Protected Users Security Group in Windows Server

By robinharwood

Archived: 2026-04-06 01:00:23 UTC

Protected Users is a global security group for Active Directory that's designed to protect against credential theft attacks. The group triggers nonconfigurable protection on devices and host computers to prevent credentials from being cached when group members sign in.

Your system must meet the following prerequisites before you can deploy a Protected Users group:

- Hosts must be running one of the following operating systems:
    - Windows 10 or Windows 11
    - Windows Server 2012 R2 or later with the most recent security updates installed
- The domain functional level must be Windows Server 2012 R2 or later. For more information about functional levels, see Forest and domain functional levels.

Note

The built-in domain Administrator, `S-1-5-<domain>-500`, is always exempt from authentication policies, even when they're assigned to an authentication policy silo. For more information, see How to Configure Protected Accounts.

- Protected Users global security group memberships restrict members to only use Advanced Encryption Standard (AES) for Kerberos. Members of the Protected Users group must be able to authenticate by using AES.

Becoming a member of the Protected Users group means Active Directory automatically applies certain preconfigured controls that the users won't be able to change unless they stop being group members.

When the signed in user is a member of the Protected Users group, the group provides the following protections:

- Credential delegation (CredSSP) doesn't cache the user's plain text credentials even when the user enables the **Allow delegating default credentials** Group Policy setting.
- Windows Digest doesn't cache the user's plaintext credentials even when they've enabled Windows Digest.
- NTLM stops caching the user's plaintext credentials or NT one-way function (NTOWF).
- Kerberos stops creating Data Encryption Standard (DES) or RC4 keys. Kerberos also doesn't cache the user's plaintext credentials, or long-term keys after acquiring the initial Ticket Granting Ticket (TGT).
- The system doesn't create a cached verifier at user sign-in or unlock, so member systems no longer support offline sign-in.

After you add a new user account to the Protected Users group, these protections activate when the new Protected User signs in to their device.

Protected User accounts that authenticate to a domain running Windows Server are unable to do the following:

- Authenticate with NTLM authentication.
- Use DES or RC4 encryption types in Kerberos preauthentication.
- Delegate with unconstrained or constrained delegation.
- Renew Kerberos TGTs beyond their initial four-hour lifetime.

The Protected Users group applies nonconfigurable settings to TGT expiration for every member account. Normally, the domain controller sets the TGT lifetime and renewal based on the following two domain policies:

- Maximum lifetime for user ticket
- Maximum lifetime for user ticket renewal

For Protected Users members, the group automatically sets these lifetime limits to 240 minutes. The user can't change this limit unless they leave the group.

You can add users to the Protected Users group by using the following methods:

- UI tools, such as Active Directory Administrative Center or Active Directory Users and Computers.
- PowerShell, by using the Add-ADGroupMember cmdlet.

Important

- Never add accounts for services and computers to the Protected Users group. For those accounts, membership doesn't provide local protections because the password and certificate is always available on the host.
- Don't add accounts that are already members of highly privileged groups, such as the Enterprise Admins or Domain Admins groups, until you can guarantee that adding them won't have negative consequences. Highly privileged users in Protected Users are subject to the same limitations and restrictions as regular users, and it's not possible to work around or change those settings. If you add all members of those groups to the Protected Users group, it's possible to accidentally lock out their accounts. It's important to test your system to make sure the mandatory setting changes won't interfere with account access for these privileged user groups.

Members of the Protected Users group can only authenticate using Kerberos with AES. This method requires AES keys for the account in Active Directory. The built-in Administrator doesn't have an AES key unless the password for the domain running Windows Server 2008 or later changes. Any account that has its password changed by a domain controller running an earlier version of Windows Server is locked out of authentication.

To avoid lockouts and missing AES keys, we recommend that you follow these guidelines:

- Don't run tests in domains unless all domain controllers run Windows Server 2008 or later.
- If you have migrated accounts from other domains, you need to reset the password so the accounts have AES hashes. Otherwise, these accounts become unable to authenticate.
- Users need to change passwords after switching to a domain functional level of Windows Server 2008 or later. Doing so ensures that they have AES password hashes after they become members of the Protected Users group.

The following table specifies the Active Directory properties of the Protected Users group.

Attribute	**Value**
Well-known SID/RID	S-1-5-21-<domain>-525
Type	Domain Global
Default container	CN=Users, DC=<domain>, DC=
Default members	None
Default member of	None
Protected by AdminSDHolder?	No
Safe to move out of default container?	Yes
Safe to delegate management of this group to non-service admins?	No
Default user rights	No default user rights

Two operational administrative logs are available to help troubleshoot events that are related to Protected Users. These new logs are located in Event Viewer and are disabled by default. They're located under **Applications and Services Logs\Microsoft\Windows\Authentication**.

To enable capturing these logs:

1. Right-click **Start** and then select **Event Viewer**.
2. Open **Applications and Services Logs\Microsoft\Windows\Authentication**.
3. For each log that you want to enable, right-click the log name and then select **Enable Log**.

Event ID and log	**Description**
104 **ProtectedUser-Client**	Reason: The security package on the client doesn't contain the credentials. The error is logged in the client computer when the account is a member of the Protected Users security group. This event indicates that the security

Event ID and log	Description
	package doesn't cache the credentials that are needed to authenticate to the server. Displays the package name, user name, domain name, and server name.
304 **ProtectedUser-Client**	Reason: The security package doesn't store the protected user's credentials. An informational event is logged in the client to indicate that the security package doesn't cache the user's sign-in credentials. It's expected that Digest (WDigest), Credential Delegation (CredSSP), and NTLM fail to have sign-on credentials for Protected Users members. Applications can still succeed if they prompt for credentials. Displays the package name, user name, and domain name.
100 **ProtectedUserFailures-DomainController**	Reason: An NTLM sign-in failure occurs for an account in the Protected Users security group. An error is logged in the domain controller to indicate that NTLM authentication failed because the account was a member of the Protected Users security group. Displays the account name and device name.
104 **ProtectedUserFailures-DomainController**	Reason: DES or RC4 encryption types are used for Kerberos authentication and a sign-in failure occurs for a user in the Protected Users security group. Kerberos preauthentication failed because DES and RC4 encryption types can't be used when the account is a member of the Protected Users security group. (AES is acceptable.)
303 **ProtectedUserSuccesses-DomainController**	Reason: A Kerberos TGT was successfully issued for a member of the Protected Users group.

- Credentials Protection and Management
- Authentication Policies and Authentication Policy Silos
- How to Configure Protected Accounts

Source: https://docs.microsoft.com/en-us/windows-server/security/credentials-protection-and-management/protected-users-security-group