Top 10 Password Policies and Best Practices for System Administrators

Devolutions

SYSTEM ADMINISTRATORS PLAY A MAJOR ROLE IN MAKING SURE THAT EACH USER IS WELL AWARE OF THE SECURITY RISKS THEY FACE EVERY DAY.

We all know that a strong password policy is the front line of defense to protect our financial transactions, personal communications and private information stored online. For end-users, using a strong password at work is as important as it is at home, it is your own personal bodyguard defending you with everything he has against serious security threats, scammers and hackers. That's when the system administrator comes in to makes sure that proper rules and policies are in place to help you alleviate that burden.

Most users understand the nature of security risks related to easy-to-guess passwords, but become frustrated when dealing with unfamiliar criteria or trying to remember 30 different passwords for their multiple accounts. That is why system administrators now play a major role in making sure that each user is well aware of the security risks they face every day. To achieve that, they need strong password policies and best practices.

Password policies are a set of rules which were created to increase computer security by encouraging users to create reliable, secure passwords and then store and utilize them properly.

Here are some of the password policies and best practices that every system administrator should implement:

1. ENFORCE PASSWORD HISTORY POLICY

The Enforce Password History policy **will set how often an old password can be reused**. It should be implemented with a minimum of 10 previous passwords remembered. This policy will discourage users from reusing a previous password, thus preventing them from alternating between several common passwords. Some tech-savvy users might try to work around the Enforce Password History policy, to prevent that from happening use the Minimum Password Age policy.

2. MINIMUM PASSWORD AGE POLICY

This policy determines **how long users must keep a password before they can change it**. The Minimum Password Age will prevent a user from dodging the password system by using a new password and then changing it back to their old one. To prevent this, the specific minimum age should be set fromthree to seven days, making sure that users are less prone to switch back to an old paword, but are still able to change it in a reasonable amount of time. As a system administrator you must keep in mind that **this policy could also prevent a user from immediately changing a compromised password**, so if the user can't change it, it will be up to you to make the change.

3. MAXIMUM PASSWORD AGE POLICY

The Maximum Password Age policy **determines how long users can keep a password before they are required to change it**. This policy forces the user to change their passwords regularly. To ensure a network's security you should set the value to 90 days for passwords and 180 days for passphrases.

4. MINIMUM PASSWORD LENGTH POLICY

This policy determines the minimum number of characters needed to create a password. You would generally want to **set the Minimum Password Length to at least eight characters since long passwords are harder to crack than short ones**. For even greater security, you could set the minimum password length to 14 characters. A word of advice: if you haven't changed the default setting, you should change it immediately since sometimes the default is set to zero characters, meaning that it allows empty passwords.

5. PASSWORDS MUST MEET COMPLEXITY REQUIREMENTS POLICY

By enabling the Passwords Must Meet Complexity Requirements policy, you'll go beyond the basic password and account policies and ensure that every password is secured following these guidelines:

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

6. RESET PASSWORD

The local **administrator password should be reset every 180 days for greater security** and the service account password should be reset at least once a year during maintenance time.

7. USE STRONG PASSPHRASES

Strong passphrases with a minimum of 15 characters should always be used to protect domain administrator accounts. While passwords and passphrases serve the same purpose, passwords are usually short, hard to remember and easy to crack, while passphrases are easier to remember and type but much harder to crack due to length.

8. PASSWORD AUDIT POLICY

Enabling the Password Audit policy **allows you to track all password changes**. By monitoring the modifications that are made it is easier to track potential security problems. This helps to ensure user accountability and provides evidence in the event of a security breach.

9. E-MAIL NOTIFICATIONS

Create **e-mail notifications prior to password expiry to remind your users when it's time to change their passwords** before they actually expire.

10. STORE PASSWORD USING REVERSIBLE ENCRYPTION FOR ALL USERS POLICY

I'll start by saying that **this policy should only be enabled on a per-user basis and then only to meet the user's actual needs**. As you all know, passwords in the password database are all encrypted and this encryption can't normally be reversed. If your company uses an application that needs to read a password, then that is the only time you would want to enable this setting. Keep in mind that when enabling the Store Password Using Reversible Encryption for All Users policy, it's like your passwords are stored as plain text, representing the same security risks. Always be cautious when enabling that policy.

Conclusion

We can't emphasize enough the importance of educating your users on how to manage their strong passwords. Passwords are only one piece of the security puzzle. To keep your user accounts safe, it takes both an exhaustive process for a strong password and an easy to use password management solution, like Devolutions Server, to store and safeguard all those passwords. Never forget that a chain is only as strong as its weakest link.