

# Help users create complex passwords that are easy to remember

**Date:** January 16th, 2008

**Author:** Mike Mullins

**Category:** Passwords, Risk Management, Security Solutions

**Tags:** Mike Mullins

While most end users understand the importance of using passwords to secure corporate systems and data, they don't always know how to create a strong password. That's why it's just as important to create a strong password policy in your organization. Remember: Passwords are only as good as the policy that enforces their use.

By default, Windows disables the password filter in the Default Domain Group Policy Object (GPO) and in the local security policy of workstations and servers. That's one more reason why it's imperative that organizations employ a written password policy — and that they take steps to enforce it.

For example, if your company's password policy only requires a minimum of six characters and doesn't require complexity (i.e., a combination of uppercase and lowercase characters, digits, and/or nonalphanumeric characters), then you've got a pretty weak policy. That means most users will use passwords that are easy to crack through either brute force or social engineering.

How do you make sure your users create strong passwords that hackers can't easily guess? Your first step is to enable the password filter in the GPO or on local stand-alone workstations and servers. To find the password filter, go to Computer Configuration\Windows Settings\Security Settings\Account Policies>Password Policy in the Group Policy MMC in the Default Domain policy. After enabling the password filter, you can start creating an effective password policy for your users.

## Craft a strong password policy

Let's look at some best practices for effective password policies. Most organizations require users' passwords to have a minimum of eight characters. They also specify that passwords must meet at least three of the four complexity requirements — uppercase letters, lowercase letters, numbers, and nonalphanumeric characters.

Organizations should also configure the password history to remember the last 24 passwords, which is the maximum setting. This virtually ensures that users won't reuse passwords.

In addition, you should set the minimum and maximum age of the password to an appropriate level. I recommend setting a maximum age of 180 days and a minimum age of 90 days. This prevent users from cycling through passwords until they can return to the one they want.

## Put your policy in action — and enforce it

It's smart to establish a good password policy in your organization, but it's even more important to actually enforce it. A strong policy that no one has to follow doesn't add any more security than no policy at all.

In addition, it's important to remember that a good password policy doesn't work if users have to write down their password because it's so complex. That only transfers the security risk instead of mitigating it.

So how can you make sure users' passwords are complicated enough to deter hackers and easier enough to remember? One of my colleagues offers the following trick for creating complex passwords that meet complexity requirements while still being possible to remember.

### **Step 1: Come up with a base word**

Pick the name of a pet or any common thing that's easy to remember. For example, say you once lived in Louisville. You can use that to establish the base of your password and satisfy the required criteria for a strong password.

Remember: You need at least one capital letter and either a number or special character. So, using Louisville as your base word, you can substitute an *!* or *1* for *i* and replace the *s* with *\$* — e.g., Lou1\$ville or LOu!\$ville.

### **Step 2: Add more characters to the base word**

Pick any four characters to add to the base word.

### **Step 3: Store your password without worry**

Now, write down the added four characters, along with a clue for the base word. Using our previous example, you would write down *city1xyza*, where *city1* signifies *Louisville* with a 1 and \$ and *xyza* represents the four additional characters.

So, even written down, this password reference would serve as a reminder of your complete password while revealing nothing to any roaming eyes. (Keep in mind that this example is a 14-character password. While that may be longer than the actual requirement, it may be easier to remember.)

## **Final thoughts**

Password policies only work if you turn them on. Make sure you've trained your users on how to create complex passwords that they can remember without leaving a paper trail that prying eyes can easily follow.

*Worried about security issues? Who isn't? Automatically sign up for our free Security Solutions newsletter, delivered each Friday, and get hands-on advice for locking down your systems*

## **People who read this, also read...**

The truth about email spam

The three most important security steps the small business should take

Retrospective: 10 security blunders

How to spoof a MAC address

Sanity check: Eight trends that will rock technology in 2008

## **Print/View all Posts**

### **Comments on this blog**

### **Trackbacks**

The URI to TrackBack this entry is: *<http://blogs.techrepublic.com.com/security/wp-trackback.php?p=392>*

No trackbacks yet.

Copyright © 2008 CNET Networks, Inc. All Rights Reserved.