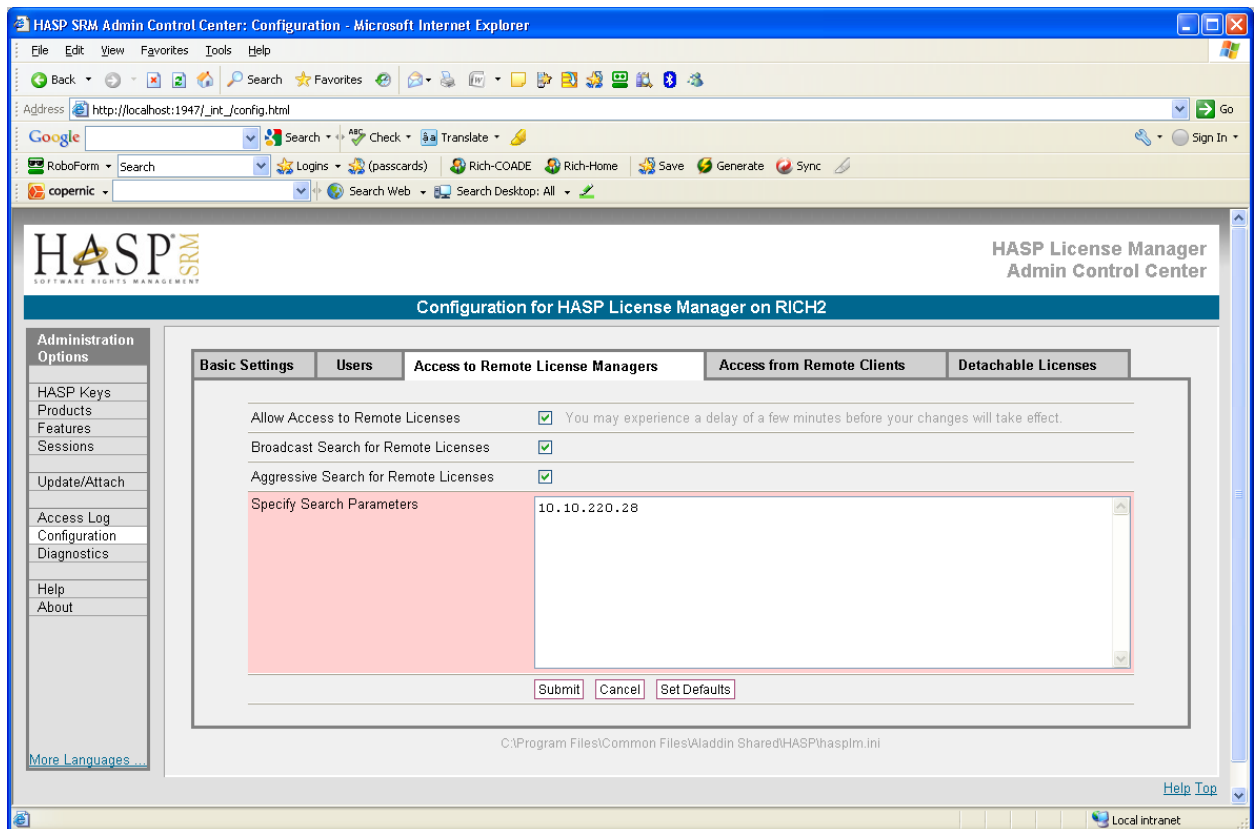


ICAS Network Licensing

Configuration for Network Licenses:

At the present time ICAS's software utilizes both the SRM and the HASP systems. For workstations to properly access a network license (either hardware or software) the following configuration steps should be followed:

- 1) In Admin Control Center (ACC) **on the License Server**, click on the "Access from Remote Clients" tab. Make sure the checkbox to "Allow Access from Remote Clients" is checked. (Admin Control Center runs inside a browser window and can be invoked by typing <http://localhost:1947>.)
- 2) In ACC, **on the Workstation**, click on the "Access to Remote License Managers" tab. Check all three checkboxes **AND** specify the IP address of the License Server, as shown here.



- 3) Copy the <\program\assidrv>\nethasp.ini file up into the program directory. Edit this INI file to:
 - a) Uncomment (remove the two semi-colons from the front of) all lines except for the "port number" line.
 - b) Set the NH_Server_Addr to the same Server IP address as set in the ACC.
 - c) Save this modified INI file.

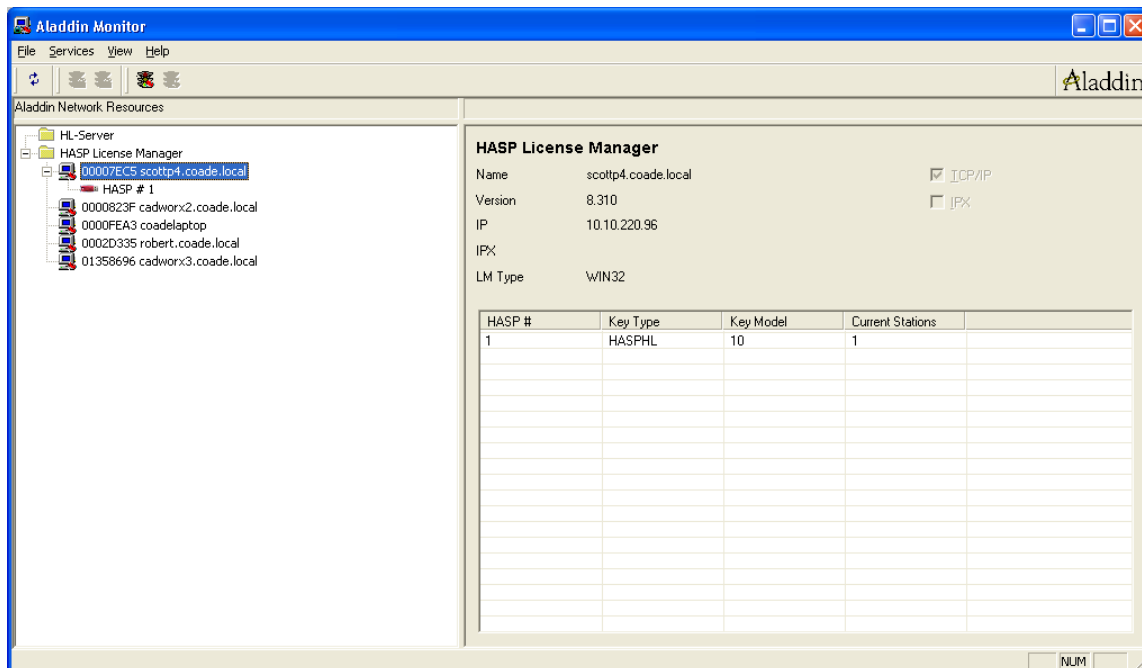
- 4) Check any firewall settings. Both ports 475 and 1947 must be open to allow the SRM/HASP system on the workstation to communicate with the License Server.

Verification of Network Licenses:

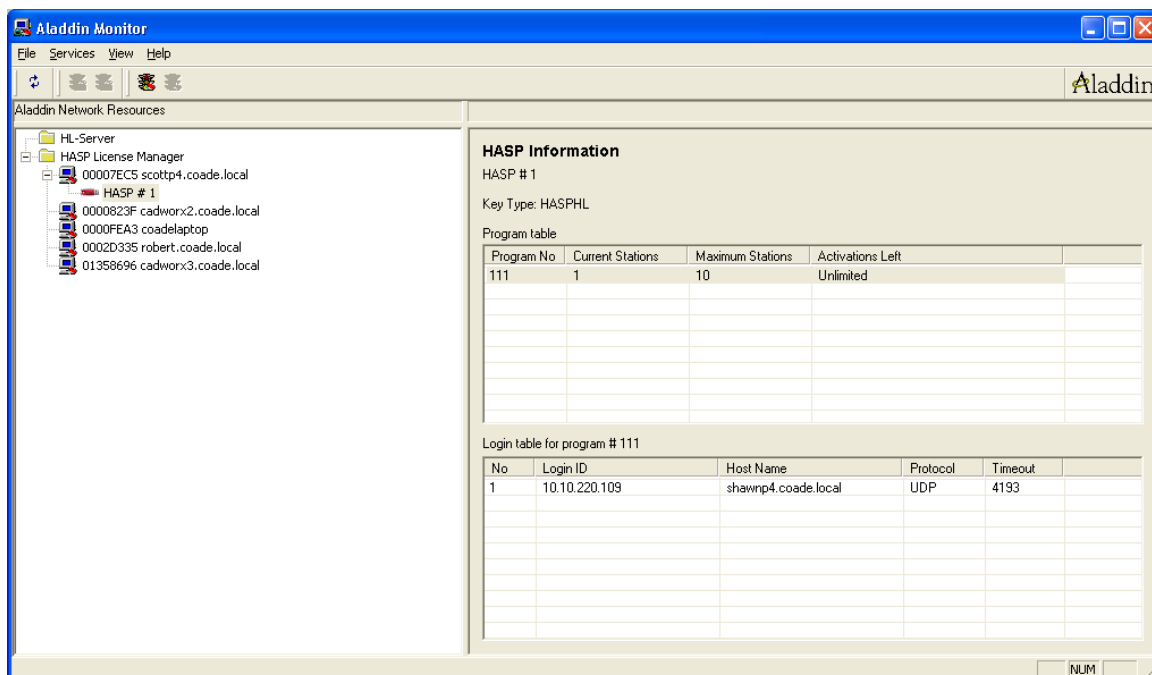
The ACC tool can be used to verify the operation of SRM network licenses (as discussed above). However, for HASP network licenses the “MONITOR” utility should be used. After installation, MONITOR can be invoked by clicking the desktop icon, which produces a window similar to the image below.



This window shows, in the left pane, all of the NetHASP Servers (keys) visible from the current workstation. Clicking on a particular Server shows the keys attached to that server, as shown below.



Clicking on a particular key shows, in the right hand pane, the licenses assigned to a particular key as well as how many licenses are in use.



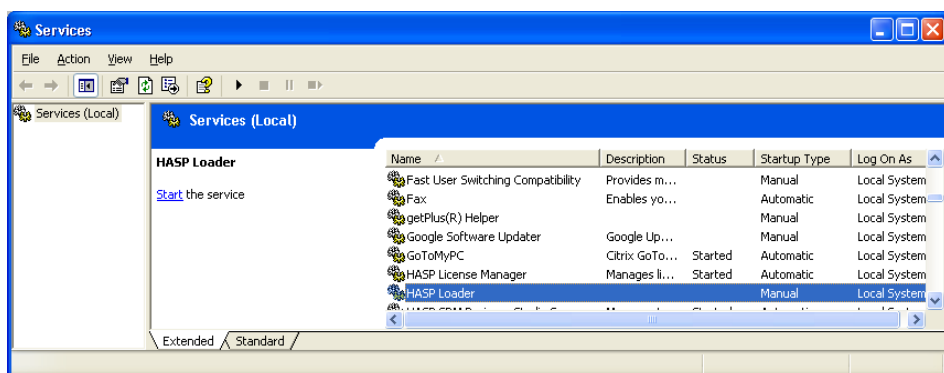
The NetHASP system relies on the “nethasp.ini” file on the client workstation, in the application directory. The “nethasp.ini” file should be setup as discussed above. Also as mentioned above, port 475 must be open for proper communication between the workstation and the License Manager (Server).

Trouble Shooting:

In the event that ICAS software cannot find the NetHASP key, MONITOR should be used from the workstation to verify communications. If MONITOR cannot find the key, then ICAS software won't be able to find the key either.

Items to check/verify include:

- Make sure you're dealing with a ICAS key. Verify that the gold lettering on the clear label states "MQCQX". If not, then the key will not run ICAS software products.
- Make sure the License Manager is running as a service, and the NetHASP key is plugged into a functioning USB port.



There are two HASP service entries in the table above. The first (HASP License Manager) is the newer SRM service that serves as both the License Manager and the local driver. The second (HASP Loader) is the older HASP HL License Manager. For HASP HL network licenses, both services must be running on the Server where the key is attached.

- Use the "PULSE.exe" program found in <ICAS program>\assidrv to verify that the NetHASP key can be accessed on the Server. This will treat the NetHASP as a local key, but the license data should be viewable. Verify that the license data makes sense. If you're trying to access a network key with PULSE, make sure you have a valid (correct) nethasp.ini file in the same directory as the pulse.exe file.
- After Server operations have been verified, use MONITOR on a workstation. Can the workstation find the NetHASP key? If not, check any Firewall settings.
- Go back to the NetHASP.INI file and increase the timeout values. Test again with MONITOR.
- Only after MONITOR can find the NetHASP key should ICAS products be accessed.

Most Frequent Problems:

- Not an ICAS key.
- A blank key.
- Services/LM not running.
- Driver not loaded or out of date.
- Ports blocked by a firewall.
- Inoperable USB port.
- Key not plugged in.
- Firmware update not applied.
- Incorrect/expired license data on key.

- Incorrect data in “nethasp.ini”
(wrong IP address, wrong protocol)