Store passwords using reversible encryption - Windows 10

By vinaypamnani-msft

Archived: 2026-04-05 12:37:40 UTC

▶
▶

Applies to

- Windows 11
- Windows 10

Describes the best practices, location, values, and security considerations for the **Store passwords using reversible encryption** security policy setting.

Reference

The **Store password using reversible encryption** policy setting provides support for applications that use protocols that require the user's password for authentication. Storing encrypted passwords in a way that is reversible means that the encrypted passwords can be decrypted. A knowledgeable attacker who is able to break this encryption can then sign in to network resources by using the compromised account. For this reason, never enable **Store password using reversible encryption** for all users in the domain unless application requirements outweigh the need to protect password information.

If you use the Challenge Handshake Authentication Protocol (CHAP) through remote access or Internet Authentication Services (IAS), you must enable this policy setting. CHAP is an authentication protocol that is used by remote access and network connections. Digest Authentication in Internet Information Services (IIS) also requires that you enable this policy setting.

Possible values

- Enabled
- Disabled
- Not defined

Best practices

Set the value for **Store password using reversible encryption** to Disabled. If you use CHAP through remote access or IAS, or Digest Authentication in IIS, you must set this value to **Enabled**. This setting presents a security risk when you apply the setting by using Group Policy on a user-by-user basis because it requires opening the appropriate user account object in Active Directory Users and Computers.

> **Note:** Do not enable this policy setting unless business requirements outweigh the need to protect password information.

Location

Computer Configuration\Windows Settings\Security Settings\Account Policies\Password Policy

Default values

The following table lists the actual and effective default policy values. Default values are also listed on the policy's property page.

Server type or Group Policy Object (GPO)	Default value
Default domain policy	Disabled
Default domain controller policy	Disabled
Stand-alone server default settings	Disabled
Domain controller effective default settings	Disabled
Member server effective default settings	Disabled
Effective GPO default settings on client computers	Disabled

Security considerations

This section describes how an attacker might exploit a feature or its configuration, how to implement the countermeasure, and the possible negative consequences of countermeasure implementation.

Vulnerability

Enabling this policy setting allows the operating system to store passwords in a format that can weaken your overall security.

Countermeasure

Disable the **Store password using reversible encryption** policy setting.

Note

When policy settings are disabled, only new passwords will be stored using one-way encryption by default. Existing passwords will be stored using reversible encryption until they are changed.

Potential impact

If your organization uses CHAP through remote access or IAS, or Digest Authentication in IIS, you must configure this policy setting to Enabled. This setting presents a security risk when you apply the setting through Group Policy on a user-by-user basis because it requires the appropriate user account object to be opened in Active Directory Users and Computers.

- Password Policy
