

Active Directory Accounts

By robinharwood

Archived: 2026-04-05 16:22:31 UTC

Windows Server operating systems are installed with default local accounts. In addition, you can create user accounts to meet the requirements of your organization.

This reference article describes the Windows Server default local accounts that are stored locally on the domain controller and used in Active Directory. It doesn't describe default local user accounts for a member, standalone server, or Windows client. For more information, see [Local accounts](#).

Default local accounts in Active Directory

Default local accounts are built-in accounts that are created automatically when a Windows Server domain controller is installed and the domain is created. These default local accounts have counterparts in Active Directory. They also have domain-wide access and are completely separate from the default local user accounts for a member or standalone server.

You can assign rights and permissions to default local accounts on a particular domain controller, and only on that domain controller. These accounts are local to the domain. After the default local accounts are installed, they're stored in the Users container in Active Directory Users and Computers. It's a best practice to keep the default local accounts in the User container and not attempt to move these accounts to, for example, a different organizational unit (OU).

The default local accounts in the Users container include: Administrator, Guest, and KRBTGT. The HelpAssistant account is installed when a Remote Assistance session is established. The following sections describe the default local accounts and their use in Active Directory.

Default local accounts perform the following actions:

- Let the domain represent, identify, and authenticate the identity of the user who's assigned to the account by using unique credentials (user name and password). It's a best practice to assign each user to a single account to ensure maximum security. Multiple users aren't allowed to share one account. A user account lets a user sign in to computers, networks, and domains with a unique identifier that can be authenticated by the computer, network, or domain.
- Authorize (grant or deny) access to resources. After a user's credentials have been authenticated, the user is authorized to access the network and domain resources based on the user's explicitly assigned rights on the resource.
- Audit the actions that are carried out on user accounts.

In Active Directory, administrators use default local accounts to manage domain and member servers directly and from dedicated administrative workstations. Active Directory accounts provide access to network resources. Active Directory User accounts and Computer accounts can represent a physical entity, such as a computer or person, or act as dedicated service accounts for some applications.

Each default local account is automatically assigned to a security group that's preconfigured with the appropriate rights and permissions to perform specific tasks. Active Directory security groups collect user accounts, computer accounts, and other groups into manageable units. For more information, see [Active Directory security groups](#).

On an Active Directory domain controller, each default local account is referred to as a security principal. A security principal is a directory object that's used to secure and manage Active Directory services that provide access to domain controller resources. A security principal includes objects such as user accounts, computer accounts, security groups, or the threads or processes that run in the security context of a user or computer account. For more information, see [Security principals](#).

A security principal is represented by a unique security identifier (SID). The SIDs that are related to each of the default local accounts in Active Directory are described in the next sections.

Some of the default local accounts are protected by a background process that periodically checks and applies a specific security descriptor. A security descriptor is a data structure that contains security information that's associated with a protected object. This process ensures that any successful unauthorized attempt to modify the security descriptor on one of the default local accounts or groups is overwritten with the protected settings.

This security descriptor is present on the AdminSDHolder object. If you want to modify the permissions on one of the service administrator groups or on any of its member accounts, you must modify the security descriptor on the AdminSDHolder object to ensure that it's applied consistently. Be careful when you make these modifications, because you're also changing the default settings that are applied to all your protected accounts.

Administrator account

An Administrator account is a default account that's used in all versions of the Windows operating system on every computer and device. The Administrator account is used by the system administrator for tasks that require administrative credentials. This account can't be deleted or locked out, but the account can be renamed or disabled.

The Administrator account gives the user complete access (Full Control permissions) to the files, directories, services, and other resources that are on that local server. You can use the Administrator account to create local users, and to assign user rights and access control permissions. You can also use the account to take control of local resources at any time simply by changing the user rights and permissions. Although files and directories can be protected from the Administrator account temporarily, the account can take control of these resources at any time by changing the access permissions.

Account group membership

The Administrator account has membership in the default security groups, as described in the Administrator account attributes table later in this article.

The security groups ensure that you can control administrator rights without having to change each Administrator account. In most instances, you don't have to change the basic settings for this account. However, you might have to change its advanced settings, such as membership in particular groups.

Security considerations

After installation of the server operating system, your first task is to set up the Administrator account properties securely. This includes setting up an especially long, strong password, and securing the Remote control and Remote Desktop Services profile settings.

The Administrator account can also be disabled when it's not required. Renaming or disabling the Administrator account makes it more difficult for malicious users to try to gain access to the account. However, even when the Administrator account is disabled, it can still be used to gain access to a domain controller by using safe mode.

On a domain controller, the Administrator account becomes the Domain Admin account. The Domain Admin account is used to sign in to the domain controller, and this account requires a strong password. The Domain Admin account gives you access to domain resources.

Note

When the domain controller is initially installed, you can sign in and use Server Manager to set up a local Administrator account, with the rights and permissions you want to assign. For example, you can use a local Administrator account to manage the operating system when you first install it. By using this approach, you can set up the operating system without getting locked out. Generally, you don't need to use the account after installation. You can create local user accounts on the domain controller only before Active Directory Domain Services is installed, and not afterward.

When Active Directory is installed on the first domain controller in the domain, the Administrator account is created for Active Directory. The Administrator account is the most powerful account in the domain. It's given domain-wide access and administrative rights to administer the computer and the domain, and it has the most extensive rights and permissions over the domain. The person who installs Active Directory Domain Services on the computer creates the password for this account during the installation.

Administrator account attributes

Attribute	Value
Well-known SID/RID	S-1-5- <domain> -500
Type	User
Default container	CN=Users, DC= <domain> , DC=
Default members	N/A
Default member of	Administrators, Domain Admins, Enterprise Administrators, Domain Users (the Primary Group ID of all user accounts is

Attribute	Value
	Domain Users) Group Policy Creator Owners, and Schema Admins in Active Directory Domain Users group
Protected by AdminSdHolder?	Yes
Safe to move out of default container?	Yes
Safe to delegate management of this group to nonservice administrators?	No

Guest account

The Guest account is a default local account that has limited access to the computer and is disabled by default. By default, the Guest account password is left blank. A blank password allows the Guest account to be accessed without requiring the user to enter a password.

The Guest account enables occasional or one-time users, who don't have an individual account on the computer, to sign in to the local server or domain with restricted rights and permissions. The Guest account can be enabled, and the password can be set up if needed, but only by a member of the Administrator group on the domain.

Guest account group membership

The Guest account has membership in the default security groups that are described in the following Guest account attributes table. By default, the Guest account is the only member of the default Guests group, which lets a user sign in to a server, and the Domain Guests global group, which lets a user sign in to a domain.

A member of the Administrators group or Domain Admins group can set up a user with a Guest account on one or more computers.

Guest account security considerations

Because the Guest account can provide anonymous access, it's a security risk. It also has a well-known SID. For this reason, it's a best practice to leave the Guest account disabled, unless its use is required and then only with restricted rights and permissions for a very limited period of time.

When the Guest account is required, an Administrator on the domain controller is required to enable the Guest account. The Guest account can be enabled without requiring a password, or it can be enabled with a strong password. The Administrator also grants restricted rights and permissions for the Guest account. To help prevent unauthorized access:

- *Don't* grant the Guest account the [Shut down the system](#) user right. When a computer is shutting down or starting up, it's possible that a Guest user or anyone with local access, such as a malicious user, could gain

unauthorized access to the computer.

- *Don't* provide the Guest account with the ability to view the event logs. After the Guest account is enabled, it's a best practice to monitor this account frequently to ensure that other users can't use services and other resources, such as resources that were unintentionally left available by a previous user.
- *Don't* use the Guest account when the server has external network access or access to other computers.

If you decide to enable the Guest account, be sure to restrict its use and to change the password regularly. As with the Administrator account, you might want to rename the account as an added security precaution.

In addition, an administrator is responsible for managing the Guest account. The administrator monitors the Guest account, disables the Guest account when it's no longer in use, and changes or removes the password as needed.

For details about the Guest account attributes, see the following table:

Guest account attributes

Attribute	Value
Well-known SID/RID	S-1-5- <domain> -501
Type	User
Default container	CN=Users, DC= <domain> , DC=
Default members	None
Default member of	Guests, Domain 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

HelpAssistant account (installed with a Remote Assistance session)

The HelpAssistant account is a default local account that's 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's 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 email 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 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. In Windows Server 2008, Remote Desktop Services is called Terminal Services.
- 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 you can use it.

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> , DC=
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

KRBTGT account

The KRBTGT account is a local default account that acts as a service account for the Key Distribution Center (KDC) service. This account can't be deleted, and the account name can't be changed. The KRBTGT account can't

be enabled in Active Directory.

KRBTGT is also the security principal name used by the KDC for a Windows Server domain, as specified by RFC 4120. The KRBTGT account is the entity for the KRBTGT security principal, and it's created automatically when a new domain is created.

Windows Server Kerberos authentication is achieved by the use of a special Kerberos ticket-granting ticket (TGT) enciphered with a symmetric key. This key is derived from the password of the server or service to which access is requested. The TGT password of the KRBTGT account is known only by the Kerberos service. To request a session ticket, you must present the TGT to the KDC. The TGT is issued to the Kerberos client from the KDC.

KRBTGT account maintenance considerations

A strong password is assigned to the KRBTGT and trust accounts automatically. You should change these passwords on a regular schedule, as you would with any privileged service account. The password for the KDC account is used to derive a secret key for encrypting and decrypting the TGT requests that are issued. The password for a domain trust account is used to derive an inter-realm key for encrypting referral tickets.

To reset the password, you need to either be a member of the Domain Admins group or be delegated the appropriate authority. In addition, you must be a member of the local Administrators group or be delegated the appropriate authority.

After you reset the KRBTGT password, ensure that event ID 9 in the (Kerberos) Key-Distribution-Center event source is written to the System event log.

KRBTGT account security considerations

It's also a best practice to reset the KRBTGT account password to ensure that a newly restored domain controller doesn't replicate with a compromised domain controller. In this case, in a large forest recovery that's spread across multiple locations, you can't guarantee that all domain controllers are shut down and, if they're shut down, that they can't be rebooted again before all the appropriate recovery steps are performed. After you reset the KRBTGT account, another domain controller can't replicate this account password by using an old password.

An organization suspecting domain compromise of the KRBTGT account should consider the use of professional incident response services. The impact to restore the ownership of the account is domain-wide, labor intensive, and should be undertaken as part of a larger recovery effort.

The KRBTGT password is the key from which all trust in Kerberos chains up to. Resetting the KRBTGT password is similar to renewing the root CA certificate with a new key and immediately not trusting the old key, resulting in almost all subsequent Kerberos operations being affected.

For all account types (users, computers, and services):

- All the TGTs that are already issued and distributed will be invalid because the DCs will reject them. These tickets are encrypted with the KRBTGT so any DC can validate them. When the password changes, the tickets become invalid.

- All currently authenticated sessions that signed-in users have established (based on their service tickets) to a resource (such as a file share, SharePoint site, or Exchange server) are good until the service ticket is required to reauthenticate.
- NTLM authenticated connections aren't affected.

Because it's impossible to predict the specific errors that will occur for any given user in a production operating environment, you must assume that all computers and users will be affected.

Important

Rebooting a computer is the only reliable way to recover functionality, because doing so will cause both the computer account and user accounts to sign back in again. Signing in again will request new TGTs that are valid with the new KRBTGT, which will correct any KRBTGT-related operational issues on that computer.

Read-only domain controllers and the KRBTGT account

The RODC is advertised as the Key Distribution Center (KDC) for the branch office. The RODC uses a different KRBTGT account and password than the KDC on a writable domain controller when it signs or encrypts TGT requests. After an account is successfully authenticated, the RODC determines whether a user's credentials or a computer's credentials can be replicated from the writable domain controller to the RODC by using the Password Replication Policy.

After the credentials are cached on the RODC, the RODC can accept that user's sign-in requests until the credentials change. When a TGT is signed with the KRBTGT account of the RODC, the RODC recognizes that it has a cached copy of the credentials. If another domain controller signs the TGT, the RODC forwards requests to a writable domain controller.

KRBTGT account attributes

For details about the KRBTGT account attributes, see the following table:

Attribute	Value
Well-known SID/RID	S-1-5- <domain> -502
Type	User
Default container	CN=Users, DC= <domain> , DC=
Default members	None
Default member of	Domain Users group. (The Primary Group ID of all user accounts is Domain Users.)
Protected by AdminSdHolder?	Yes
Safe to move out of default container?	Can be moved out, but we don't recommend it.

Attribute	Value
Safe to delegate management of this group to non-Service admins?	No

Settings for default local accounts in Active Directory

Each default local account in Active Directory has several account settings that you can use to configure password settings and security-specific information, as described in the following table:

Account setting	Description
User must change password at next logon	Forces a password change the next time that the user signs in to the network. Use this option when you want to ensure that the user is the only person who knows their password.
User can't change password	Prevents the user from changing the password. Use this option when you want to maintain control over a user account, such as for a Guest or temporary account.
Password never expires	Prevents a user password from expiring. It's a best practice to enable this option with service accounts and to use strong passwords.
Store passwords using reversible encryption	<p>Provides support for applications that use protocols requiring knowledge of the plaintext form of the user's password for authentication purposes.</p> <p>This option is required when you're using Challenge Handshake Authentication Protocol (CHAP) in Internet Authentication Services (IAS), and when you're using digest authentication in Internet Information Services (IIS).</p>
Account is disabled	Prevents the user from signing in with the selected account. As an administrator, you can use disabled accounts as templates for common user accounts.
Smart card is required for interactive logon	<p>Requires that a user has a smart card to sign on to the network interactively. The user must also have a smart card reader attached to their computer and a valid personal identification number (PIN) for the smart card.</p> <p>When this attribute is applied on the account, the effect is as follows:</p> <ul style="list-style-type: none"> • The attribute restricts only initial authentication for interactive sign-in and Remote Desktop sign-in. When interactive or Remote Desktop sign-in requires a subsequent network sign-in, such as with a domain credential, an NT Hash provided by the domain controller is used to complete the smart card authentication process. • Each time the attribute is enabled on an account, the account's current password hash value is replaced with a 128-bit random number. This invalidates the use of any

Account setting	Description
	<p>previously configured passwords for the account. The value doesn't change after that unless a new password is set or the attribute is disabled and re-enabled.</p> <ul style="list-style-type: none"> Accounts with this attribute can't be used to start services or run scheduled tasks.
Account is trusted for delegation	<p>Lets a service running under this account to perform operations on behalf of other user accounts on the network. A service running under a user account (also known as a service account) that's trusted for delegation can impersonate a client to gain access to resources, either on the computer where the service is running or on other computers. For example, in a forest that's set to the Windows Server 2003 functional level, this setting is found on the Delegation tab. It's available only for accounts that have been assigned service principal names (SPNs), which are set by using the <code>setspn</code> command from Windows Support Tools. This setting is security-sensitive and should be assigned cautiously.</p>
Account is sensitive and can't be delegated	<p>Gives control over a user account, such as a Guest account or a temporary account. This option can be used if this account can't be assigned for delegation by another account.</p>
Use DES encryption types for this account	<p>Provides support for the Data Encryption Standard (DES). DES supports multiple levels of encryption, including Microsoft Point-to-Point Encryption (MPPE) Standard (40-bit and 56-bit), MPPE standard (56-bit), MPPE Strong (128-bit), Internet Protocol Security (IPSec) DES (40-bit), IPSec 56-bit DES, and IPSec Triple DES (3DES).</p>
Don't require Kerberos preauthentication	<p>Provides support for alternative implementations of the Kerberos protocol. Because preauthentication provides additional security, use caution when you're enabling this option. Domain controllers running Windows 2000 or Windows Server 2003 can use other mechanisms to synchronize time.</p>

Note

DES isn't enabled by default in Windows Server operating systems (starting with Windows Server 2008 R2) or in Windows client operating systems (starting with Windows 7). For these operating systems, computers won't use DES-CBC-MD5 or DES-CBC-CRC cipher suites by default. If your environment requires DES, this setting might affect compatibility with client computers or services and applications in your environment.

For more information, see [Hunting down DES to securely deploy Kerberos](#).

Manage default local accounts in Active Directory

After the default local accounts are installed, these accounts reside in the Users container in Active Directory Users and Computers. You can create, disable, reset, and delete default local accounts by using the Active Directory Users and Computers Microsoft Management Console (MMC) and by using command-line tools.

You can use Active Directory Users and Computers to assign rights and permissions on a specified local domain controller, and that domain controller only, to limit the ability of local users and groups to perform certain actions. A right authorizes a user to perform certain actions on a computer, such as backing up files and folders or shutting down a computer. In contrast, an access permission is a rule that's associated with an object, usually a file, folder, or printer, that regulates which users can have access to the object and in what manner.

For more information about creating and managing local user accounts in Active Directory, see [Manage local users](#).

You can also use Active Directory Users and Computers on a domain controller to target remote computers that aren't domain controllers on the network.

You can obtain recommendations from Microsoft for domain controller configurations that you can distribute by using the Security Compliance Manager (SCM) tool. For more information, see [Microsoft Security Compliance Manager](#).

Some of the default local user accounts are protected by a background process that periodically checks and applies a specific security descriptor, which is a data structure that contains security information that's associated with a protected object. This security descriptor is present on the AdminSDHolder object.

This means that, when you want to modify the permissions on a service administrator group or on any of its member accounts, you're also required to modify the security descriptor on the AdminSDHolder object. This approach ensures that the permissions are applied consistently. Be careful when you make these modifications, because this action can also affect the default settings that are applied to all your protected administrative accounts.

Restrict and protect sensitive domain accounts

Restricting and protecting domain accounts in your domain environment requires you to adopt and implement the following best practices approach:

- Strictly limit membership to the Administrators, Domain Admins, and Enterprise Admins groups.
- Stringently control where and how domain accounts are used.

Member accounts in the Administrators, Domain Admins, and Enterprise Admins groups in a domain or forest are high-value targets for malicious users. To limit any exposure, it's a best practice to strictly limit membership to these administrator groups to the smallest number of accounts. Restricting membership in these groups reduces the possibility that an administrator might unintentionally misuse these credentials, creating a vulnerability that malicious users can exploit.

Moreover, it's a best practice to stringently control where and how sensitive domain accounts are used. Restrict the use of Domain Admins accounts and other Administrator accounts to prevent them from being used to sign in to management systems and workstations that are secured at the same level as the managed systems. When Administrator accounts aren't restricted in this manner, each workstation from which a domain administrator signs in provides another location that malicious users can exploit.

Implementing these best practices is separated into the following tasks:

- [Separate Administrator accounts from user accounts](#)
- [Restrict administrator sign-in access to servers and workstations](#)
- [Disable the account delegation right for sensitive Administrator accounts](#)

To provide for instances where integration challenges with the domain environment are expected, each task is described according to the requirements for a minimum, better, and ideal implementation. As with all significant changes to a production environment, ensure that you test these changes thoroughly before you implement and deploy them. Then stage the deployment in a manner that allows for a rollback of the change if technical issues occur.

Separate Administrator accounts from user accounts

Restrict Domain Admins accounts and other sensitive accounts to prevent them from being used to sign in to lower trust servers and workstations. Restrict and protect Administrator accounts by segregating Administrator accounts from standard user accounts, by separating administrative duties from other tasks, and by limiting the use of these accounts. Create dedicated accounts for administrative personnel who require administrator credentials to perform specific administrative tasks, and then create separate accounts for other standard user tasks, according to the following guidelines:

- **Privileged account:** Allocate Administrator accounts to perform the following administrative duties only:
 - **Minimum:** Create separate accounts for domain administrators, enterprise administrators, or the equivalent, with appropriate administrator rights in the domain or forest. Use accounts that have been granted sensitive administrator rights only to administer domain data and domain controllers.
 - **Better:** Create separate accounts for administrators that have reduced administrative rights, such as accounts for workstation administrators, and accounts with user rights over designated Active Directory organizational units (OUs).
 - **Ideal:** Create multiple, separate accounts for an administrator who has several job responsibilities that require different trust levels. Set up each Administrator account with different user rights, such as for workstation administration, server administration, and domain administration, to let the administrator sign in to specified workstations, servers, and domain controllers based strictly on their job responsibilities.
- **Standard user account:** Grant standard user rights for standard user tasks, such as email, web browsing, and using line-of-business (LOB) applications. These accounts shouldn't be granted administrator rights.

Important

Ensure that sensitive Administrator accounts can't access email or browse the internet, as described in the following section.

To learn more about privileged access, see [Privileged access devices](#).

Restrict administrator sign-in access to servers and workstations

It's a best practice to restrict administrators from using sensitive Administrator accounts to sign in to lower-trust servers and workstations. This restriction prevents administrators from inadvertently increasing the risk of credential theft by signing in to a lower-trust computer.

Important

Ensure that you either have local access to the domain controller or you've built at least one dedicated administrative workstation.

Restrict sign-in access to lower-trust servers and workstations by using the following guidelines:

- **Minimum:** Restrict domain administrators from having sign-in access to servers and workstations. Before you start this procedure, identify all OUs in the domain that contain workstations and servers. Any computers in OUs that aren't identified won't restrict administrators with sensitive accounts from signing in to them.
- **Better:** Restrict domain administrators from nondomain controller servers and workstations.
- **Ideal:** Restrict server administrators from signing in to workstations, in addition to domain administrators.

Note

For this procedure, don't link accounts to the OU that contain workstations for administrators that perform administration duties only, and don't provide internet or email access.

To restrict domain administrators from workstations (minimum)

1. As a domain administrator, open the Group Policy Management Console (GPMC).
2. Open **Group Policy Management**, expand `<forest>\Domains\ <domain>`.
3. Right-click **Group Policy Objects**, and then select **New**.

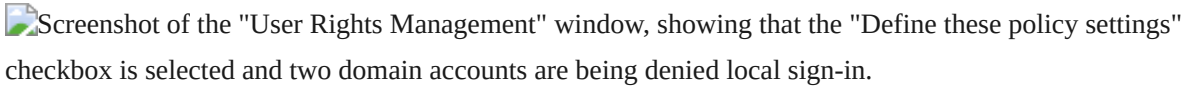
 Screenshot of the Group Policy Management console window, showing the "Group Policy Objects" command and shortcut menu.

4. In the **New GPO** window, name the GPO that restricts administrators from signing in to workstations, and then select **OK**.

 Screenshot of the "New GPO" window for entering the group name and source starter GPO.

5. Right-click **New GPO**, and then select **Edit**.
6. Configure user rights to deny sign-in locally for domain administrators.
7. Select **Computer Configuration > Policies > Windows Settings > Local Policies**, select **User Rights Assignment**, and then do the following:

1. Double-click **Deny logon locally**, and then select **Define these policy settings**.
2. Select **Add User or Group**, select **Browse**, type **Enterprise Admins**, and then select **OK**.
3. Select **Add User or Group**, select **Browse**, type **Domain Admins**, and then select **OK**.

Screenshot of the "User Rights Management" window, showing that the "Define these policy settings" checkbox is selected and two domain accounts are being denied local sign-in.


Tip

You can optionally add any groups that contain server administrators whom you want to restrict from signing in to workstations.

Note

Completing this step might cause issues with administrator tasks that run as scheduled tasks or services with accounts in the Domain Admins group. The practice of using domain Administrator accounts to run services and tasks on workstations creates a significant risk of credential theft attacks and, therefore, should be replaced with alternative means to run scheduled tasks or services.

- d. Select **OK** to complete the configuration.
8. Link the GPO to the first Workstations OU. Go to the `<forest>\Domains\ <domain> \OU` path, and then do the following:
 - a. Right-click the workstation OU, and then select **Link an Existing GPO**.

Screenshot of the Group Policy Management console window, where you right-click a Workstations item and select "Link an Existing GPO".

- b. Select the GPO that you just created, and then select **OK**.

Screenshot of the "Select GPO" window, where you select a domain and Group Policy Objects.

9. Test the functionality of enterprise applications on workstations in the first OU, and resolve any issues caused by the new policy.
10. Link all other OUs that contain workstations.

However, don't create a link to the Administrative Workstation OU if it's created for administrative workstations that are dedicated to administration duties only and are without internet or email access.

Important

If you later extend this solution, don't deny sign-in rights for the Domain Users group. The Domain Users group includes all user accounts in the domain, including Users, Domain Administrators, and Enterprise Administrators.


Disable the account delegation right for sensitive Administrator accounts

Although user accounts aren't marked for delegation by default, accounts in an Active Directory domain can be trusted for delegation. This means that a service or a computer that's trusted for delegation can impersonate an account that authenticates to it to access other resources across the network.

For sensitive accounts, such as those belonging to members of the Administrators, Domain Admins, or Enterprise Admins groups in Active Directory, delegation can present a substantial risk of rights escalation. For example, if an account in the Domain Admins group is used to sign in to a compromised member server that's trusted for delegation, that server can request access to resources in the context of the Domain Admins account and escalate the compromise of that member server to a domain compromise.

It's a best practice to configure the user objects for all sensitive accounts in Active Directory by selecting the **Account is sensitive and cannot be delegated** checkbox under **Account options** to prevent the accounts from being delegated. For more information, see [Settings for default local accounts in Active Directory](#).

As with any configuration change, test this enabled setting fully to ensure that it performs correctly before you implement it.

 Screenshot of the Active Directory account properties window. The "Account is sensitive and cannot be delegated" checkbox is selected.

Secure and manage domain controllers

It's a best practice to strictly enforce restrictions on the domain controllers in your environment. This ensures that the domain controllers:

- Run only required software.
- Require that software is regularly updated.
- Are configured with the appropriate security settings.

One aspect of securing and managing domain controllers is to ensure that the default local user accounts are fully protected. It's of primary importance to restrict and secure all sensitive domain accounts, as described in the preceding sections.

Because domain controllers store credential password hashes of all accounts in the domain, they're high-value targets for malicious users. When domain controllers aren't well managed and secured by using restrictions that are strictly enforced, they can be compromised by malicious users. For example, a malicious user could steal sensitive domain administrator credentials from one domain controller, and then use these credentials to attack the domain and forest.

In addition, installed applications and management agents on domain controllers might provide a path for escalating rights that malicious users can use to compromise the management service or administrators of that service. The management tools and services that your organization uses to manage domain controllers and their administrators are equally important to the security of the domain controllers and the domain Administrator accounts. Ensure that these services and administrators are fully secured with equal effort.

Related content

- [Security principals](#)
- [Access control overview](#)

Source: <https://docs.microsoft.com/en-us/windows/security/identity-protection/access-control/active-directory-accounts>