Configuration Overview

Once all classes of an application have been registered on the client and server machines, certain aspects of the application's behavior can be controlled and configured with system registry settings. This section summarizes the relevant registry entries and their meaning for NaturalX applications. For detailed background information about the registry keys and their administration, please refer to the specific DCOM registry documentation of the appropriate platform.

The registry keys relevant in this context are maintained with commonly-used tools like `DCOMCNFG` or the Registry Editor (`REGEDIT`). These tools present the registry keys in a different way. Therefore only the names of the registry keys are mentioned here. The section *DCOM Configuration on Windows* describes how to set registry keys.

Note:
"HKLM" is the common short form of the registry key *HKEY_LOCAL_MACHINE*, where "HKCR" stands for *HKEY_CLASSES_ROOT*.

This chapter covers the following topics:

- Server Configuration - General Settings
- Server Configuration - Application-Specific Settings
- Client Configuration - General Settings
- Client Configuration - Application-Specific Settings

Server Configuration - General Settings

This section discusses general server configuration settings.

- The registry entry *HKLM\Software\Microsoft\OLE\EnableDCOM* must be set to "Y" to enable access to the server machine via DCOM.
- If guests (users who do not have their own account on the server machine) are to be able to access applications on the server machine, the predefined account "Guest" must be enabled in the User Manager (Windows 2000 only).
- The registry entries *HKLM\Software\Microsoft\OLE\DefaultLaunchPermissions* and *HKLM\Software\Microsoft\OLE\DefaultAccessPermissions* define which users or groups are allowed or not allowed to launch DCOM applications and to access their classes. The authorizations defined here apply for all applications for which no application-specific settings are defined.
- The registry entry *HKLM\Software\Microsoft\OLE\LegacyAuthenticationLevel* controls the level of authentication that is performed for clients that access DCOM applications on this machine. If a NaturalX server is to be able to pass the client's user ID to Natural Security, the setting should be at least "Connect". Choose "None" if no authentication is to take place. In this case, the NaturalX server does not retrieve the client's user ID. Instead it performs each request under the user ID under which it was launched. If this entry is defined differently on the client side and on the server side, the stricter setting applies.

- The registry entry *HKLM\Software\Microsoft\OLE\LegacyImpersonationLevel* controls how much information a server may retrieve about the client, or if it may even use this information to act in the role of the client against other servers. If a NaturalX server is to be able to pass the client's user ID to Natural Security, the setting should be at least "Identify". The settings "Impersonate" or "Delegate" have the same effect for a NaturalX server. Choose "Anonymous", if the server is not to be able to retrieve the client's user ID. In this case, the server performs each request under the user ID under which it was launched. If this entry is defined differently on the client side and on the server side, the stricter setting applies.

Server Configuration - Application-Specific Settings

The application-specific settings can be set up differently for each NaturalX application. But the question is where to apply these settings. It is important to remember that all classes registered under one NaturalX server ID form one application in the DCOM sense, and are thus assigned to one AppID key in the registry. This is why the application-specific settings are applied under the AppID key.

- The registry entries *HKCR\AppID\<APPID>\LaunchPermission* and *HKCR\AppID\<APPID>\AccessPermission* define which users or groups are allowed or not allowed to launch the DCOM application with the specified AppID and to access its classes.

- The registry entry *HKCR\AppID\<APPID>\RunAs* defines the user account this NaturalX server will run when it is launched by DCOM. There are three options:

  - **Interactive user:**
    The NaturalX server is started under the account of the user that is interactively logged in on the server machine. This is usually not desirable but can be useful for test reasons.

  - **Launching user:**
    The NaturalX server is started under the account of the client that creates the first object on this server (remember that the first request for an object forces DCOM to launch the server). This setting should be used if each client is to be served by its own server process. Obviously, the client must have permission to launch the server.

  - **This user:**
    The server is started under the account of a given user. This setting should be used if all clients are to be served by the same server process. The user entered here must have permission to launch the server.

Client Configuration - General Settings

This section discusses general client configuration settings.

- The registry key *HKLM\Software\Microsoft\OLE\LegacyAuthenticationLevel* controls the degree of authentication that is performed for clients running on this machine when they access DCOM applications. For a client that accesses a NaturalX server, a similar consideration to that in the section *Server Configuration - General Settings* applies: only if it specifies at least "Connect", will the NaturalX server be able to use its user ID against Natural Security. If this entry is defined differently on the client side and on the server side, the stricter setting applies.

- The registry key *HKLM\Software\Microsoft\OLE\LegacyImpersonationLevel* controls how much information a server may retrieve about the client, or if it may even use this information to act in the role of the client against other servers. For a client that accesses a NaturalX server, a similar

consideration to that in the section *Server Configuration - General Settings* applies: only if it specifies at least "Identify", will the NaturalX server be able to retrieve its user ID and use it against Natural Security. If this entry is defined differently on the client side and on the server side, the stricter setting applies.

Client Configuration - Application-Specific Settings

The application-specific settings can be set up differently for each NaturalX application. But the question is where to apply these settings. Remember that all classes registered under one NaturalX server ID form one application in the DCOM sense, and are thus assigned to one AppID key in the registry. This is why the application-specific settings are applied under the AppID key.

- The registry key *HKCR\AppID\<APPID>\RemoteServerName* defines on which remote machine DCOM should start the server when a class hosted by this server is requested. If the server is to be started locally, "Run on this computer" and no RemoteServerName must be specified.