Increase scheduling priority

By Archiveddocs

Archived: 2026-04-06 03:15:16 UTC

Applies To: Windows Vista, Windows Server 2008, Windows 7, Windows 8.1, Windows Server 2008 R2, Windows Server 2012 R2, Windows Server 2012, Windows 8

This security policy reference topic for the IT professional describes the best practices, location, values, policy management, and security considerations for this policy setting.

This policy setting determines which user accounts can increase the base priority class of a process. It is not a privileged operation to increase relative priority within a priority class. This user right is not required by administrative tools that are supplied with the operating system, but it might be required by software development tools.

Specifically, this security setting determines which accounts can use a process with Write Property access to another process to increase the run priority that is assigned to the other process. A user with this privilege can change the scheduling priority of a process through the Task Manager user interface.

This policy setting is supported on versions of Windows that are designated in the **Applies To** list at the beginning of this topic.

Constant: SeIncreaseBasePriorityPrivilege

- User-defined list of accounts
- Not defined
- Administrators

1. Allow the default value, Administrators, as the only account responsible for controlling process scheduling priorities.

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

By default this setting is Administrators 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	Administrators
Stand-Alone Server Default Settings	Administrators
Domain Controller Effective Default Settings	Administrators
Member Server Effective Default Settings	Administrators
Client Computer Effective Default Settings	Administrators

There are no differences in the way this policy setting works between the supported versions of Windows that are designated in the **Applies To** list at the beginning of this topic.

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

A restart of the computer 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.

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.

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.

A user who is assigned this user right could increase the scheduling priority of a process to Real-Time, which would leave little processing time for all other processes and could lead to a denial-of-service condition.

Verify that only Administrators have the **Increase scheduling priority** user right assigned to them.

None. Restricting the **Increase scheduling priority** user right to members of the Administrators group is the default configuration.

User Rights Assignment
