Restricted access licensing

LM-X License Manager enables you to precisely control which users are authorized to access your application. Software integrated with LM-X is bound to a license file that enforces usage restrictions and is designed to accommodate standard industry scenarios, such as the following.

Node-locked/machine-specific restrictions

Locking a license to an exact hardware identifier (hostid) is the most widely used restriction. Standalone licenses allow an application to run only on the specific machine for which they were granted. Likewise, network licenses that run on a license server prevent duplication by locking the license to a specific host. The result is an efficient copy protection mechanism: software and corresponding licenses that end up in the hands of unauthorized users simply will not run. LM-X supports a wide variety of hostids. To learn more about which type of hostid will work best for your needs, see Determining which HostID to use.

Named user restrictions

Local licenses can be locked to a specific username, while network licenses can be both user- and host-based. You can specify the number of “seats” in a license by setting the USERBASED and/or HOSTBASED directives and naming valid users and/or hosts in the license server configuration file. You have complete control over the user list, although there are restrictions on how frequently names can be changed.

Time zone restrictions

Time-zone-restricted licenses let you control license usage based on geographical location, ensuring that licenses are used only in the country or region you intend. You can limit license usage to specific time zones for both local and network licenses by setting the TIME_ZONES directive.

Dongle restrictions

You can lock your application with an X-Formation or 3rd-party dongle using the special hostid type DONGLE_HASPHL. With both local and network licenses, background checking can be done every few minutes to ensure that users do not move the dongle to other machines.