SSL Filtering and LCT Do Not Mix

SSL Filtering firewalls/routers will prevent the License Configuration Tool from connecting to the server for licensing, even though the user appears to have unblocked access to oms.cummins.com.

Purpose of SSL Filtering and How it Works

The Purpose of SSL filtering is allow network firewalls to scan the contents of encrypted connections in order to presumably look for viruses or block other undesirable content.

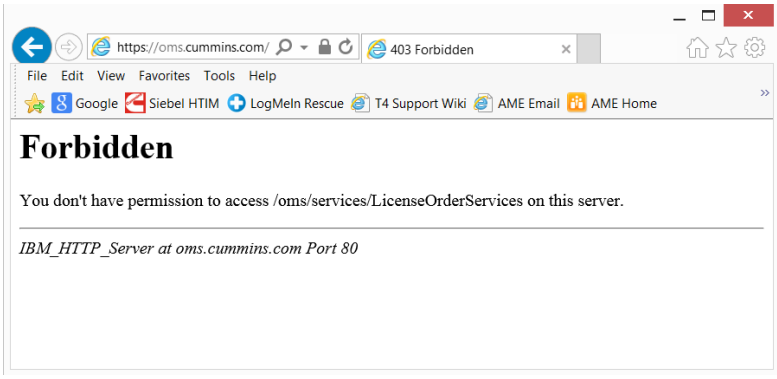
To do this, the firewall decrypts the connection and breaks the chain of trust. Then the firewall can read **all** encrypted content (including hypothetically personal emails, credit card numbers, etc). In order to stop PC's from recognizing the connection has been tampered with, the user's IT installs a certificate provided by the firewall onto the user's PC's as a "trusted" certificate, and then the firewall re-encrypts all SSL connections with that new "trusted" certificate.

Why SSL Filtering Breaks LCT

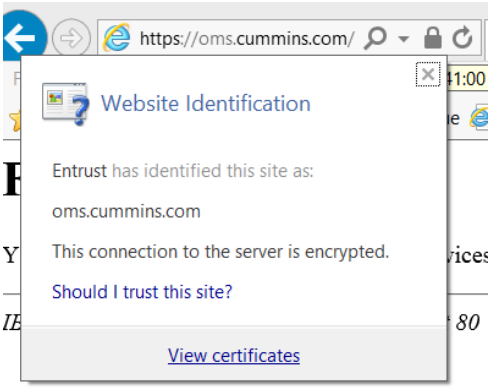
Unlike Internet Explorer, LCT has its own SSL certificate hardwired into the program, rather than one provided in Windows Certificate Manager. Since the firewall changes the certificate of oms.cummins.com to something other than the original certificate provider (currently Entrust), LCT's key will no longer work with oms.cummins.com's changed certificate. This is like changing the locks but LCT is still trying to use the old key, which no longer works.

How to Detect SSL Filtering

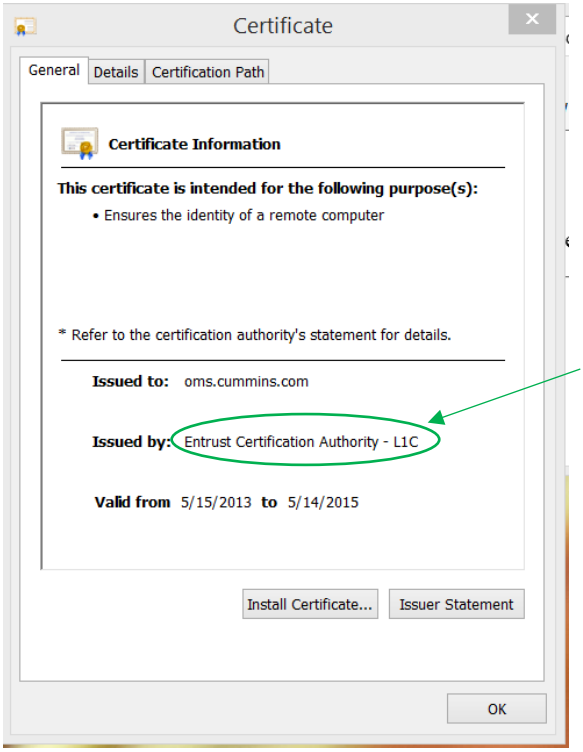
1. Open Internet Explorer. Do not use Firefox as it has its own certificate storage. Use only IE.
2. Go to oms.cummins.com. You should see the Forbidden page. If you don't, you have other connectivity issues besides SSL Filtering.



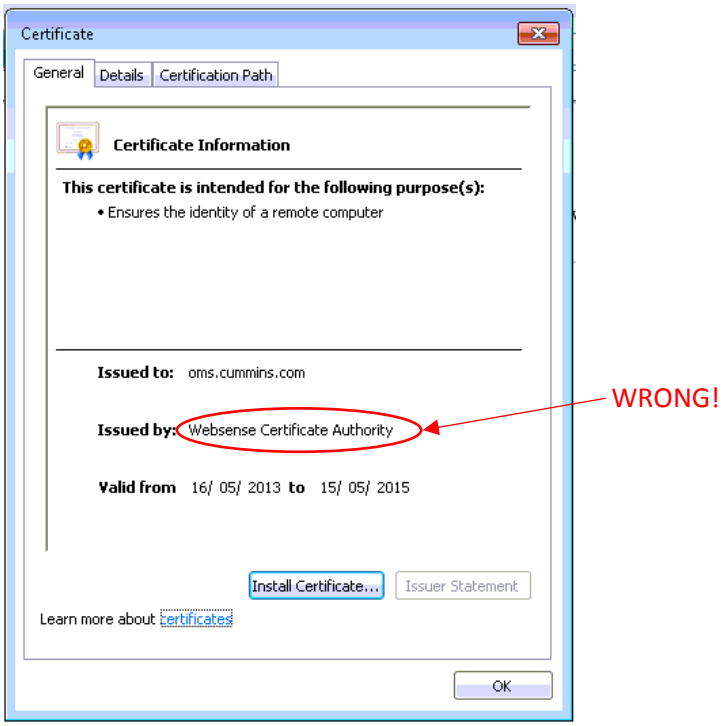
3. Click on the padlock next to the refresh button, and choose “View certificates”



4. In the General tab, verify the certificate was issued by Entrust, as the screenshot below:



IF IT SAYS ANYTHING BUT **Entrust**, SSL filtering is active, and LCT **will not work**. Below is an example of SSL Filtering done by Websense firewall:



How to allow LCT to Connect to OMS

The firewall is usually not on the computer itself and instead the user's IT must exclude oms.cummins.com from the firewall's SSL Filter. Most SSL filters have a "whitelist" of sites that are excluded from filtering. Since oms.cummins.com is used exclusively for licensing, there is no security compromise by placing it on the whitelist. If this is not possible, they could alternatively connect to a different network that does not have SSL filtering in place, or they could use offline activation.

LCT will likely never work with SSL filtering enabled as it can allow nefarious users to study the unencrypted communication between LCT and OMS.