Turn on automatic logon in Windows

- 01/15/2025

This article describes how to configure Windows to automate the logon process by storing your password and other pertinent information in the registry database. By using this feature, other users can start your computer and use the account that you establish to automatically log on.

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows 10, Windows 11
Original KB number: 324737

Important

The autologon feature is provided as a convenience. However, this feature may be a security risk. If you set a computer for autologon, anyone who can physically obtain access to the computer can gain access to all the computer's contents, including any networks it is connected to. Additionally, when autologon is turned on, the password is stored in the registry in plain text. The specific registry key that stores this value can be remotely read by the Authenticated Users group. This setting is recommended only for cases in which the computer is physically secured and steps have been taken to make sure that untrusted users cannot remotely access the registry.

Use Registry Editor to turn on automatic logon

Important

This section, method, or task contains steps that tell you how to modify the registry. However, serious problems might occur if you modify the registry incorrectly. Therefore, make sure that you follow these steps carefully. For added protection, back up the registry before you modify it. Then, you can restore the registry if a problem occurs. For more information about how to back up and restore the registry, see **How to back up and restore the registry in Windows**.

To use Registry Editor to turn on automatic logon, follow these steps:

1. Select **Start**, and then select **Run**.
2. In the **Open** box, type *Regedit.exe*, and then press `Enter`.

3. Locate the `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon` subkey in the registry.
4. On the **Edit** menu, select **New**, and then point to **String Value**.
5. Type *AutoAdminLogon*, and then press `Enter`.
6. Double-click **AutoAdminLogon**.
7. In the **Edit String** dialog box, type **1** and then select **OK**.
8. Double-click the **DefaultUserName** entry, type your user name, and then select **OK**.
9. Double-click the **DefaultPassword** entry, type your password, and then select **OK**.

   If the **DefaultPassword** value doesn't exist, it must be added. To add the value, follow these steps:

   a. On the **Edit** menu, select **New**, and then point to **String Value**.
   b. Type *DefaultPassword*, and then press `Enter`.
   c. Double-click **DefaultPassword**.
   d. In the **Edit String** dialog, type your password and then select **OK**.

   > **Note**
   >
   > If no DefaultPassword string is specified, Windows automatically changes the value of the `AutoAdminLogon` key from **1** (true) to **0** (false), disabling the AutoAdminLogon feature.

10. If you have joined the computer to a domain, you should add the **DefaultDomainName** value, and the data for the value should be set as the fully qualified domain name (FQDN) of the domain, for example `contoso.com.`.
11. Exit Registry Editor.
12. Select **Start**, select **Shutdown**, and then type a reason in the **Comment** text box.
13. Select **OK** to turn off your computer.
14. Restart your computer. You can now log on automatically.

Use Sysinternals tool Autologon to configure AutoAdminLogon

For download and usage details, see Autologon - Sysinternals. After AutoAdminLogon is configured by using the tool, the password will be stored in a Local Security Authority (LSA) secret instead of the Winlogon key.

Note

- To bypass the AutoAdminLogon process and to log on as a different user, press and hold the Shift key after you log off or after Windows restarts.
- This registry change does not work if the Logon Banner value is defined on the server either by a Group Policy object (GPO) or by a local policy. When the policy is changed so that it does not affect the computer, the autologon feature works as expected.
- When Exchange Active Sync (EAS) password restrictions are active, the autologon feature does not work. This behavior is by design. This behavior is caused by a change in Windows 8.1 and does not affect Windows 8 or earlier versions. To work around this behavior in Windows 8.1 and later versions, remove the EAS policies in Control Panel.
- An interactive console logon that has a different user on the server changes the **DefaultUserName** registry entry as the last logged-on user indicator. AutoAdminLogon relies on the **DefaultUserName** entry to match the user and password. Therefore, AutoAdminLogon may fail. You can configure a shutdown script to set the correct **DefaultUserName**.

AutoAdminLogon and Active Directory domains

When a computer starts up, it may take some time until a network connection is established because of the following reasons:

- Configuration of a dynamics IP address through the Dynamic Host Configuration Protocol (DHCP) configuration may necessitate the use of DHCP relays.
- Requirement to authenticate to a wireless network access point.
- Requirement to authenticate to wired network authentication services.
- Other network services are required to establish a connection between the client network and a network with domain controllers.

The group policy (Always wait for the network at computer startup and logon) can help ensure the computer as a domain member waits for a domain network to become available. For more information, see the following articles:

- Logon Optimization
- Always wait for the network at computer startup and logon

The group policy can be used to delay the logon attempt until the group policy processing on boot is completed. It also ensures a network with domain controllers is available.