


# Protected Users Security Group

---

 [learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/dn466518\(v=ws.11\)](https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/dn466518(v=ws.11))

- Article
- 08/31/2016

## In this article

---

1. [How the Protected Users group works](#)
2. [Event log information](#)
3. [Deployment requirements](#)
4. [Additional resources](#)

Applies To: Windows 8.1, Windows Server 2012 R2

This topic for the IT professional describes the Active Directory security group Protected Users, and explains how it works. This group was introduced in Windows Server 2012 R2.

Members of this group are afforded additional protections against the compromise of credentials during authentication processes.

This security group is designed as part of a strategy to effectively protect and manage credentials within the enterprise. Members of this group automatically have non-configurable protections applied to their accounts. Membership in the Protected Users group is meant to be restrictive and proactively secure by default. The only method to modify these protections for an account is to remove the account from the security group.

### Warning

Accounts for services and computers should not be members of the Protected Users group. This group provides no local protection because the password or certificate is always available on the host. Authentication will fail with the error “the user name or password is incorrect” for any service or computer that is added to the Protected Users group.

This domain-related, global group triggers non-configurable protection on devices and host computers running Windows Server 2012 R2 and Windows 8.1, and on domain controllers in domains with a primary domain controller running Windows Server 2012 R2. This greatly reduces the memory footprint of credentials when users sign in to computers on the network from a non-compromised computer.

Depending on the account’s domain functional level, members of the Protected Users group are further protected due to behavior changes in the authentication methods that are supported in Windows.

- The member of the Protected Users group cannot authenticate by using NTLM, Digest Authentication, or CredSSP. On a device running Windows 8.1, passwords are not cached, so the device that uses any one of these Security Support Providers (SSPs) will fail to authenticate to a domain when the account is a member of the Protected User group.
- The Kerberos protocol will not use the weaker DES or RC4 encryption types in the pre-authentication process. This means that the domain must be configured to support at least the AES cipher suite.
- The user's account cannot be delegated with Kerberos constrained or unconstrained delegation. This means that former connections to other systems may fail if the user is a member of the Protected Users group.
- The default Kerberos Ticket Granting Tickets (TGTs) lifetime setting of four hours is configurable by using Authentication Policies and Silos, which can be accessed through the Active Directory Administrative Center (ADAC). This means that when four hours has passed, the user must authenticate again.

For more information, see [How the Protected Users group works](#) in this topic.

The following table specifies the 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

Attribute	Value
Default user rights	No default user rights

## How the Protected Users group works

This section explains how the Protected Users group works when:

- Windows 8.1 devices are connecting to Windows Server 2012 R2 hosts.
- The account is located at the Windows Server 2012 R2 domain functional level.

### When Windows 8.1 devices are connecting to Windows Server 2012 R2 hosts

When the Protected Users' group account is upgraded to the Windows Server 2012 R2 domain functional level, domain controller-based protections are automatically applied. Members of the Protected Users group who authenticate to a Windows Server 2012 R2 domain can no longer authenticate by using:

- Default credential delegation (CredSSP). Plain text credentials are not cached even when the **Allow delegating default credentials** Group Policy setting is enabled.
- Windows Digest. Plain text credentials are not cached even when Windows Digest is enabled.
- NTLM. The result of the NT one-way function, NTOWF, is not cached.
- Kerberos long-term keys. The keys from Kerberos initial TGT requests are typically cached so the authentication requests are not interrupted. For accounts in this group, Kerberos protocol verifies authentication at each request..
- Sign-in offline. A cached verifier is not created at sign-in.

Non-configurable settings to the TGTs expiration are established for every account in the Protected Users group. Normally, the domain controller sets the TGTs lifetime and renewal, based on the domain policies, **Maximum lifetime for user ticket** and **Maximum lifetime for user ticket renewal**. For the Protected Users group, 600 minutes is set for these domain policies.

After the user account is added to the Protected Users group, protection is already in place when the user signs in to the domain.

### When domain controllers other than Windows Server 2012 R2 require the Protected Users security group

The Protected Users group can be applied to domain controllers that run an operating system earlier than Windows Server 2012 R2. This allows the added security that is achieved by using the Protected Users group to be applied to all domain controllers. The Protected Users group can be created by [HYPERLINK](#)

"[https://technet.microsoft.com/library/cc816944\(v=ws.10\).aspx](https://technet.microsoft.com/library/cc816944(v=ws.10).aspx)" transferring the primary domain controller (PDC) emulator role to a domain controller that runs Windows Server 2012 R2. After that group object is replicated to other domain controllers, the PDC emulator role can be hosted on a domain controller that runs an earlier version of Windows Server.

For more information, see [How to Configure Protected Accounts](#).

## Built in restrictions of the Protected Users security group

Accounts that are members of the Protected Users group that authenticate to a Windows Server 2012 R2 domain are unable to:

- Authenticate with NTLM authentication.
- Use DES or RC4 encryption types in Kerberos pre-authentication.
- Be delegated with unconstrained or constrained delegation.
- Renew the Kerberos TGTs beyond the initial four-hour lifetime.

## Warning

Accounts for services and computers should not be members of the Protected Users group. This group provides no local protection because the password or certificate is always available on the host.

## Event log information

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, and are located under **Applications and Services Logs\Microsoft\Windows\Microsoft\Authentication**.

Event ID and Log	Description
------------------	-------------

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

## Deployment requirements

---

Requirements to provide client-side protection for members of the Protected Users group include:

- The Protected Users global security group is replicated to all domain controllers in the account domain.
- Devices and hosts are running Windows 8.1 or Windows Server 2012 R2.

Requirements to provide domain controller protection for members of the Protected Users group include:

The domain functional level in the account domains is set to Windows Server 2012 R2.

To enable Windows Server 2012 R2 and Windows 8.1 protection for clients on domains with pre-Windows Server 2012 R2 domain functional levels, after the Protected Users group has replicated throughout the domain, a user signs in with an account that is a member of a Protected Users group.

## Additional resources

---

- [Credentials Protection and Management](#)
- [Authentication Policies and Authentication Policy Silos](#)
- [How to Configure Protected Accounts](#)