Set up a secure password system

Most users who log on to their local PC or remote computers often use a combination of username and a password entered from the keyboard. So finding a good password and imposing a measure

Introduce

Most users who log on to their local PC or remote computers often use a combination of username and a password entered from the keyboard. Although there are many other techniques for authentication, such as smart cards, biometrics, or login password of operating systems, most organizations still depend on traditional passwords and still will continue in the coming years. So finding a good password and imposing a password on computers is an important and necessary issue for organizations. A good password must be a password with a certain amount of complexity - including length and type of characters - to make passwords more difficult to guess than password criminals. Setting up a good password policy for your organization can help prevent an attacker from playing the role of a legitimate user and thereby prevent data loss, sensitive information disclosure. In this article we will explain how to implement a password policy on computers running Microsoft Windows 2000, Windows XP, and Windows Server 2003 operating systems.

Depending on whether the computer in the organization is a member of the Active Directory, standalone computer, or both cases to enforce good password policies, you must perform one or two tasks below:

1. Configure password policy settings in Active Directory Domain.
2. Configure settings on stand-alone computers.

Once you have configured the appropriate password settings, the users in your organization will be able to create new passwords that meet length and complexity and users will not be able to immediately change their new passwords.

Note : All specific step-by-step instructions in this document have been developed using the default Start menu when installing the operating system. If you have changed the Start menu, the steps may be slightly different.

Before start

Before you can configure password settings on a network computer, you need to see what settings are involved, specify the values ??to use for these settings, and understand Windows to store password configuration settings. where.

Note : Windows 95, Windows 98, and Windows Millennium Edition operating systems do not support advanced security features such as password settings. If your network consists of stand-alone computers (computers not related to a domain) running these operating systems, you won't be able to set this password function on them. If the network of computers running this operating system is a member of the Active Directory directory service domain, you can enforce password settings at the domain level.

Identify settings related to passwords

For Windows 2000, Windows XP, and Windows Server 2003, there are five settings that you have to configure regarding password properties: **Enforce password history** , **Maximum password age** , **Minimum password age** , **Minimum password length** , and **Must meet complexity. requirements** .

1. **Enforce password history** indicates the number of new passwords a user must use before an old password is reused. The value of this setting can be between 0 and 24; If this value is set to 0, enforce password history is disabled. For most organizations usually set this value to 24.

2. **Maximum password age** indicates how many days a password can be used before a user is asked to change it. This value is between 0 and 99; if it is set to 0, passwords will never expire. Setting this value too low can cause a loss of effectiveness for users; otherwise this value is too high or disabling them, it will allow attackers to have more time to identify the passwords. For most organizations, this value is set to 42 days.
3. **Minimum password age** indicates how many days a user must keep new passwords before they can change them. This setting is designed to work with the **Enforce password history setting** so that users cannot quickly reset their passwords and then change their old passwords again. The value of this setting can be from 0 to 999; If it is set to 0, the user can immediately change the new password. We recommend setting this value to 2 days.
4. **Minimum password length** indicates how the minimum length of passwords is. Although Windows 2000, Windows XP and Windows Server 2003 support passwords with up to 28 characters, the value of this setting is only between 0 and 4 characters. If set to 0, the user is allowed to have blank passwords, so you should not use the value 0. In this case we recommend using 8 characters.
5. **Passwords must meet complexity requirements** (**complexity requirements**) show how complex the passwords are required. If this setting is enabled then the user password should follow the requirements below.
    1. Password must be at least 6 characters long
    2. The password consists of at least three characters in the following five categories:
        1. Uppercase characters in the alphabet (AZ)
        2. Lowercase letters in the alphabet (az)
        3. 10 basic digits (0 - 9)
        4. Special characters (eg:!, $, #, Or%)
        5. Unicode characters
    3. Passwords are no more than three characters in the user account name.

       If the account name is less than three characters, this test will not be performed because the speed of these passwords will be removed too high. When checking looks at a number of characters as separators to separate names into separate sections: commas, dots, dashes / hyphens, underlines, 'space' keys, pound symbols and tab keys. When those parts are longer than 3 characters, they are searched in the password; If it appears, the password will be disqualified. For example, the name "Erin M. Hagens" will be divided into three parts: "Erin", "M" and "Hagens". Because the second part has one character, it is ignored. So this user cannot have a password including "erin" or "hagens" as a substring anywhere in the password. All these tests are very sensitive.

       Complex requirements are required for password changes or new creation. We recommend enabling this setting.

Find out how the Windows operating system stores password configuration information

Before you implement the organization's password policies, you should learn a little about how the password configuration information is stored in Windows 2000, Windows XP and Windows Server 2003. This is necessary because Because password storage techniques limit the number of different password policies you can implement and influence.

They can be a simple policy for each account database. An Active Directory domain is treated as a single account database, as a stand-alone local account database in the computer. Computers that are members of this domain also have a local account database, but most organizations that have deployed Active Directory domains

require users to log on to their computers and the network using use domain-based accounts. So if you specify a minimum password length of 14 characters for the domain, all domain users must use a password that has more than 14 characters. To set up other requests for a specific number of users you must create a new domain for their accounts.

Active Directory domains use Group Policy objects (GPOs) to store a variety of configuration information including password policy settings. Although Active Directory is a hierarchical directory service, they support multiple classes of 'organizational units' (OUs) and multiple GPOs, so the password policy settings for the domain must be defined in a significant way. Original 'container' for domain. When the first domain controller created for a new Active Directory domain will have two GPOs created automatically: the default domain policy GPO and the default domain controller GPO policy. The default domain policy is linked to the original 'container'. It includes several important domain-wide settings including default password policy settings. The default domain control policy is linked to domain controllers OU and includes initial security settings for domain controllers.

A best practice solution to avoid changing the GPOs attached. If you need to apply password policy settings that are dispersed into default settings, you should create a new GPO and link it to the original 'container' or to the OU domain controller and assign it at the preferred level. Advanced is higher than the attached GPO: if there are two GPOs that conflict with the settings linked to the original 'container', the high priority GPO will take precedence.

See section II: Step by step implementation of password policy settings