Registry Key Security and Access Rights - Win32 apps

By stevewhims

Archived: 2026-04-05 18:30:43 UTC

The Windows security model enables you to control access to registry keys. For more information about security, see Access-Control Model.

You can specify a security descriptor for a registry key when you call the **RegCreateKeyEx** or **RegSetKeySecurity** function. If you specify **NULL**, the key gets a default security descriptor. The ACLs in a default security descriptor for a key are inherited from its direct parent key.

To get the security descriptor of a registry key, call the **RegGetKeySecurity**, **GetNamedSecurityInfo**, or **GetSecurityInfo** function.

The valid access rights for registry keys include the DELETE, READ_CONTROL, WRITE_DAC, and WRITE_OWNER standard access rights. Registry keys do not support the SYNCHRONIZE standard access right.

The following table lists the specific access rights for registry key objects.

Value	Meaning
KEY_ALL_ACCESS (0xF003F)	Combines the STANDARD_RIGHTS_REQUIRED, KEY_QUERY_VALUE, KEY_SET_VALUE, KEY_CREATE_SUB_KEY, KEY_ENUMERATE_SUB_KEYS, KEY_NOTIFY, and KEY_CREATE_LINK access rights.
KEY_CREATE_LINK (0x0020)	Reserved for system use.
KEY_CREATE_SUB_KEY (0x0004)	Required to create a subkey of a registry key.
KEY_ENUMERATE_SUB_KEYS (0x0008)	Required to enumerate the subkeys of a registry key.
KEY_EXECUTE (0x20019)	Equivalent to KEY_READ.
KEY_NOTIFY (0x0010)	Required to request change notifications for a registry key or for subkeys of a registry key.
KEY_QUERY_VALUE (0x0001)	Required to query the values of a registry key.
KEY_READ (0x20019)	Combines the STANDARD_RIGHTS_READ, KEY_QUERY_VALUE, KEY_ENUMERATE_SUB_KEYS, and KEY_NOTIFY values.

Value	Meaning
KEY_SET_VALUE (0x0002)	Required to create, delete, or set a registry value.
KEY_WOW64_32KEY (0x0200)	Indicates that an application on 64-bit Windows should operate on the 32-bit registry view. This flag is ignored by 32-bit Windows. For more information, see Accessing an Alternate Registry View. This flag must be combined using the OR operator with the other flags in this table that either query or access registry values. **Windows 2000:** This flag is not supported.
KEY_WOW64_64KEY (0x0100)	Indicates that an application on 64-bit Windows should operate on the 64-bit registry view. This flag is ignored by 32-bit Windows. For more information, see Accessing an Alternate Registry View. This flag must be combined using the OR operator with the other flags in this table that either query or access registry values. **Windows 2000:** This flag is not supported.
KEY_WRITE (0x20006)	Combines the STANDARD_RIGHTS_WRITE, KEY_SET_VALUE, and KEY_CREATE_SUB_KEY access rights.

When you call the **RegOpenKeyEx** function, the system checks the requested access rights against the key's security descriptor. If the user does not have the correct access to the registry key, the open operation fails. If an administrator needs access to the key, the solution is to enable the SE_TAKE_OWNERSHIP_NAME privilege and open the registry key with WRITE_OWNER access. For more information, see Enabling and Disabling Privileges.

You can request the ACCESS_SYSTEM_SECURITY access right to a registry key if you want to read or write the key's system access control list (SACL). For more information, see Access-Control Lists (ACLs) and SACL Access Right.

To view the current access rights for a key, including the predefined keys, use the Registry Editor (Regedt32.exe). After navigating to the desired key, go to the **Edit** menu and select **Permissions**.
