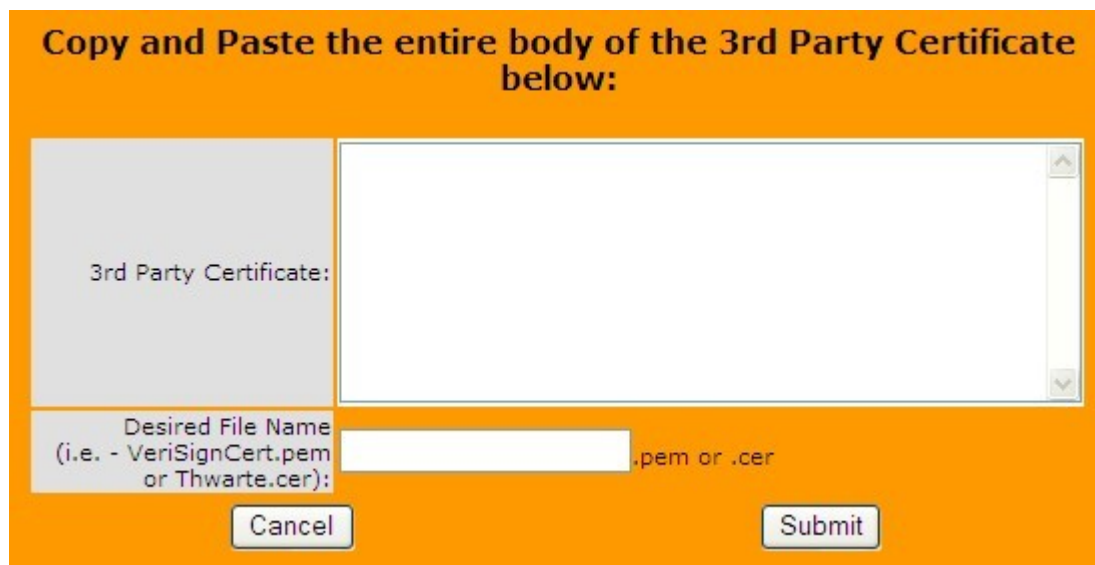
Once you have downloaded your 3rd party certificate you can then login to the LoadMaster WUI and select the “3rd Party Certs.” sub-menu from the “Certificates” main menu.



To add the 3rd party certificate you can click the “Add New” button. You should also open the certificate file that you downloaded using an ASCII text editor of choice. You will need to copy the contents of the file into the LoadMaster WUI.



Copy and paste to contents of the file into the “3rd Party Certificate:” textbox and also name the certificate.



Once the intermediate certificate is installed, you'll want to de-activate and re-activate the associated Virtual Service (which will cause a short amount of downtime). LoadMaster will then associate the intermediate certificate with the appropriate virtual service (or services, if you have multiple intermediate-reliant certificates that use the same intermediate).

Once this is completed, you are finished. The certificate chain is built automatically by LoadMaster, and you can browse the site to check that the certificate is valid.