Configuration Best Practices

Performance & Scalability

- Run the CLIENT process as a Pathway Server Class. See CLIENT Process Configuration.
  - The CLIENT process does not use TMF. Set the SERVER TMF option to OFF.
  - Configure other server class options as you would any other context-sensitive server class to accommodate the application load.
  - Use the SERVER STARTUP option to configure a startup command file, which allows the startup options to be changed without re-configuring the server class.
- Use configuration files to specify logging options, which allows the options to be changed without re-configuring the server class. See Using Configuration Files.
- Use the monitor option where appropriate, to monitor changes to configuration files. See monitor.
- Do not use diagnostic logging in performance sensitive environments unless absolutely necessary.
- When using TLS connections with HTTP Basic authentication, use the *pre-auth* option. See http-credentials.
- If parameters in an API definition change between development, test, certification, and production environments, consider using API Parameters when defining the API. See Working with API Parameters.

Security

- Use TLS connections whenever possible, both when accessing REST applications and accessing the LightWave Client Console.
- Use the *sensitive* schema property to avoid disclosing sensitive data in logs. See Sensitive Data Masking.
- Use credentials files to supply configuration credentials. See Using Credentials Files
- Use Guardian security to appropriately secure API, configuration, credential, and program files.
- Only install the Console in production environments when necessary, or only run the Console in production when necessary.
  - The Console is generally not necessary outside of the development environment.
  - Not installing it will reduce the system's attack surface.