DuplicateTokenEx function (securitybaseapi.h) - Win32 apps

By GrantMeStrength

Archived: 2026-04-05 19:58:08 UTC

The **DuplicateTokenEx** function creates a new access token that duplicates an existing token. This function can create either a primary token or an impersonation token.

Syntax

```
BOOL DuplicateTokenEx(
  [in]           HANDLE                       hExistingToken,
  [in]           DWORD                        dwDesiredAccess,
  [in, optional] LPSECURITY_ATTRIBUTES        lpTokenAttributes,
  [in]           SECURITY_IMPERSONATION_LEVEL ImpersonationLevel,
  [in]           TOKEN_TYPE                   TokenType,
  [out]          PHANDLE                      phNewToken
);
```

Parameters

`[in] hExistingToken`

A handle to an access token opened with TOKEN_DUPLICATE access.

`[in] dwDesiredAccess`

Specifies the requested access rights for the new token. The **DuplicateTokenEx** function compares the requested access rights with the existing token's discretionary access control list (DACL) to determine which rights are granted or denied. To request the same access rights as the existing token, specify zero. To request all access rights that are valid for the caller, specify MAXIMUM_ALLOWED.

For a list of access rights for access tokens, see Access Rights for Access-Token Objects.

`[in, optional] lpTokenAttributes`

A pointer to a SECURITY_ATTRIBUTES structure that specifies a security descriptor for the new token and determines whether child processes can inherit the token. If *lpTokenAttributes* is **NULL**, the token gets a default security descriptor and the handle cannot be inherited. If the security descriptor contains a system access control list (SACL), the token gets ACCESS_SYSTEM_SECURITY access right, even if it was not requested in *dwDesiredAccess*.

To set the owner in the security descriptor for the new token, the caller's process token must have the **SE_RESTORE_NAME** privilege set.

`[in] ImpersonationLevel`

Specifies a value from the SECURITY_IMPERSONATION_LEVEL enumeration that indicates the impersonation level of the new token.

`[in] TokenType`

Specifies one of the following values from the TOKEN_TYPE enumeration.

Value	Meaning
TokenPrimary	The new token is a primary token that you can use in the CreateProcessAsUser function.
TokenImpersonation	The new token is an impersonation token.

`[out] phNewToken`

A pointer to a **HANDLE** variable that receives the new token.

When you have finished using the new token, call the CloseHandle function to close the token handle.

Return value

If the function succeeds, the function returns a nonzero value.

If the function fails, it returns zero. To get extended error information, call GetLastError.

The **DuplicateTokenEx** function allows you to create a primary token that you can use in the CreateProcessAsUser function. This allows a server application that is impersonating a client to create a process that has the security context of the client. Note that the DuplicateToken function can create only impersonation tokens, which are not valid for **CreateProcessAsUser**.

The following is a typical scenario for using **DuplicateTokenEx** to create a primary token. A server application creates a thread that calls one of the impersonation functions, such as ImpersonateNamedPipeClient, to impersonate a client. The impersonating thread then calls the OpenThreadToken function to get its own token, which is an impersonation token that has the security context of the client. The thread specifies this impersonation token in a call to **DuplicateTokenEx**, specifying the TokenPrimary flag. The **DuplicateTokenEx** function creates a *primary token* that has the security context of the client.

Requirements

Requirement	Value
Minimum supported client	Windows XP [desktop apps | UWP apps]
Minimum supported server	Windows Server 2003 [desktop apps | UWP apps]
Target Platform	Windows
Header	securitybaseapi.h (include Windows.h)
Library	Advapi32.lib
DLL	Advapi32.dll

See also

Access Control

Basic Access Control Functions

CloseHandle

CreateProcessAsUser

DdeImpersonateClient

DuplicateToken

ImpersonateNamedPipeClient

OpenThreadToken

RevertToSelf

RpcImpersonateClient

SECURITY_ATTRIBUTES

SECURITY_IMPERSONATION_LEVEL
