

# LoadMaster SSL Certificate Quickstart Guide

*for the LM-1500, LM-2460, LM-2860, LM-3620, SM-1020*

This guide serves as a complement to the LoadMaster documentation, and is not a replacement for the full LoadMaster/SSL-Master documentation. For concepts and issues not covered in this document, consult the *LoadMaster Installation and Configuration Guide* located on the CD included with each LoadMaster/SSL-Master.

## Table of Contents

Introduction.....	2
SSL Acceleration Network Architecture.....	2
Converting from IIS.....	2
Exporting IIS Certificate.....	3
Converting the Key and Certificate.....	7
Loading Certificate and Key Files.....	8
Adding Via the WUI.....	8
Configuring Virtual Service.....	9
Uploading via SSH/Text.....	10
Intermediate Certificates.....	12
Generating a Certificate Request (CSR).....	14



# Introduction

---

The world of SSL certificates can be a bit confusing, so this document was assembled to help guide users of LoadMasters and SSL-Masters through the various processes involving certificates that you may encounter.

At KEMP, we are always striving to enhance our documentation, so if you have any suggestions for additional topics to be covered, questions, or comments, send them to [support@kemptechnologies.com](mailto:support@kemptechnologies.com).

## 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 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 or a SSL-Master 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 (the process described in the QuickStart Guide), or they can be issued by a CA (Certificate Authority).

This document covers several common scenarios, such as how to convert an existing Microsoft IIS SSL certificate for use with the LoadMaster/SSL-Master, and how to install an intermediate certificate.

## Converting from IIS

---

When putting a LoadMaster or SSL-Master in a situation where a Microsoft IIS server was previously performing SSL, you'll need to convert your IIS certificate into a format that the LoadMaster/SSL-Master can recognize.

Here is a list of the steps that will need to be taken.

- Export the SSL certificate and key to a file
- Converting the SSL certificate into a PEM key file and certificate file



- Loading the key and certificate files onto the LoadMaster/SSL-Master

## Exporting IIS Certificate

The first step is to get the certificate out of IIS, and then you'll need to convert the certificate into the PEM format. To do that, run `mmc.exe` from a command-line window (figure 1).

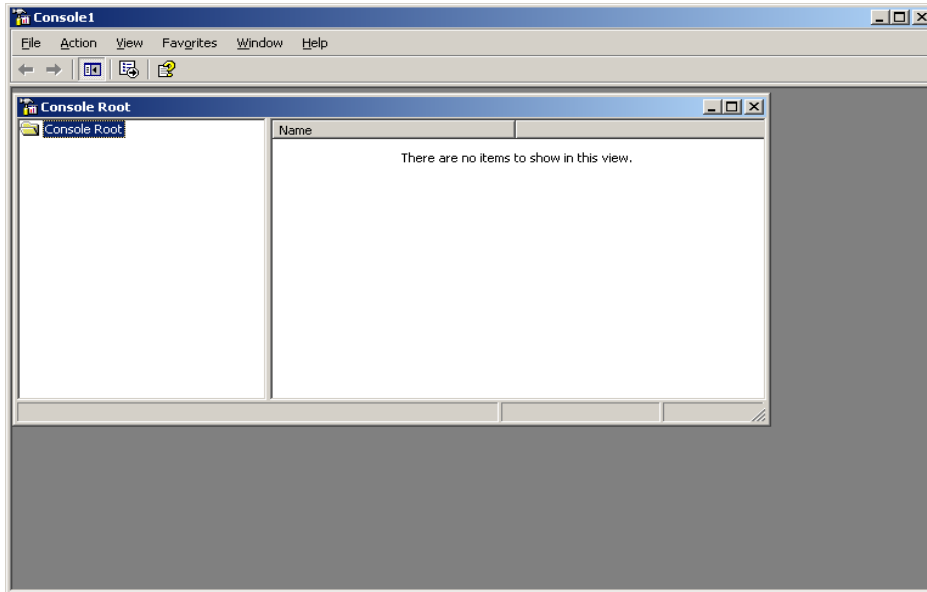


Figure 1: mmc.exe Console

From there, go to File -> Add/Remove Snap-in (figure 2).

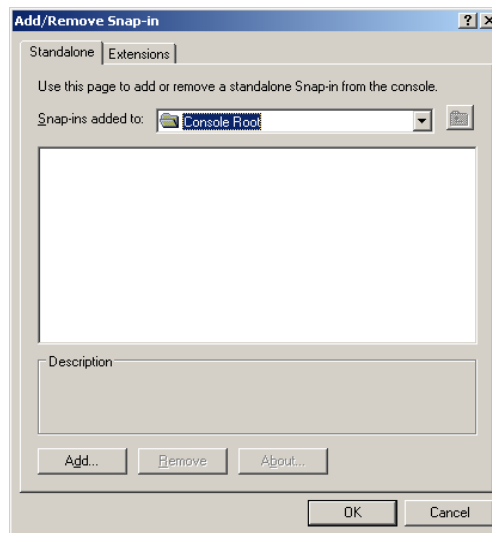


Figure 2: Add/Remove Snap-in



Click the “Add...” button at the bottom.

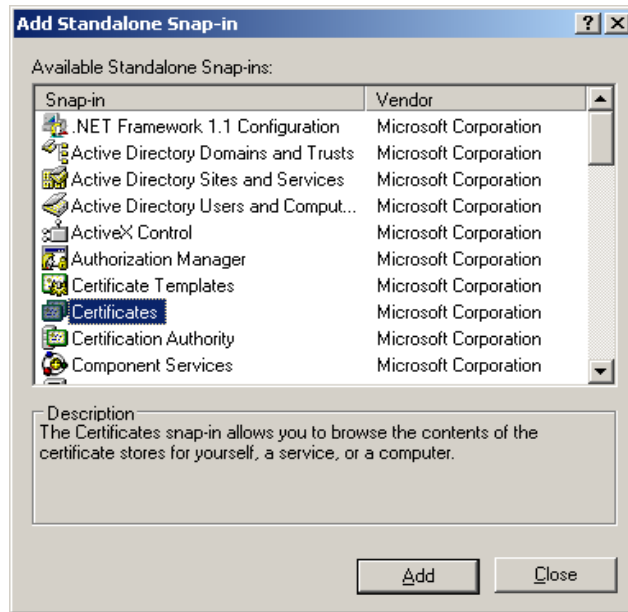


Figure 3: Standalone Snap-in

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 (figure 4).

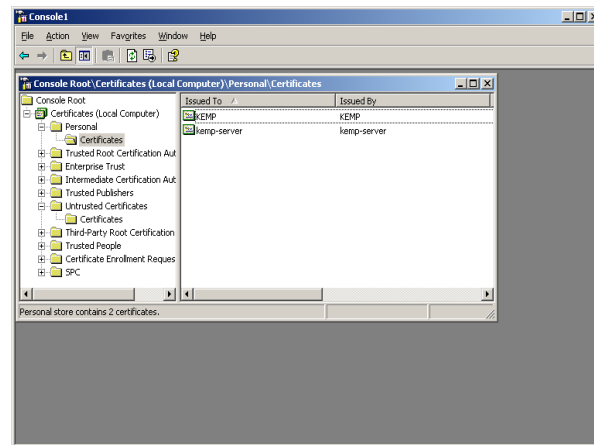


Figure 4: Certificates (Local Computer)

Right-mouse click on the certificate you wish to export, and select “All tasks” -> 'Export'. This will start up the Certificate Export Wizard (figure 5).





Figure 5: Certificate Export Wizard

In the first screen, select “Yes” for whether to export the private key (figure 6). You will definitely need this.

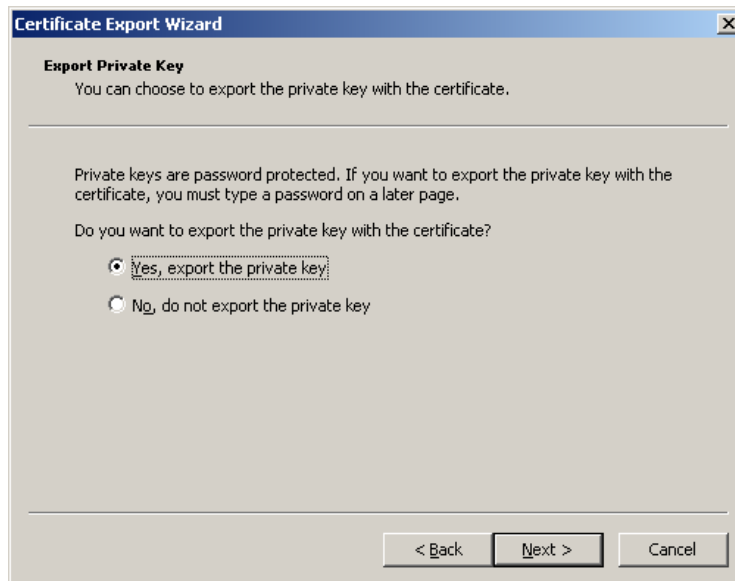


Figure 6: Export Key

Select the PKCS #12 format, and select “Enable strong protection” (figure 7).



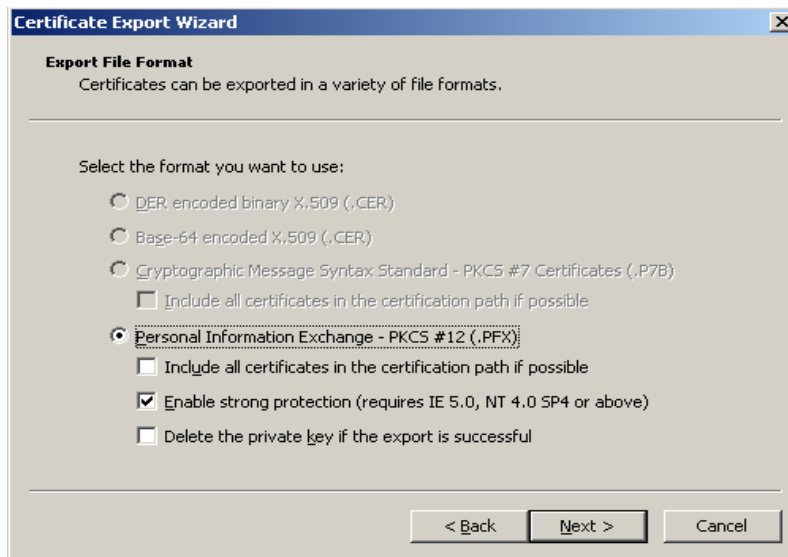


Figure 7: Selecting PFX

You will be required to set a password. Select a password you can remember. You will need this password in a future step (figure 8).

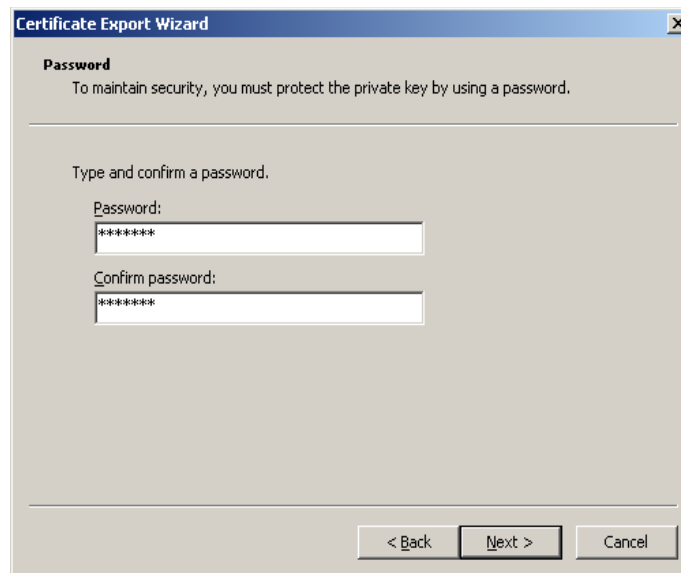


Figure 8: Password

The wizard will now ask you where to put the PFX file (figure 9). 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.



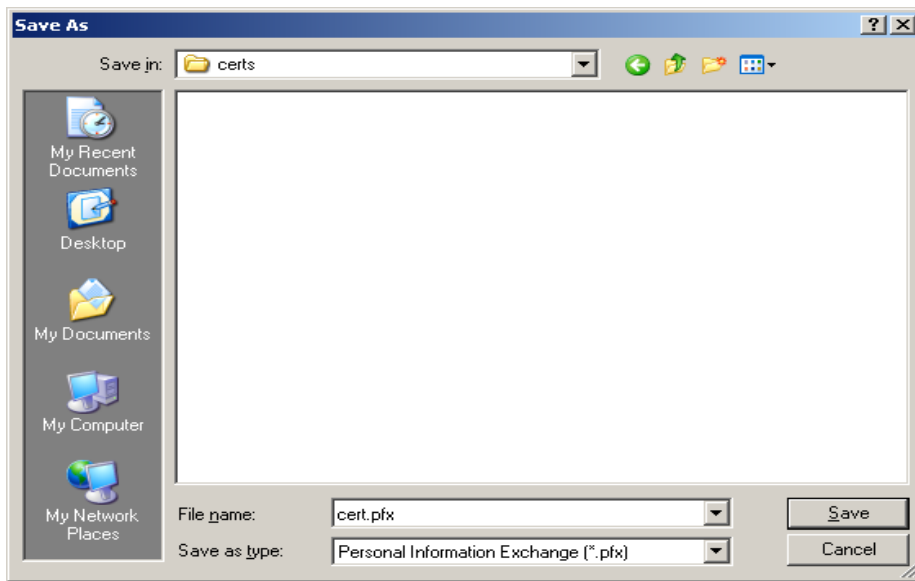


Figure 9: Place the PFX file on filesystem

You've now completed the exporting process (figure 10).



Figure 10: Successful Export

## Converting the Key and Certificate

The next step is to convert the PFX file into a format the LoadMaster/SSL-Master can understand. You'll need a utility called OpenSSL to do this. This utility is included with virtually every Linux system, and Windows binaries can be found here:

<http://www.slproweb.com/download/Win32OpenSSL-v0.9.7i.exe>

Place the pfx file somewhere, 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 you entered when you exported the key file.

```
Enter Import Password:
```

```
MAC verified OK
```



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. To do this, run the following command:

```
openssl rsa -in key.pem -out server.key
```

You'll then have a new file called “server.key”. This is one of the two files that will go on 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/SSL-Master.

Run the following command:

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

You'll be asked again for the password from IIS.

```
Enter Import Password:
```

```
MAC verified OK
```

You will then have a file called “cert.pem”, this will be your certificate file that you load into the LoadMaster/SSL-Master.

The files have been successfully exported and converted. You can move to the next section which covers uploading the certificate and key files onto the LoadMaster/SSL-Master.

## Loading Certificate and Key Files

---

There are two ways to upload certificate and key files into a LoadMaster/SSL-Master. The first way is through the WUI (Web User Interface), and the second way is through the SSH textual interface.

### ***Adding Via the WUI***

When adding via the WUI, you'll need to have either an FTP server or HTTP server available with the key and certificate files that you need (In the SSH textual interface, you have the additional option of scp, which is copy over encrypted SSH).

To select the protocol used, log into the WUI and select the “System Properties” tab at the top. Then select “Miscellaneous”. The second section down should read “Transfer Protocol to Balancer”. Use the drop-down menu to select the desired protocol (figure 11).



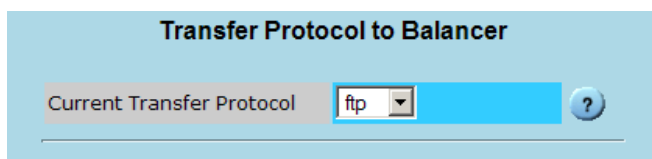


Figure 11: Transfer Protocol Dialog

***Be aware that when using FTP or HTTP as the transfer protocol, your private key is traversing the network in plain-text. Do not do this with a public network between the LoadMaster/SSL-Master and the HTTP/FTP server. If you wish to use an encrypted protocol, go to the textual menu section.***

## Configuring Virtual Service

If you're adding a new virtual service, select the “Enable” button in the SSL Acceleration section. If you've already setup the virtual service and are using the self-signed certificate, simply de-select SSL acceleration and re-select it again. Either way, you'll then be presented with a pop-up window (figure 12).

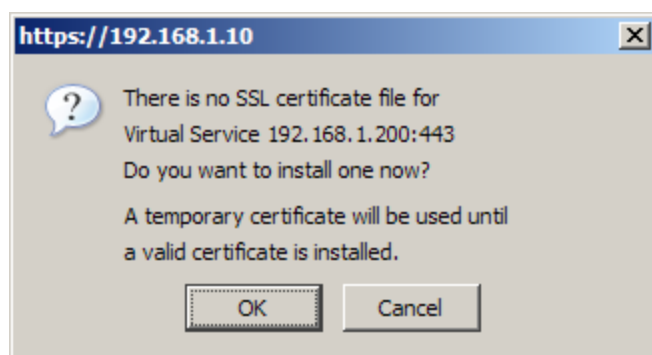


Figure 12: Certificate Upload Dialog

Select “OK”. You'll then be presented with a screen to upload the certificate and key files (figure 13).

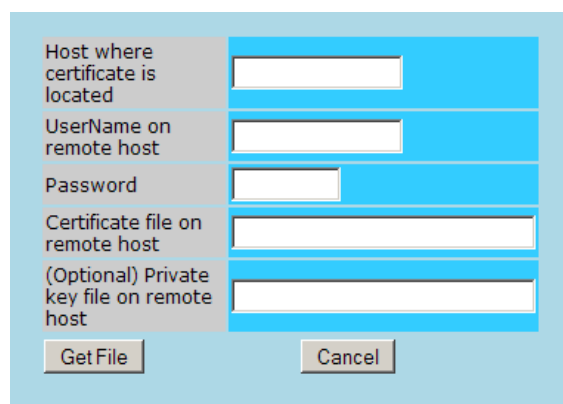
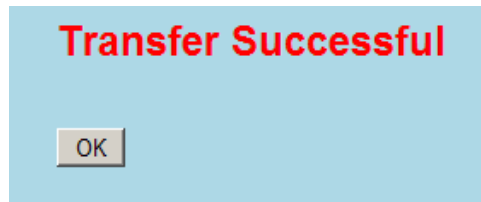


Figure 13: Upload Menu



Under host, enter the hostname (or IP address) of the system that contains the certificate and key files. For username, enter the username. If HTTP is your transfer protocol, enter “anonymous” for username, and leave the password blank.

If the transfer is successful, you'll get the following screen (figure 14). You've successfully installed a certificate.



*Figure 14: Transfer Successful*

If you need to change the certificate for any reason, simply de-select and then select again the “Enabled” option the SSL Acceleration section of the modify Virtual Service screen in the WUI. You'll be presented again with the opportunity to upload a certificate and key file.

### ***Uploading via SSH/Text***

Another way to upload a certificate is to use the textual menu system. This can be accessed either by SSH or through the VGA console ports. (For more information on accessing the LoadMaster/SSL-Master this way, consult the QuickStart Guide or LoadMaster/SSL-Master documentation.)

The first step is to select the method of uploading the certificate and key files. You can use one of three transfer methods: HTTP, FTP, or scp (secure copy over SSH). It is recommended you use scp. The scp protocol utilizes the secure nature of SSH, which encrypts all data being transferred.

You can select this protocol through the WUI (in “System Properties” and then “Miscellaneous”), or through the textual menu system.

In the console, select “Utilities” (option 7) from the main menu, and then option “2” (figure 15).



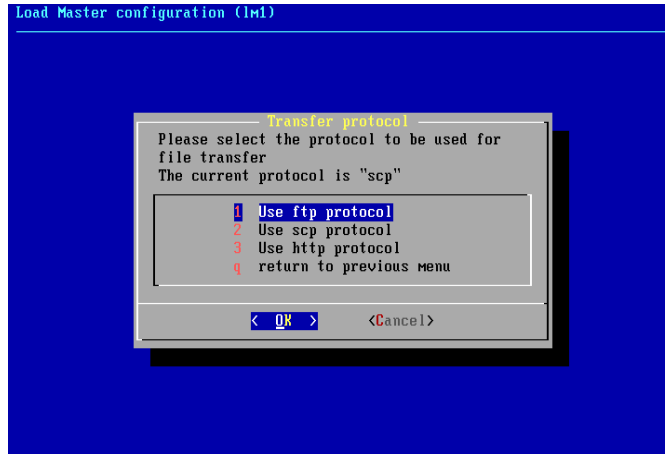


Figure 15: Transfer Protocol Menu

To add a certificate, select “SSL Certificate Administration” (option 4 in Utilities). Select “1”, for “VIP Specific Certificates. You must have already added the virtual service in question and enabled SSL acceleration (you can opt to use the temporary certificate until this step). If you haven't done so yet, do so now in the WUI.

There is one certificate per virtual service. Select the virtual service that you wish to add a certificate to (figure 16).

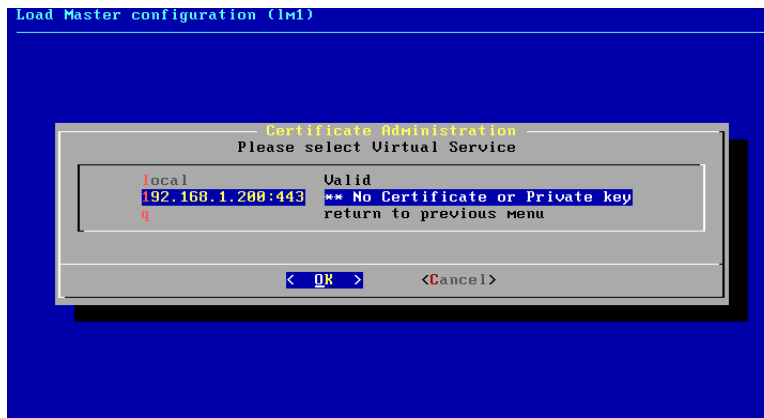


Figure 16: Certificate Administration

From there, you will see a menu where you can add certificate and key files, as well as delete existing certificate key pairs (figure 17).



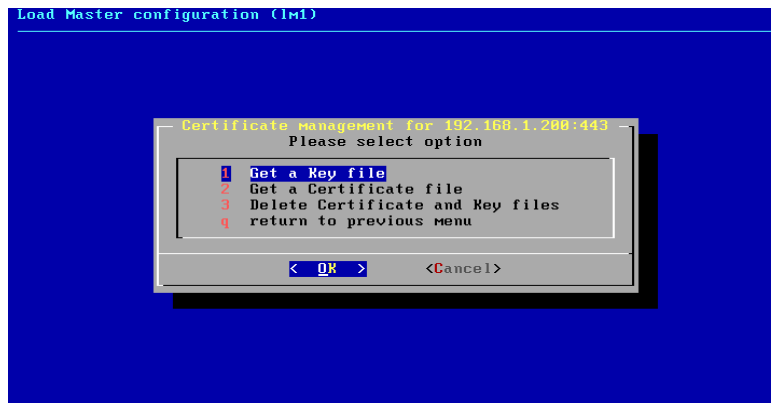


Figure 17: Get Key and Certificate Files

Select “Get a Key file”. You'll be asked for the hostname of the system where the key file is located. Enter the hostname or IP address of the appropriate machine (figure 18).

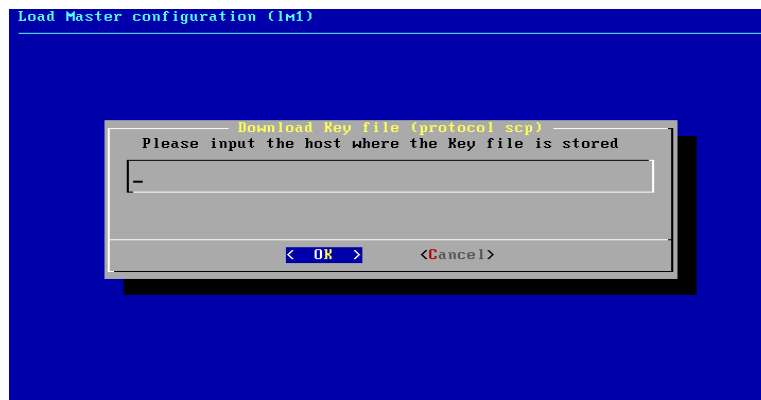


Figure 18: Host system

You'll then be asked for the username. Enter in the appropriate username. If the transfer protocol is FTP and the account is anonymous, enter “anonymous”. If the transfer protocol is HTTP, enter “none” for username.

If the transfer is successful, you'll see a message saying “New Key file installed”. Repeat this process with the certificate file.

Enter “Q” to exit this menu, and you'll see that the virtual service has a valid certificate and key file installed.

## Intermediate Certificates

---

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.

To install an intermediate certificate, you'll need to log into the textual menuing system either through SSH, or through the console (USB/VGA or serial). Currently, you cannot



install an intermediate certificate through the WUI.

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/secure-site-pro-intermediate/index.html>

**Save it to a file with .PEM as the extension.** For instance, call the Verisign certificate `verisign-interm.pem`.

Next, log into the textual menu system, either remotely through SSH, or locally on the console (USB/VGA or serial). From the main menu, select option number 7, for “Utilities”. Then select option number 4, “SSL Certificate Administration”.

Select option 2, “3<sup>rd</sup> Party Certificates”, and then select option 1, “Import 3<sup>rd</sup> Party Certificate (figure 19).

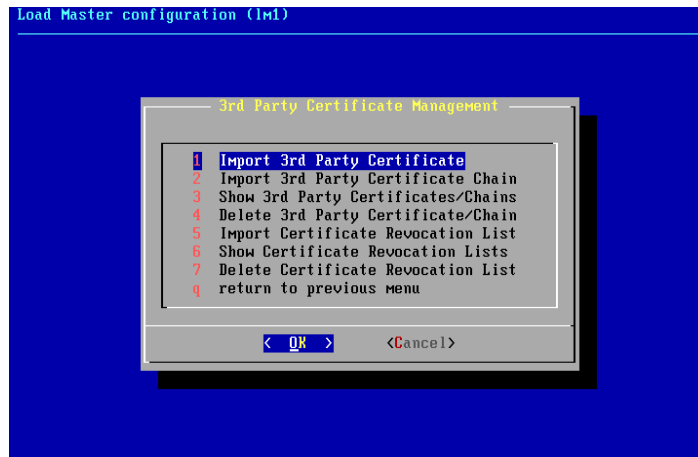


Figure 19: 3<sup>rd</sup> Party Certificate Menu

You'll then be asked for the host name where the file is available. These are the same questions you were asked in the WUI to install the primary certificate (also the same questions from the textual menu system if you installed the primary certificate that way).

Once the intermediate certificate is installed, you'll want to de-activate and re-activate the virtual service (which will cause a short amount of downtime). Go back to the WUI and un-check the check box in the “Activate or Deactivate” section of the modify screen for the virtual service in question. Then, check the box again, re-activating the virtual service (figure 20). This LoadMaster/SSL-Master 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).



Activate or Deactivate Service

Figure 20: Activate or Deactivate Service

Once this is completed, you are finished. The certificate chain is built automatically by the load balancer, and you can browse the site to check that the certificate is valid. To check, load the site in your favorite browser. In Microsoft Internet Explorer, there will be a padlock icon on the bottom right of the window for SSL sites. Double click this padlock, and you will see if the certificate chain is valid or not.

## Generating a Certificate Request (CSR)

---

When setting up an SSL site, 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, such as the error that Internet Explorer gives in figure 21.



Figure 21: Self-signed Certificate Warning

Most Internet users would probably not know what that message meant, 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 IE.



Once you've selected a CA, the next step is to generate what's known as a CSR, or Certificate Signing Request. This can be done with OpenSSL, which is a free utility that comes with most Linux/UNIX distributions, and can be downloaded for Windows. The Windows download can be found here (KEMP recommends the 0.9.8 version):

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

With OpenSSL, you can use the following command line command to generate the CSR:

```
C:\> openssl req -newkey rsa:1024 -nodes -keyout domainname.key -out domainname.csr
```

You will be prompted for the country abbreviation (such as US), address, and other information.

```
Loading 'screen' into random state - done
Generating a 1024 bit RSA private key
.....++++++
.++++++
writing new private key to 'domainname.key'
-----
You are about to be asked to enter information that will be
incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a
DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:US
State or Province Name (full name) [Some-State]:New York
Locality Name (eg, city) []:Bethpage
...
```

When you're asked for a challenge password, leave the entry blank.

```
A challenge password []:
An optional company name []:
```

This process will generate two files: `domainname.key`, and `domainname.csr`. The `.key` file is important to keep safe and secure, as it is your private key. If you ever need to re-install the certificate, you'll need the file. If it gets into the wrong hands, someone could potentially pretend to be your site.

Often, the CA will ask you to either email the `domainname.csr` file to them, or to cut and paste the contents into a web window.

When you submit the CSR to the CA, they might ask which format, either Apache or IIS. The LoadMaster/SSL-Master uses the Apache format, so select that one.



When you receive the certificate file, you will install that file along with the key file into the LoadMaster/SSL-Master. See the previous section on loading certificates for more information.

