Replace a process level token - Windows 10

By vinaypamnani-msft

Archived: 2026-04-05 14:27:29 UTC

Applies to

- Windows 11
- Windows 10

Describes the best practices, location, values, policy management, and security considerations for the **Replace a process level token** security policy setting.

Reference

This policy setting determines which parent processes can replace the access token that is associated with a child process.

Specifically, the **Replace a process level token** setting determines which user accounts can call the CreateProcessAsUser() application programming interface (API) so that one service can start another. An example of a process that uses this user right is Task Scheduler, where the user right is extended to any processes that can be managed by Task Scheduler.

An access token is an object that describes the security context of a process or thread. The information in a token includes the identity and privileges of the user account that is associated with the process or thread. With this user right, every child process that runs on behalf of this user account would have its access token replaced with the process level token.

Constant: SeAssignPrimaryTokenPrivilege

Possible values

- User-defined list of accounts
- Defaults
- Not defined

Best practices

- For member servers, ensure that only the Local Service and Network Service accounts have the **Replace a process level token** user right.

Location

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

Default values

By default this setting is Network Service and Local Service on domain controllers and on stand-alone servers.

The following table lists the actual and effective default policy values for the most recent supported versions of Windows. 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	Network Service Local Service
Stand-Alone Server Default Settings	Network Service Local Service
Domain Controller Effective Default Settings	Network Service Local Service
Member Server Effective Default Settings	Network Service Local Service
Client Computer Effective Default Settings	Network Service Local Service

Policy management

This section describes features, tools, and guidance to help you manage this policy.

A restart of the device is not 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

Users with the **Replace a process level token** user right can start processes as another user if they know the user's credentials.

Countermeasure

For member servers, ensure that only the Local Service and Network Service accounts have the **Replace a process level token** user right.

Potential impact

On most computers, restricting the **Replace a process level token** user right to the Local Service and the Network Service built-in accounts is the default configuration, and there is no negative impact. However, if you have installed optional components such as ASP.NET or IIS, you may need to assign the **Replace a process level token** user right to additional accounts. For example, IIS requires that the Service, Network Service, and IWAM_<*ComputerName*> accounts be explicitly granted this user right.

- User Rights Assignment
