

## Configuration guide for a Kemp Technologies LoadMaster V7.2.50 for Load Balancing USS Gateway Proxies

### Contents

<b>Step 1. Preparing everything.</b> .....	2
<b>Step 2. Configuring the Primary Proxy.</b> .....	3
<b>Step 3. Configuring the Secondary Proxy</b> .....	7
<b>Step 4. Configuring your Kemp Technologies LoadMaster</b> .....	11



Please note, this document is intended as a rough guide for preparing a Kemp Technologies LoadMaster for Load Balancing Censornet USS Gateway proxies. Please contact your Kemp Technologies provider for assistance with the best practices or troubleshooting this setup.

Instructions on installing the Censornet Cloud USS proxies are outside of the scope of this document. The instructions can be found here:

<https://help.clouduss.com/gateway/uss-gateway-installation>



## Step 1. Preparing everything.

In order for load balancing of the USS proxies to work, you have to ensure that both are using the same SSL configuration and duplicate the authentication configuration between them. This guide will assume you are load balancing only two proxies. However, you can add more if you wish.

You will need:

- Two USS proxy servers.
- Three static IP addresses.
- An SSL certificate generated on one of the proxies.
- Kerberos keys generated on one of the proxies.

For our example, we will be using the following IP addresses:

- Primary: 10.10.10.5
- Secondary: 10.10.10.6
- Load Balancer: 10.10.10.10

We will also be using the following hostnames:

- gateway1.domain.local
- gateway2.domain.local
- filter.domain.local

Ultimately we will end up with a configuration of:

- gateway1.domain.local on 10.10.10.5
- gateway2.domain.local on 10.10.10.6
- filter.domain.local on 10.10.10.10

However please note that during the configuration we will have to configure the proxies with the details for filter.domain.local and then change it afterwards. This is due to Kerberos using the hostname as part of it's hashing algorithm.



## Step 2. Configuring the Primary Proxy.

This first proxy will be our primary proxy and used to generate the Kerberos keys and the SSL certificate.

Build the proxy as per the installation instructions linked above, but with the hostname and IP address that will become our load balancer hostname and IP address. So give it the hostname filter.domain.local and the IP address 10.10.10.10.

First, configure the IP address:

### Configuration

Interface: ens160

Friendly name:

IP address (IPv4):

Netmask:

Then configure the hostname (please note, this is the SHORT hostname you need to use here):

### Network Settings

Default Gateway:

Primary DNS:

Secondary DNS:

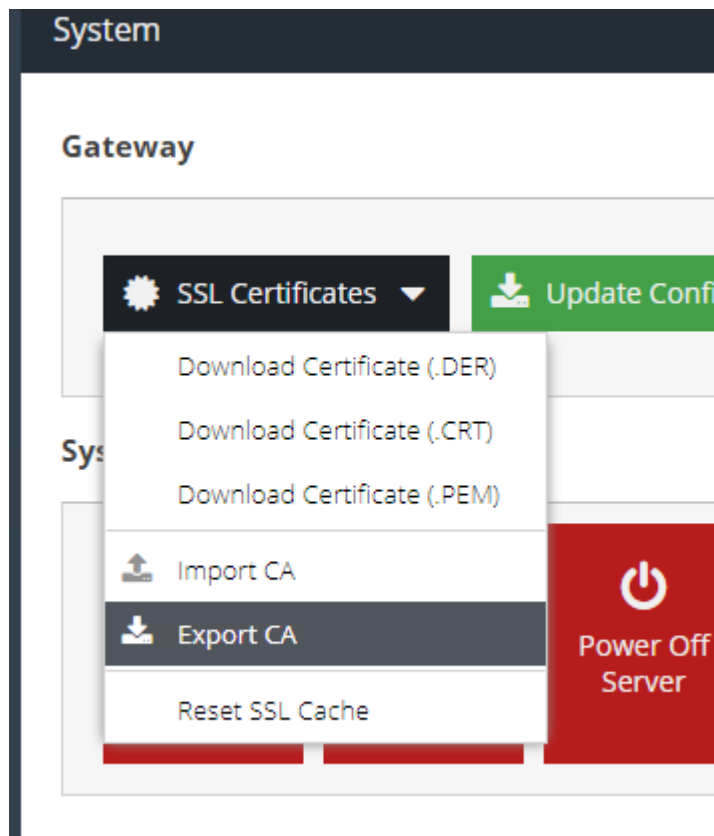
Hostname:

Agent name (leave blank to default to hostname):



Reboot the proxy to ensure that these settings take effect. This is very important, as we will be generating the Kerberos keys using this hostname.

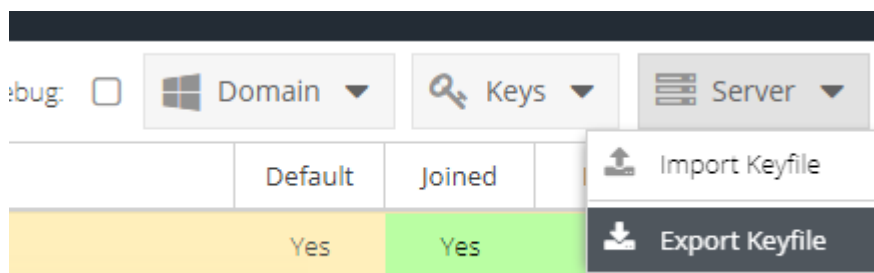
Next, export the SSL CA Certificate:



Save this somewhere safe as you may need to use this again if any of the proxies fail for any reason in the future.

Now configure the authentication as per the instructions here:  
<https://help.clouduss.com/configure/authentication-identification>

Once this is complete, export the Kerberos keys:





Again, please save this somewhere safe as you may need to reuse this at a later date.



Now, you need to configure this proxy with its final hostname and IP address – in the case of our example gateway1.domain.local and 10.10.10.5:

### Configuration

 Save  Manage ▼


**Interface:** ens160

Friendly name:

IP address (IPv4):

Netmask:

### Network Settings

 Save

Default Gateway:

Primary DNS:

Secondary DNS:

Hostname:


Agent name (leave blank to default to hostname):



Reboot the proxy again for this configuration to take effect.

Finally, configure the load balancer VIP setting. This is very important, and if you miss this step, it will not work:

## Advanced

 Save

- Early Access:** Enable proxy version (includes web socket support)
- Reduce noise from background Web requests to increase performance and report visibility
- Reuse the same key when using temporary/ephemeral Diffie-Hellman key exchanges

Loadbalancer VIP:



## Step 3. Configuring the Secondary Proxy.

Initially, the configuration here is identical to the primary proxy. You need to build it and configure it with the hostname and IP address that will ultimately become the load balancers.

So give it the hostname `filter.domain.local` and the IP address `10.10.10.10`.

First, configure the IP address:

### Configuration

Interface: `ens160`

Friendly name:

IP address (IPv4):

Netmask:

Then configure the hostname (please note, this is the SHORT hostname you need to use here):

### Network Settings

Default Gateway:

Primary DNS:

Secondary DNS:

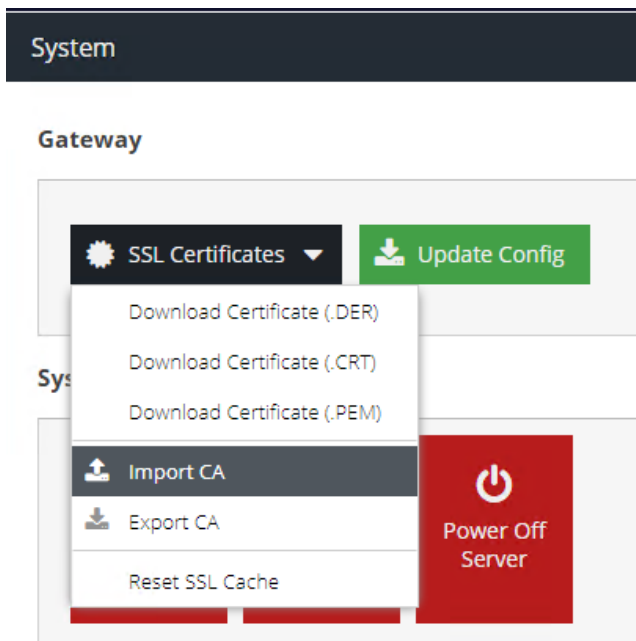
Hostname:

Agent name (leave blank to default to hostname):





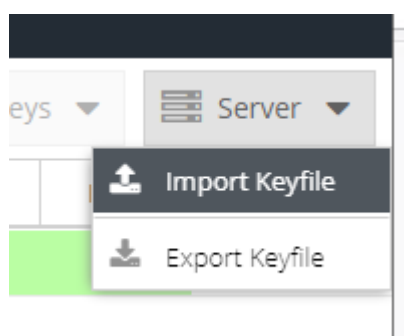
Next, you need to import the SSL CA certificate you exported earlier:



When this is done, you will again need to follow the instructions on joining the proxy to your active directory domain: <https://help.clouduss.com/configure/authentication-identification>

**NB: It is very important that you DO NOT create the keys here, just create the domain configuration and join the proxy to it.**


Once this is done, please import the keys you exported from the first proxy:






Next, you need to reconfigure the proxy to its final hostname and IP address. In this example, gateway1.domain.local and 10.10.10.6

## Configuration

 Save

 Manage ▼

Interface: ens160

Friendly name:

Main


IP address (IPv4):

10.10.10.6

Netmask:

255.255.0.0

## Network Settings

 Save

Default Gateway:

10.10.10.254

Primary DNS:

10.10.10.253

Secondary DNS:

Hostname:

gateway2


Agent name (leave blank to default to hostname):



Reboot the proxy for this to take effect.

Once it's back upon its new IP address, connect to it and configure the load balancer VIP setting with the IP address for the load balancer:

## Advanced

 Save

- Early Access:** Enable proxy version (includes web socket support)
- Reduce noise from background Web requests to increase performance and report visibility
- Reuse the same key when using temporary/ephemeral Diffie-Hellman key exchanges

Loadbalancer VIP:

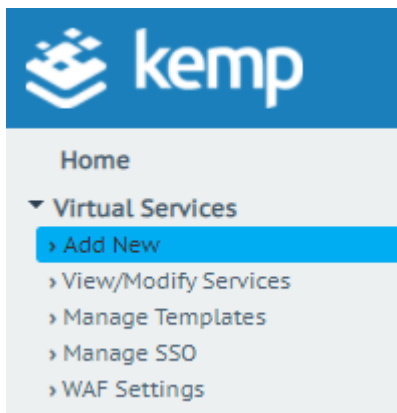


## Step 4. Configuring your Kemp Technologies LoadMaster.

**NOTE:** You may need to consult your Kemp Technologies partner or Kemp Technologies documentation/support to assist with best practices for this setup and how to configure this for your environment, as Censornet cannot provide direct support for third-party software. This guide offers a configuration that will work for load balancing Censornet USS Gateways assumes that your Kemp Technologies LoadMaster environment is already set up ready for these steps.



First, add a new Virtual Service. Navigate to Virtual Services, Add New.



This will show the "Add a new Virtual Service" page, Enter the required details as shown below.

**LoadMaster**  
Add a new Virtual Service

Please Specify the Parameters for the Virtual Service.

Virtual Address	<input type="text" value="10.10.10.10"/>
Port	<input type="text" value="8080"/>
Service Name (Optional)	<input type="text" value="filter.domain.local"/>
Use Template	<input type="text" value="Select a Template"/>
Protocol	<input type="text" value="tcp"/>

Then click add this Virtual Service.



Next, specify the "Persistence Option", "Scheduling Method" and Enable "Use Address for Server NAT". Expand the "Standard Options" section on the newly created VIP.

[<-Back](#)

**Basic Properties**

Service Name:  [Set Nickname](#)

Alternate Address:  [Set Alternate Address](#)

Service Type:  ▾

Activate or Deactivate Service:

---

**Standard Options**

Force L4:

Transparency:

Subnet Originating Requests:

Extra Ports:  [Set Extra Ports](#)

---

Persistence Options Mode:  ▾

Timeout:  ▾

---

Scheduling Method:  ▾

Idle Connection Timeout (Default 660):  [Set Idle Timeout](#)

Use Address for Server NAT:

Quality of Service:  ▾

Next, Add the Censornet USS Gateways to the VIP, Expand the "Real Servers" section, then select "8080 for the Checked Port, then select "Set Check Port" and then select "Add New."

**Real Servers** [Add New ...](#)

Real Server Check Method:  ▾

Checked Port:  [Set Check Port](#)

Enhanced Options:

Add the details for the Censornet USS Gateway, as shown below, then select "Add This Real Server."

Please Specify the Parameters for the Real Server

Allow Remote Addresses:

Real Server Address:  ▾

Port:

Forwarding method:  ▾

Weight:

Connection Limit:

[<-Back](#) [Add This Real Server](#)

The following Real Servers are already configured

The Real Server can be on any network

Select "Back"

[<-Back](#) [Add This Real Server](#)

Then repeat the above process to add another Censornet USS Gateway. The Kemp Technologies LoadMaster is now configured to load balance request to a pool of Censornet USS Gateways.