**User Rights Assignment**

* 04/19/2017
* 2 minutes to read

**Applies to**

* Windows 10

Provides an overview and links to information about the User Rights Assignment security policy settings user rights that are available in Windows. User rights govern the methods by which a user can log on to a system. User rights are applied at the local device level, and they allow users to perform tasks on a device or in a domain. User rights include logon rights and permissions. Logon rights control who is authorized to log on to a device and how they can log on. User rights permissions control access to computer and domain resources, and they can override permissions that have been set on specific objects. User rights are managed in Group Policy under the **User Rights Assignment** item.

Each user right has a constant name and a Group Policy name associated with it. The constant names are used when referring to the user right in log events. You can configure the user rights assignment settings in the following location within the Group Policy Management Console (GPMC) under **Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment**, or on the local device by using the Local Group Policy Editor (gpedit.msc).

For information about setting security policies, see [Configure security policy settings](https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/how-to-configure-security-policy-settings).

The following table links to each security policy setting and provides the constant name for each. Setting descriptions contain reference information, best practices for configuring the policy setting, default values, differences between operating system versions, and considerations for policy management and security.

|  | |
| --- | --- |
| **Group Policy Setting** | **Constant Name** |
| [Access Credential Manager as a trusted caller](https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/access-credential-manager-as-a-trusted-caller) | SeTrustedCredManAccessPrivilege |
| [Access this computer from the network](https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/access-this-computer-from-the-network) | SeNetworkLogonRight |
| [Act as part of the operating system](https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/act-as-part-of-the-operating-system) | SeTcbPrivilege |
| [Add workstations to domain](https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/add-workstations-to-domain) | SeMachineAccountPrivilege |
| [Adjust memory quotas for a process](https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/adjust-memory-quotas-for-a-process) | SeIncreaseQuotaPrivilege |
| [Allow log on locally](https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/allow-log-on-locally) | SeInteractiveLogonRight |
| [Allow log on through Remote Desktop Services](https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/allow-log-on-through-remote-desktop-services) | SeRemoteInteractiveLogonRight |
| [Back up files and directories](https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/back-up-files-and-directories) | SeBackupPrivilege |
| [Bypass traverse checking](https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/bypass-traverse-checking) | SeChangeNotifyPrivilege |
| [Change the system time](https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/change-the-system-time) | SeSystemtimePrivilege |
| [Change the time zone](https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/change-the-time-zone) | SeTimeZonePrivilege |
| [Create a pagefile](https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/create-a-pagefile) | SeCreatePagefilePrivilege |
| [Create a token object](https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/create-a-token-object) | SeCreateTokenPrivilege |
| [Create global objects](https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/create-global-objects) | SeCreateGlobalPrivilege |
| [Create permanent shared objects](https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/create-permanent-shared-objects) | SeCreatePermanentPrivilege |
| [Create symbolic links](https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/create-symbolic-links) | SeCreateSymbolicLinkPrivilege |
| [Debug programs](https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/debug-programs) | SeDebugPrivilege |
| [Deny access to this computer from the network](https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/deny-access-to-this-computer-from-the-network) | SeDenyNetworkLogonRight |
| [Deny log on as a batch job](https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/deny-log-on-as-a-batch-job) | SeDenyBatchLogonRight |
| [Deny log on as a service](https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/deny-log-on-as-a-service) | SeDenyServiceLogonRight |
| [Deny log on locally](https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/deny-log-on-locally) | SeDenyInteractiveLogonRight |
| [Deny log on through Remote Desktop Services](https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/deny-log-on-through-remote-desktop-services) | SeDenyRemoteInteractiveLogonRight |
| [Enable computer and user accounts to be trusted for delegation](https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/enable-computer-and-user-accounts-to-be-trusted-for-delegation) | SeEnableDelegationPrivilege |
| [Force shutdown from a remote system](https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/force-shutdown-from-a-remote-system) | SeRemoteShutdownPrivilege |
| [Generate security audits](https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/generate-security-audits) | SeAuditPrivilege |
| [Impersonate a client after authentication](https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/impersonate-a-client-after-authentication) | SeImpersonatePrivilege |
| [Increase a process working set](https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/increase-a-process-working-set) | SeIncreaseWorkingSetPrivilege |
| [Increase scheduling priority](https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/increase-scheduling-priority) | SeIncreaseBasePriorityPrivilege |
| [Load and unload device drivers](https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/load-and-unload-device-drivers) | SeLoadDriverPrivilege |
| [Lock pages in memory](https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/lock-pages-in-memory) | SeLockMemoryPrivilege |
| [Log on as a batch job](https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/log-on-as-a-batch-job) | SeBatchLogonRight |
| [Log on as a service](https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/log-on-as-a-service) | SeServiceLogonRight |
| [Manage auditing and security log](https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/manage-auditing-and-security-log) | SeSecurityPrivilege |
| [Modify an object label](https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/modify-an-object-label) | SeRelabelPrivilege |
| [Modify firmware environment values](https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/modify-firmware-environment-values) | SeSystemEnvironmentPrivilege |
| [Perform volume maintenance tasks](https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/perform-volume-maintenance-tasks) | SeManageVolumePrivilege |
| [Profile single process](https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/profile-single-process) | SeProfileSingleProcessPrivilege |
| [Profile system performance](https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/profile-system-performance) | SeSystemProfilePrivilege |
| [Remove computer from docking station](https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/remove-computer-from-docking-station) | SeUndockPrivilege |
| [Replace a process level token](https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/replace-a-process-level-token) | SeAssignPrimaryTokenPrivilege |
| [Restore files and directories](https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/restore-files-and-directories) | SeRestorePrivilege |
| [Shut down the system](https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/shut-down-the-system) | SeShutdownPrivilege |
| [Synchronize directory service data](https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/synchronize-directory-service-data) | SeSyncAgentPrivilege |
| [Take ownership of files or other objects](https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/take-ownership-of-files-or-other-objects) | SeTakeOwnershipPrivilege |

**Related topics**

* [Security policy settings reference](https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/security-policy-settings-reference)