Password must meet complexity requirements - Windows 10

By vinaypamnani-msft

Archived: 2026-04-05 21:59:38 UTC

Applies to

- Windows 11
- Windows 10

Describes the best practices, location, values, and security considerations for the **Password must meet complexity requirements** security policy setting.

The **Passwords must meet complexity requirements** policy setting determines whether passwords must meet a series of strong-password guidelines. When enabled, this setting requires passwords to meet the following requirements:

1. Passwords may not contain the user's samAccountName (Account Name) value or entire displayName (Full Name value). Neither of these checks is case-sensitive.

   The samAccountName is checked in its entirety only to determine whether it's part of the password. If the samAccountName is fewer than three characters long, this check is skipped. The displayName is parsed for delimiters: commas, periods, dashes or hyphens, underscores, spaces, pound signs, and tabs. If any of these delimiters are found, the displayName is split and all parsed sections (tokens) are confirmed not to be included in the password. Tokens that are shorter than three characters are ignored, and substrings of the tokens aren't checked. For example, the name "Erin M. Hagens" is split into three tokens: "Erin", "M", and "Hagens". Because the second token is only one character long, it's ignored. So, this user couldn't have a password that included either "erin" or "hagens" as a substring anywhere in the password.

2. The password contains characters from three of the following categories:

   - Uppercase letters of European languages (A through Z, with diacritic marks, Greek and Cyrillic characters).
   - Lowercase letters of European languages (a through z, sharp-s, with diacritic marks, Greek and Cyrillic characters).
   - Base 10 digits (0 through 9).
   - Non-alphanumeric characters (special characters):

     ```
     '-!"#$%&()*,./:;?@[]^_`{|}~+<=>
     ```

Currency symbols such as the Euro or British Pound aren't counted as special characters for this policy setting.

- Any Unicode character that's categorized as an alphabetic character but isn't uppercase or lowercase. This group includes Unicode characters from Asian languages.

Complexity requirements are enforced when passwords are changed or created.

The rules that are included in the Windows Server password complexity requirements are part of `Passfilt.dll`, and they can't be directly modified.

When enabled, the default Passfilt.dll may cause some more Help Desk calls for locked-out accounts, because users are used to passwords that contain only characters that are in the alphabet. But this policy setting is liberal enough that all users should get used to it.

Other settings that can be included in a custom `Passfilt.dll` are the use of non-upper-row characters. To type upper-row characters, you hold the SHIFT key and press one of any of the keys on the number row of the keyboard (from 1 through 9 and 0).

- Enabled
- Disabled
- Not defined

Set **Passwords must meet complexity requirements** to Enabled. This policy setting, combined with a minimum password length of 8, ensures that there are at least 159,238,157,238,528 different possibilities for a single password. This setting makes a brute force attack difficult, but still not impossible.

The use of ALT key character combinations may greatly enhance the complexity of a password. However, requiring all users in an organization to adhere to such stringent password requirements might result in unhappy users and an over-worked Help Desk. Consider implementing a requirement in your organization to use ALT characters in the range from 0128 through 0159 as part of all administrator passwords. (ALT characters outside of that range can represent standard alphanumeric characters that don't add more complexity to the password.)

Short passwords that contain only alphanumeric characters are easy to compromise by using publicly available tools. To prevent this vulnerability, passwords should contain other characters and/or meet complexity requirements.

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

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	Enabled
Default domain controller policy	Enabled

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

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.

Passwords that contain only alphanumeric characters are easy to discover with several publicly available tools.

Configure the **Passwords must meet complexity requirements** policy setting to *Enabled* and advise users to use various characters in their passwords.

When combined with a Minimum password length of 8, this policy setting ensures that the number of different possibilities for a single password is so great that it's difficult (but possible) for a brute force attack to succeed. (If the Minimum password length policy setting is increased, the average amount of time necessary for a successful attack also increases.)

If the default configuration for password complexity is kept, more Help Desk calls for locked-out accounts could occur because users might not be used to passwords that contain non-alphabetical characters, or they might have problems entering passwords that contain accented characters or symbols on keyboards with different layouts. However, all users should be able to follow the complexity requirement with minimal difficulty.

If your organization has more stringent security requirements, you can create a custom version of the `Passfilt.dll` file that allows the use of arbitrarily complex password strength rules. For example, a custom password filter might require the use of non-upper-row symbols. (Upper-row symbols are those symbols that require you to press and hold the SHIFT key and then press any of the keys on the number row of the keyboard, from 1 through 9 and 0.) A custom password filter might also perform a dictionary check to verify that the proposed password doesn't contain common dictionary words or fragments.

The use of ALT key character combinations may greatly enhance the complexity of a password. However, such stringent password requirements might result in more Help Desk requests. Alternatively, your organization could consider a requirement for all administrator passwords to use ALT characters in the 0128-0159 range. (ALT characters outside of this range can represent standard alphanumeric characters that wouldn't add more complexity to the password.)

- Password Policy
