Registry Values for System-Wide Security - Win32 apps

By stevewhims

Archived: 2026-04-06 00:34:37 UTC

It is not recommended that you change the system-wide security settings, because this will affect all COM server applications that do not set their own process-wide security, and might prevent them from working properly. If you are changing the system-wide security settings to affect the security settings for a particular COM application, then you should instead change the process-wide security settings for that particular COM application. For more information about setting process-wide security, see Setting Process-Wide Security.

Certain values in the registry are used to determine security settings for applications that do not call **CoInitializeSecurity**. You can use Dcomcnfg.exe to modify these default security settings for a computer. For step-by-step procedures that describe how to use Dcomcnfg.exe for this purpose, see Setting System-Wide Security Using DCOMCNFG.

Another way to change default system-wide settings is to manipulate registry values directly. However, only administrators and the system have full access to the portion of the registry that contains the default system-wide call-security settings. All other users have read-access only.

The named values that affect system-wide security defaults are as follows:

- DefaultLaunchPermission
- DefaultAccessPermission
- LegacyAuthenticationLevel
- LegacyImpersonationLevel
- LegacySecureReferences
- SRPRunningObjectChecks
- SRPActivateAsActivatorChecks

Setting Process-Wide Security

Source: https://msdn.microsoft.com/en-us/library/windows/desktop/ms694331(v=vs.85).aspx