**Microsoft Tip: Best Practices for Enforcing Password Policies**

No matter how secure you make a user’s password initially, she will eventually choose her own password. Therefore, you should set account policies that define a secure password for your systems. Account policies are a subset of the policies configurable in Group Policy. Here’s a look at the key settings you will work with.

**Enforce Password History**
This sets how frequently old passwords can be reused. With this policy, you can discourage users from alternating between several common passwords. Windows Server 2008 R2 can store up to 24 passwords for each user in the password history. To disable this feature, set the value of the password history to 0. To enable this feature, set the value of the password history using the Passwords Remembered field. Windows Server 2008 R2 then tracks old passwords using a password history that’s unique for each user, and users aren’t allowed to reuse any of the stored passwords.

*Note:* To prevent users from working around the Enforce Password History settings, you should prevent users from changing passwords immediately. This stops users from changing their passwords several times to wipe the history and get back to the old password. You can set the time required to keep a password with the Minimum Password Age policy.

**Maximum Password Age**
This determines how long users can keep a password before they have to change it. The aim is to force users to change their passwords periodically. Generally, you use a shorter period when security is very important and a longer period when security is less important. You can set the maximum password age to any value from 0 to 999, where a value of 0 specifies that passwords don’t expire. Although you might be tempted to set no expiration date, users should change passwords regularly to ensure the network’s security. Where security is a concern, good values are 30, 60, or 90 days. Where security is less important, good values are 120, 150, or 180 days.

*Note:* Windows Server 2008 R2 notifies users when the password expiration date is approaching. Any time the expiration date is less than 30 days away, users see a warning when they log on that they have to change their password within a specific number of days.

**Minimum Password Age**
This determines how long users must keep a password before they can change it. You can use this field to prevent users from bypassing the password system by entering a new password and then changing it right back to the old one. If the minimum password age is set to 0, users can change their passwords immediately. To prevent this, set a specific minimum age. Reasonable settings are from three to seven days. In this way you make sure that users are less inclined to switch back to an old password but are able to change their passwords in a reasonable amount of time if they want to.

*Note:* Keep in mind that a minimum password age could prevent a user from changing a compromised password. If a user can’t change the password, an administrator has to make the change.

**Minimum Password Length**
This sets the minimum number of characters for a password. If you haven’t changed the default setting, you should do so immediately. The default in some cases is to allow empty passwords (passwords with zero characters), which is definitely not a good idea. For security reasons you’ll generally want passwords of at least eight characters because long passwords are usually harder to crack than short ones. If you want greater security, set the minimum password length to 14 characters.

**Passwords Must Meet Complexity Requirements**
Beyond the basic password and account policies, Windows Server 2008 R2 includes facilities for creating additional password controls. These facilities enforce the use of secure passwords that follow these guidelines:

* Passwords must have at least six characters.
* Passwords can’t contain the user name or parts of the user’s full name, such as his first name.
* Passwords must use at least three of the four available character types: lowercase letters, uppercase letters, numbers, and symbols.

To enforce these rules, enable the Passwords Must Meet Complexity Requirements policy.

**Store Password Using Reversible Encryption For All Users**
Passwords in the password database are encrypted. This encryption can’t normally be reversed. The only time you would want to change this setting is when your organization uses applications that need to read the password. If this is the case, enable Store Password Using Reversible Encryption For All Users. But with this policy enabled, passwords might as well be stored as plain text—it presents the same security risks. With this in mind, a much better technique is to enable the option on a per-user basis and then only as required to meet the user’s actual needs.

From the Microsoft Press book [*Windows Server 2008 Administrator’s Pocket Consultant, Second Edition*](https://www.microsoft.com/learning/en/us/Book.aspx?ID=13931) by William R. Stanek.

<https://technet.microsoft.com/en-us/library/ff741764.aspx>

For more tips on Microsoft products and technologies, visit the [TechNet Tips library](https://technet.microsoft.com/en-us/magazine/dd310316.aspx).