Create a token object - Windows 10

By vinaypamnani-msft

Archived: 2026-04-05 15:04:33 UTC

Applies to

- Windows 11
- Windows 10

Describes the best practices, location, values, policy management, and security considerations for the **Create a token object** security policy setting.

Reference

This policy setting determines which accounts a process can use to create a token, and which accounts it can then use to gain access to local resources when the process uses NtCreateToken() or other token-creation APIs.

When a user signs in to the local device or connects to a remote device through a network, Windows builds the user’s access token. Then the system examines the token to determine the level of the user's privileges. When you revoke a privilege, the change is immediately recorded, but the change isn't reflected in the user's access token until the next time the user logs on or connects.

Constant: SeCreateTokenPrivilege

Possible values

- User-defined list of accounts
- Not Defined

Best practices

- This user right is used internally by the operating system. Unless it's necessary, don't assign this user right to a user, group, or process other than Local System.

Location

Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment

Default values

This user right is used internally by the operating system. By default, it isn't assigned to any user groups.

The following table lists the actual and effective default policy values. Default values are also listed on the policy's property page.

Server type or GPO	Default value
Default Domain Policy	Not Defined
Default Domain Controller Policy	Not Defined
Stand-Alone Server Default Settings	Not Defined
Domain Controller Effective Default Settings	Local System
Member Server Effective Default Settings	Local System
Client Computer Effective Default Settings	Local System

Policy management

A restart of the device isn't required for this policy setting to be effective.

Any change to the user rights assignment for an account becomes effective the next time the owner of the account logs on.

Group Policy

Settings are applied in the following order through a Group Policy Object (GPO), which will overwrite settings on the local computer at the next Group Policy update:

1. Local policy settings
2. Site policy settings
3. Domain policy settings
4. OU policy settings

When a local setting is greyed out, it indicates that a GPO currently controls that setting.

Security considerations

This section describes how an attacker might exploit a feature or its configuration, how to implement the countermeasure, and the possible negative consequences of countermeasure implementation.

Vulnerability

> **Caution:** A user account that is given this user right has complete control over the system, and it can lead to the system being compromised. We highly recommend that you do not assign this right to any user accounts.

Windows examines a user's access token to determine the level of the user's privileges. Access tokens are built when users sign in to the local device or connect to a remote device over a network. When you revoke a privilege, the change is immediately recorded, but the change isn't reflected in the user's access token until the next time the user logs on or connects. Users with the ability to create or modify tokens can change the level of access for any account on a computer if they're currently logged on. They could escalate their privileges or create a DoS condition.

Countermeasure

Don't assign the **Create a token object** user right to any users. Processes that require this user right should use the Local System account, which already includes it, instead of a separate user account that has this user right assigned.

Potential impact

None. Not Defined is the default configuration.

- User Rights Assignment
