SSL Guide

From MyKemp Wiki

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.

Contents

- 1 SSL Acceleration Network Architecture
- 2 Generating a Certificate Signing Request (CSR) from LoadMaster
- 3 Installing a Certificate
- 4 Migrating SSL from Microsoft Internet Information Server to LoadMaster
 - 4.1 Exporting IIS Certificate
 - 4.2 Loading IIS Certificate into LoadMaster
- 5 Intermediate Certificates (3rd Party)

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):			
State/Province (Entire Name - New York, not NY):			
City:			
Company:			
Organization (e.g., Marketing, Finance, Sales):			
Common Name: (The fully qualified domain name for your web server)			
Email Address:			
Create Reset	Cancel		

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.)

	SSL Properties
SSL Acceleration	Enabled: 🗌

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.

SSL Properties			
SSL Acceleration	Enabled: 🗹 Reversed: 🗌		
Certificates	Self Signed Certificate in use: Add New Add 3rd Party Cert		
Rewrite Rules	None 💌		

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 second step is to import the PFX 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.

Consolet-	
He Action View Favorites Wind ← → 100 15 12	w Heb
Console Root	
	Name There are no items to show in this view.

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

Add/Remove Snap-in	<u>? x</u>
Standalone Extensions	
Use this page to add or remove a standalone Snap	p in from the console.
Snap-ins added to: Encode Root	• 🖻
Description	
Add Bemove About	
	-
	OK Cancel

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

nap-in	Vendor	-
NET Framework 1.1 Configuration	Microsoft Corporation	
Active Directory Domains and Trusts	Microsoft Corporation	
Active Directory Sites and Services	Microsoft Corporation	
Active Directory Users and Comput	Microsoft Corporation	
≟ ActiveX Control	Microsoft Corporation	
Authorization Manager	Microsoft Corporation	
🖬 Certificate Templates	Microsoft Corporation	
Certificates	Microsoft Corporation	
Certification Authority	Microsoft Corporation	
Component Services	Microsoft Corporation	
Description he Certificates snap-in allows you to brow artificate stores for yourself, a service, or	use the contents of the a computer.	

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.

	the comparison provide an other	-TA BET		
Conside Flash Conside Flash Construction (Construction)	Instand Ta /	Tenued By		
Certificates Traded Read Certification Discover Traded Read Certification Discover Traded Read Certification Discover Traded Certification Traded Reads Traded Reads Traded Reads Traded Reads Traded Reads Certificate Sectioner Reads Soc	Ligi kong-rarver Add Add	kang-server		
			2	
csonal store contains 2 certificates			11	

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

Čertificate Export Wizard		×
	Welcome to the Certificate Export Wizard This wizard helps you copy certificates, certificate trust lists and certificate revocation lists from a certificate store to your disk. A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept. To continue, click Naxt.	

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

rtificate Export Wizard	X
Export Private Key You can choose to export the private key with the certificate.	
Private keys are password protected. If you want to export the private key with the certificate, you must type a password on a later page.	he
Do you want to export the private key with the certificate?	
Mes, export the private key	
🔿 Ng, do not export the private key	
< Back Next > C	ancel

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.

tificate Export Wizard			
Password			
To maintain security, you must prote	at the private key bγ	using a password	
Type and confirm a password.			
Bassword:			
akan dalam kan			
, Confirm password:			

	< <u>B</u> adk	<u>N</u> ext >	Cancel

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.

Save As					?]
Savə jn:	Certs		•	000	
My Recent Documents					
My Computer					
	File name:	Cert t/x			Save
Places	5 ave as <u>t</u> ype:	Personal Informat	ion Exchange (*.pl	(x) <u>*</u>	Carcel

Loading IIS Certificate into LoadMaster

Importing a PFX file into LoadMaster can be accomplished with 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.)

	SSL Properties
SSL Acceleration E	inabled: 🗌

Once you confirm the dialog you will see a set of options that allow you to configure additional SSL options. To install the IIS PFX file select the "Add New" button.

SSL Properties		
SSL Acceleration	Enabled: 🗹 Reversed: 🗌	
Certificates	Self Signed Certificate in use: Add New Add 3rd Party Cert	
Rewrite Rules	None 💌	

To install your PFX file simply select the "Browse.." button located next to "An IIS Certificate:" option. Select the PFX file that you wish to install for this Virtual Service.



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.

Certificates		
> 3rd Party Certs.		
Generate CSR		

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.

3rd Party Certificates currently installed on your Load Master		
Add New		
	File Name	Options
<u>1</u>	No 3rd Party Certificates Currently Installed	

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

Copy and Paste the entire body of the 3rd Party Certificate below:		
3rd Party Certificate:		
Desired File Name (i.e VeriSignCert.pem or Thwarte.cer):	.pem or .cer	
Cancel	Submit	

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.

Retrieved from "http://10.0.0.170/wiki/index.php/SSL_Guide"

Categories: SSL | LoadMaster 4.2

• This page was last modified 22:13, 20 February 2008.