

Get/set local security settings programmatically

Source:

<http://www.derkeiler.com/Newsgroups/microsoft.public.platformsdk.security/2008-04/msg00005.html>

- *From:* "JH" <jh_ng@xxxxxxxxxxxxxxxxxxx>
 - *Date:* Thu, 3 Apr 2008 11:46:18 -0700
-

I asked a question about getting and settings Public Key Policies in Local Security Settings console. Along the same line, we are also trying to get and set the other entries. We have found Windows APIs to access some settings. For some other settings we are having a hard time finding the right APIs.

We have tried WMI with some of the settings but WMI support seems to be spotty and does not reliably work on all versions of Windows, or is not available on earlier versions.

So we'd like to get some help regarding retrieving and modifying the values for the settings below. There might be a few more – we we are still looking.

Thanks!
JH

Account Policies|Password Policy
Password must meet complexity requirements
Store passwords using reversible encryption

Local Policies|Security Options
Accounts: Administrator account status
Accounts: Guest account status
Accounts: Rename administrator account
Accounts: Rename guest account
Network access: Allow anonymous SID/Name translation
Network access: Do not allow anonymous enumeration of SAM accounts
Network access: Do not allow anonymous enumeration of SAM accounts and shares
Network access: Do not allow storage of credentials or .NET Passports for network authentication
Network access: Remotely accessible registry paths and sub-paths
Network access: Remotely accessible registry paths
Network access: Restrict anonymous access to Named Pipes and Shares

Get/set local security settings programmatically

DCOM: Machine Access Restrictions in Security Descriptor Definition

Language (SDDL) syntax

DCOM: Machine Launch Restrictions in Security Descriptor Definition

Language (SDDL) syntax

Domain controller: LDAP server signing requirements

Domain controller: Refuse machine account password changes

Interactive logon: Prompt user to change password before expiration

Interactive logon: Require Domain Controller authentication to unlock workstation

Interactive logon: Display user information when session is locked

System cryptography: Force strong key protection for user keys stored on the computer

System cryptography: Use FIPS compliant algorithms for encryption, hashing and signing

System settings: Optional subsystems

System settings: Use Certificate Rules on Windows Executables for Software Restriction Policies

.