Create symbolic links - Windows 10

By vinaypamnani-msft

Archived: 2026-04-05 18:29:32 UTC

▶
▶

Applies to

- Windows 11
- Windows 10

Describes the best practices, location, values, policy management, and security considerations for the **Create symbolic links** security policy setting.

Reference

This user right determines if users can create a symbolic link from the device they're logged on to.

A symbolic link is a file system object that points to another file system object that is called the target. Symbolic links are transparent to users. The links appear as normal files or directories, and they can be acted upon by the user or application in exactly the same manner. Symbolic links are designed to aid in migration and application compatibility with UNIX operating systems. Microsoft has implemented symbolic links to function just like UNIX links.

Warning

This privilege should only be given to trusted users. Symbolic links can expose security vulnerabilities in applications that aren't designed to handle them.

Constant: SeCreateSymbolicLinkPrivilege

Possible values

- User-defined list of accounts
- Not Defined

Best practices

- Only trusted users should get this user right. Symbolic links can expose security vulnerabilities in applications that aren't designed to handle them.

Location

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

Default values

By default, members of the Administrators group have this right.

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	Administrators
Member Server Effective Default Settings	Administrators
Client Computer Effective Default Settings	Administrators

Policy management

This section describes different features and tools available to help you manage this policy.

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:

- Local policy settings
- Site policy settings
- Domain policy settings
- OU policy settings

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

Command-line tools

This setting can be used in conjunction with a symbolic link file system setting that can be manipulated with the command-line tool to control the kinds of symlinks that are allowed on the device. For more info, type `fsutil`

`behavior set symlinkevaluation /?` at the command prompt.

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 who have the **Create symbolic links** user right could inadvertently or maliciously expose your system to symbolic link attacks. Symbolic link attacks can be used to change the permissions on a file, to corrupt data, to destroy data, or as a DoS attack.

Countermeasure

Don't assign the **Create symbolic links** user right to standard users. Restrict this right to trusted administrators. You can use the **fsutil** command to establish a symbolic link file system setting that controls the kind of symbolic links that can be created on a computer.

Potential impact

None. Not defined is the default configuration.

- User Rights Assignment
