Local Accounts

By officedocspr5

Archived: 2026-04-05 13:12:25 UTC

This article describes the default local user accounts for Windows operating systems, and how to manage the built-in accounts.

About local user accounts

Local user accounts are defined locally on a device, and can be assigned rights and permissions on the device only. Local user accounts are security principals that are used to secure and manage access to the resources on a device, for services or users.

Default local user accounts

The *default local user accounts* are built-in accounts that are created automatically when the operating system is installed. The default local user accounts can't be removed or deleted and don't provide access to network resources.

Default local user accounts are used to manage access to the local device's resources based on the rights and permissions that are assigned to the account. The default local user accounts, and the local user accounts that you create, are located in the *Users* folder. The Users folder is located in the Local Users and Groups folder in the local *Computer Management* Microsoft Management Console (MMC). *Computer Management* is a collection of administrative tools that you can use to manage a local or remote device.

Default local user accounts are described in the following sections. Expand each section for more information.

Administrator

The default local Administrator account is a user account for system administration. Every computer has an Administrator account (SID S-1-5-*domain*-500, display name Administrator). The Administrator account is the first account that is created during the Windows installation.

The Administrator account has full control of the files, directories, services, and other resources on the local device. The Administrator account can create other local users, assign user rights, and assign permissions. The Administrator account can take control of local resources at any time by changing the user rights and permissions.

The default Administrator account can't be deleted or locked out, but it can be renamed or disabled.

Windows setup disables the built-in Administrator account and creates another local account that is a member of the Administrators group.

Members of the Administrators groups can run apps with elevated permissions without using the *Run as Administrator* option. Fast User Switching is more secure than using `runas` or different-user elevation.

Account group membership

By default, the Administrator account is a member of the Administrators group. It's a best practice to limit the number of users in the Administrators group because members of the Administrators group have Full Control permissions on the device.

The Administrator account can't be removed from the Administrators group.

Security considerations

Because the Administrator account is known to exist on many versions of the Windows operating system, it's a best practice to disable the Administrator account when possible to make it more difficult for malicious users to gain access to the server or client computer.

You can rename the Administrator account. However, a renamed Administrator account continues to use the same automatically assigned security identifier (SID), which can be discovered by malicious users. For more information about how to rename or disable a user account, see Disable or activate a local user account and Rename a local user account.

As a security best practice, use your local (non-Administrator) account to sign in and then use **Run as administrator** to accomplish tasks that require a higher level of rights than a standard user account. Don't use the Administrator account to sign in to your computer unless it's entirely necessary. For more information, see Run a program with administrative credentials.

Group Policy can be used to control the use of the local Administrators group automatically. For more information about Group Policy, see Group Policy Overview.

Important

- Blank passwords are not allowed
- Even when the Administrator account is disabled, it can still be used to gain access to a computer by using safe mode. In the Recovery Console or in safe mode, the Administrator account is automatically enabled. When normal operations are resumed, it's disabled.

Guest

The Guest account lets occasional or one-time users, who don't have an account on the computer, temporarily sign in to the local server or client computer with limited user rights. By default, the Guest account is disabled and has a blank password. Since the Guest account can provide anonymous access, it's considered a security risk. For this reason, it's a best practice to leave the Guest account disabled, unless its use is necessary.

Guest account group membership

By default, the Guest account is the only member of the default Guests group `SID S-1-5-32-546`, which lets a user sign in to a device.

Guest account security considerations

When enabling the Guest account, only grant limited rights and permissions. For security reasons, the Guest account shouldn't be used over the network and made accessible to other computers.

In addition, the guest user in the Guest account shouldn't be able to view the event logs. After the Guest account is enabled, it's a best practice to monitor the Guest account frequently to ensure that other users can't use services and other resources. This includes resources that were unintentionally left available by a previous user.

HelpAssistant

The HelpAssistant account is a default local account that is enabled when a Remote Assistance session is run. This account is automatically disabled when no Remote Assistance requests are pending.

HelpAssistant is the primary account that is used to establish a Remote Assistance session. The Remote Assistance session is used to connect to another computer running the Windows operating system, and it's initiated by invitation. For solicited remote assistance, a user sends an invitation from their computer, through e-mail or as a file, to a person who can provide assistance. After the user's invitation for a Remote Assistance session is accepted, the default HelpAssistant account is automatically created to give the person who provides assistance limited access to the computer. The HelpAssistant account is managed by the Remote Desktop Help Session Manager service.

HelpAssistant account security considerations

The SIDs that pertain to the default HelpAssistant account include:

- SID: `S-1-5-<domain>-13`, display name *Terminal Server User*. This group includes all users who sign in to a server with Remote Desktop Services enabled.
- SID: `S-1-5-<domain>-14`, display name *Remote Interactive Logon*. This group includes all users who connect to the computer by using a remote desktop connection. This group is a subset of the Interactive group. Access tokens that contain the Remote Interactive Logon SID also contain the Interactive SID.

For the Windows Server operating system, Remote Assistance is an optional component that isn't installed by default. You must install Remote Assistance before it can be used.

For details about the HelpAssistant account attributes, see the following table.

HelpAssistant account attributes

Attribute	Value
Well-Known SID/RID	`S-1-5-<domain>-13 (Terminal Server User), S-1-5-<domain>-14 (Remote Interactive Logon)`
Type	User
Default container	`CN=Users, DC=<domain>`
Default members	None
Default member of	Domain Guests Guests
Protected by ADMINSDHOLDER?	No
Safe to move out of default container?	Can be moved out, but we don't recommend it.
Safe to delegate management of this group to non-Service admins?	No

DefaultAccount

The DefaultAccount account, also known as the Default System Managed Account (DSMA), is a well-known user account type. DefaultAccount can be used to run processes that are either multi-user aware or user-agnostic.

The DSMA is disabled by default on the desktop editions and on the Server operating systems with the desktop experience.

The DSMA has a well-known RID of `503`. The security identifier (SID) of the DSMA will thus have a well-known SID in the following format: `S-1-5-21-\<ComputerIdentifier>-503`.

The DSMA is a member of the well-known group **System Managed Accounts Group**, which has a well-known SID of `S-1-5-32-581`.

The DSMA alias can be granted access to resources during offline staging even before the account itself is created. The account and the group are created during first boot of the machine within the Security Accounts Manager (SAM).

How Windows uses the DefaultAccount

From a permission perspective, the DefaultAccount is a standard user account. The DefaultAccount is needed to run multi-user-manifested-apps (MUMA apps). MUMA apps run all the time and react to users signing in and signing out of the devices. Unlike Windows Desktop where apps run in context of the user and get terminated when the user signs off, MUMA apps run by using the DSMA.

MUMA apps are functional in shared session SKUs such as Xbox. For example, Xbox shell is a MUMA app. Today, Xbox automatically signs in as Guest account and all apps run in this context. All the apps are multi-user-aware and respond to events fired by user manager. The apps run as the Guest account.

Similarly, Phone auto logs in as a *DefApps* account, which is akin to the standard user account in Windows but with a few extra privileges. Brokers, some services and apps run as this account.

In the converged user model, the multi-user-aware apps and multi-user-aware brokers will need to run in a context different from that of the users. For this purpose, the system creates DSMA.

How the DefaultAccount is created on domain controllers

If the domain was created with domain controllers running Windows Server 2016, the DefaultAccount exists on all domain controllers in the domain. If the domain was created with domain controllers running an earlier version of Windows Server, the DefaultAccount is created after the PDC Emulator role is transferred to a domain controller that runs Windows Server 2016. The DefaultAccount is then replicated to all other domain controllers in the domain.

Recommendations for managing the Default Account (DSMA)

Microsoft doesn't recommend changing the default configuration, where the account is disabled. There's no security risk with having the account in the disabled state. Changing the default configuration could hinder future scenarios that rely on this account.

Default local system accounts

SYSTEM

The *SYSTEM* account is used by the operating system and by services running under Windows. There are many services and processes in the Windows operating system that need the capability to sign in internally, such as during a Windows installation. The SYSTEM account was designed for that purpose, and Windows manages the SYSTEM account's user rights. It's an internal account that doesn't show up in User Manager, and it can't be added to any groups.

On the other hand, the SYSTEM account does appear on an NTFS file system volume in File Manager in the **Permissions** portion of the **Security** menu. By default, the SYSTEM account is granted Full Control permissions to all files on an NTFS volume. Here the SYSTEM account has the same functional rights and permissions as the Administrator account.

Note

To grant the account Administrators group file permissions does not implicitly give permission to the SYSTEM account. The SYSTEM account's permissions can be removed from a file, but we do not recommend removing them.

NETWORK SERVICE

The *NETWORK SERVICE* account is a predefined local account used by the service control manager (SCM). A service that runs in the context of the NETWORK SERVICE account presents the computer's credentials to remote servers. For more information, see NetworkService Account.

LOCAL SERVICE

The *LOCAL SERVICE* account is a predefined local account used by the service control manager. It has minimum privileges on the local computer and presents anonymous credentials on the network. For more information, see LocalService Account.

How to manage local user accounts

The default local user accounts, and the local user accounts you create, are located in the Users folder. The Users folder is located in Local Users and Groups. For more information about creating and managing local user accounts, see Manage Local Users.

You can use Local Users and Groups to assign rights and permissions on only the local server to limit the ability of local users and groups to perform certain actions. A right authorizes a user to perform certain actions on a server, such as backing up files and folders or shutting down a server. An access permission is a rule that is associated with an object, usually a file, folder, or printer. It regulates which users can have access to an object on the server and in what manner.

You can't use Local Users and Groups on a domain controller. However, you can use Local Users and Groups on a domain controller to target remote computers that aren't domain controllers on the network.

Note

You use Active Directory Users and Computers to manage users and groups in Active Directory.

You can also manage local users by using NET.EXE USER and manage local groups by using NET.EXE LOCALGROUP, or by using various PowerShell cmdlets and other scripting technologies.

Restrict and protect local accounts with administrative rights

An administrator can use many approaches to prevent malicious users from using stolen credentials such as a stolen password or password hash, for a local account on one computer from being used to authenticate on another computer with administrative rights. This is also called *lateral movement*.

The simplest approach is to sign in to your computer with a standard user account, instead of using the Administrator account for tasks. For example, use a standard account to browse the Internet, send email, or use a word processor. When you want to perform administrative tasks such as installing a new program or changing a setting that affects other users, you don't have to switch to an Administrator account. You can use User Account Control (UAC) to prompt you for permission or an administrator password before performing the task, as described in the next section.

The other approaches that can be used to restrict and protect user accounts with administrative rights include:

- Enforce local account restrictions for remote access
- Deny network logon to all local Administrator accounts
- Create unique passwords for local accounts with administrative rights

Each of these approaches is described in the following sections.

Note

These approaches do not apply if all administrative local accounts are disabled.

Enforce local account restrictions for remote access

User Account Control (UAC) is a security feature that informs you when a program makes a change that requires administrative permissions. UAC works by adjusting the permission level of your user account. By default, UAC is set to notify you when applications try to make changes to your computer, but you can change when UAC notifies you.

UAC makes it possible for an account with administrative rights to be treated as a standard user nonadministrator account until full rights, also called elevation, is requested and approved. For example, UAC lets an administrator enter credentials during a nonadministrator's user session to perform occasional administrative tasks without having to switch users, sign out, or use the *Run as* command.

In addition, UAC can require administrators to specifically approve applications that make system-wide changes before those applications are granted permission to run, even in the administrator's user session.

For example, a default feature of UAC is shown when a local account signs in from a remote computer by using Network logon (for example, by using NET.EXE USE). In this instance, it's issued a standard user token with no administrative rights, but without the ability to request or receive elevation. Consequently, local accounts that sign in by using Network logon can't access administrative shares such as C$, or ADMIN$, or perform any remote administration.

For more information about UAC, see User Account Control.

The following table shows the Group Policy and registry settings that are used to enforce local account restrictions for remote access.

Note

You can also enforce the default for LocalAccountTokenFilterPolicy by using the custom ADMX in Security Templates.

To enforce local account restrictions for remote access

1. Start the **Group Policy Management** Console (GPMC)
2. In the console tree, expand <*Forest*>\Domains<*Domain*>, and then **Group Policy Objects** where *forest* is the name of the forest, and *domain* is the name of the domain where you want to set the Group Policy

Object (GPO)

3. In the console tree, right-click **Group Policy Objects > New**
4. In the **New GPO** dialog box, type <**gpo_name**>, and > **OK** where *gpo_name* is the name of the new GPO. The GPO name indicates that the GPO is used to restrict local administrator rights from being carried over to another computer
5. In the details pane, right-click <**gpo_name**>, and > **Edit**
6. Ensure that UAC is enabled and that UAC restrictions apply to the default Administrator account by following these steps:
    - Navigate to the **Computer Configuration** > **Windows Settings** > **Security Settings** > **Local Policies** > **Security Options**
    - Select **User Account Control: Run all administrators in Admin Approval Mode** > **Enabled** > **OK**
    - Select **User Account Control: Admin Approval Mode for the Built-in Administrator account** > **Enabled** > **OK**
7. Ensure that the local account restrictions are applied to network interfaces by following these steps:
    - Navigate to *Computer Configuration\Preferences and Windows Settings*, and > **Registry**
    - Right-click **Registry**, and > **New** > **Registry Item**
    - In the **New Registry Properties** dialog box, on the **General** tab, change the setting in the **Action** box to **Replace**
    - Ensure that the **Hive** box is set to **HKEY_LOCAL_MACHINE**
    - Select (**…**), browse to the following location for **Key Path** > **Select** for: `SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System`
    - In the **Value name** area, type `LocalAccountTokenFilterPolicy`
    - In the **Value type** box, from the drop-down list, select **REG_DWORD** to change the value
    - In the **Value data** box, ensure that the value is set to **0**
    - Verify this configuration, and > **OK**
8. Link the GPO to the first **Workstations** organizational unit (OU) by doing the following:
    - Navigate to the `*Forest*\<Domains>\*Domain*\*OU*` path
    - Right-click the **Workstations > Link an existing GPO**
    - Select the GPO that you created, and > **OK**
9. Test the functionality of enterprise applications on the workstations in that first OU and resolve any issues caused by the new policy
10. Create links to all other OUs that contain workstations
11. Create links to all other OUs that contain servers

Deny network logon to all local Administrator accounts

Denying local accounts the ability to perform network logons can help prevent a local account password hash from being reused in a malicious attack. This procedure helps to prevent lateral movement by ensuring that stolen credentials for local accounts from a compromised operating system can't be used to compromise other computers that use the same credentials.

Note

To perform this procedure, you must first identify the name of the local, default Administrator account, which might not be the default user name "Administrator", and any other accounts that are members of the local Administrators group.

The following table shows the Group Policy settings that are used to deny network logon for all local Administrator accounts.

No.	Setting	Detailed Description
	Policy location	Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment
1	Policy name	Deny access to this computer from the network
	Policy setting	Local account and member of Administrators group
2	Policy location	Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment
	Policy name	Deny log on through Remote Desktop Services
	Policy setting	Local account and member of Administrators group

To deny network logon to all local administrator accounts

1. Start the **Group Policy Management** Console (GPMC)
2. In the console tree, expand <*Forest*>\Domains<*Domain*>, and then **Group Policy Objects**, where *forest* is the name of the forest, and *domain* is the name of the domain where you want to set the Group Policy Object (GPO)
3. In the console tree, right-click **Group Policy Objects**, and > **New**
4. In the **New GPO** dialog box, type <**gpo_name**>, and then > **OK** where *gpo_name* is the name of the new GPO indicates that it's being used to restrict the local administrative accounts from interactively signing in to the computer
5. In the details pane, right-click <**gpo_name**>, and > **Edit**

6. Configure the user rights to deny network logons for administrative local accounts as follows:
7. Navigate to the Computer Configuration\Windows Settings\Security Settings, and > **User Rights Assignment**
8. Double-click **Deny access to this computer from the network**
9. Select **Add User or Group**, type **Local account and member of Administrators group**, and > **OK**
10. Configure the user rights to deny Remote Desktop (Remote Interactive) logons for administrative local accounts as follows:
11. Navigate to Computer Configuration\Policies\Windows Settings and Local Policies, and then select **User Rights Assignment**
12. Double-click **Deny log on through Remote Desktop Services**
13. Select **Add User or Group**, type **Local account and member of Administrators group**, and > **OK**
14. Link the GPO to the first **Workstations** OU as follows:
    - Navigate to the <*Forest*>\Domains<*Domain*>\OU path
    - Right-click the **Workstations** OU, and > **Link an existing GPO**
    - Select the GPO that you created, and > **OK**
15. Test the functionality of enterprise applications on the workstations in that first OU and resolve any issues caused by the new policy
16. Create links to all other OUs that contain workstations
17. Create links to all other OUs that contain servers

Note

You might have to create a separate GPO if the user name of the default Administrator account is different on workstations and servers.

Create unique passwords for local accounts with administrative rights

Passwords should be unique per individual account. While it's true for individual user accounts, many enterprises have identical passwords for common local accounts, such as the default Administrator account. This also occurs when the same passwords are used for local accounts during operating system deployments.

Passwords that are left unchanged or changed synchronously to keep them identical add a significant risk for organizations. Randomizing the passwords mitigates "pass-the-hash" attacks by using different passwords for local accounts, which hamper the ability of malicious users to use password hashes of those accounts to compromise other computers.

Passwords can be randomized by:

- Purchasing and implementing an enterprise tool to accomplish this task. These tools are commonly referred to as "privileged password management" tools
- Configuring Local Administrator Password Solution (LAPS) to accomplish this task
- Creating and implementing a custom script or solution to randomize local account passwords

---