LESSON 3 : Understanding Security Policies

OBJECTIVE DOMAIN MATRIX

SKILLS/CONCEPTS	MTA EXAM OBJECTIVE	MTA EXAM OBJECTIVE NUMBER
Using Password Policies to Enhance Security	Understand password policies.	2.3

KEY TERMS

account lockout

cracked password

dictionary attack

Group Policy Object (GPO)

keylogger

password

sniffers

strong password

One of the foundations of information security is the protection of networks, systems, and most important of all, data. In fact, the need to protect data is basic to all information security policies, procedures, and processes.

Much of today's data protection is based on the ***password***. Think about your life. You use passwords to secure your voice mail, your ATM access, your email account, your Facebook account, and a host of other things. In order to keep these accounts secure, you need to select strong passwords. In this lesson, we discuss what goes into creating a strong password, as well as how you can configure password settings to ensure that the passwords in your environment stay secure.

Using Password Policies to Enhance Security

> **THE BOTTOM LINE**
> There are a variety of configuration settings you can use on your system to ensure that your users are required to set and maintain strong passwords. As hard as it may be to believe, when left to their own devices, many users will still select weak passwords when securing their accounts. However, with user education and system controls, you can reduce the risk of weak passwords compromising your data and applications.

One basic component of your information security program is ensuring that all employees select and use ***strong passwords***. The strength of a password can be determined by looking at the password's length, complexity, and randomness.

Microsoft provides a number of controls that can be used to ensure password security is maintained. These include controls related to:

CERTIFICATION READY
How do you enforce stronger passwords for your organization?
2.3

- Password complexity
- Account lockout
- Password length
- Password history
- Time between password changes
- Enforcement using group policies
- Common attack methods

Using Password Complexity to Make a Stronger Password

Password complexity involves the characters used to make up a password. A complex password uses characters from at least three of the following categories:

- English uppercase characters (A through Z)
- English lowercase characters (a through z)
- Numeric characters (0 through 9)
- Nonalphanumeric characters (!, @, #, $, %, ^, &, etc.)

Microsoft's password complexity settings, when enabled, require characters from three of these categories by default on domain controllers, and the domain can be configured to require this setting for all passwords.

This setting can either be enabled or disabled. There are no additional configurations available.

Of course, even when you enforce password complexity, there is no guarantee that users will not continue to use easily guessable passwords. For example, the password "Summer2010" meets the current complexity guidelines required by the Windows password complexity setting. It's also a terrible password, because it is easily guessable.

Some password selections that should be avoided include words you would find in a dictionary, derivatives of user IDs, and common character sequences such as "123456" or "QWERTY." Likewise, personal details such as spouse's name, license plate number, Social Security number, or date of birth should be avoided. Finally, you should avoid passwords based on proper names, geographical locations, common acronyms, and slang terms.

Some recommended methods for selecting strong passwords include the following:

- **Bump the characters in a word a certain number of letters up or down the alphabet:** For instance, a three-letter shift translation of “AArdvark!!” would yield the password “44DDvhzdvo!!”
- **Create acronyms from words in a song, poem, or other familiar sequence of words:** For example, the phrase “Ask not what you can do for your country?” could yield the password “Anwycdfyc?” Add $$ to the beginning, and you get the strong password $$Anwycdfyc?
- **Combine a number of personal facts like birth dates and favorite colors, foods, etc. with special characters:** This method would yield passwords like “##Yell0w419” or “$^327p!zZ@.”

TAKE NOTE*
One of the easiest ways to set a complex password is to start with a dictionary word and use character substitution to make it complex.
For example, computer could be changed to C0mput3r.

Using Account Lockout to Prevent Hacking

Account lockout refers to the number of incorrect logon attempts permitted before a system locks an account. Each bad logon attempt is tracked by the bad logon counter, and when the counter exceeds the account lockout threshold, no further logon attempts are permitted. This setting is critical because one of the most common password attacks (discussed later in the lesson) involves repeatedly attempting to log on with guessed passwords.

Microsoft provides three separate settings with respect to account lockout:

- **Account lockout duration:** This setting determines the length of time a lockout will remain in place before another logon attempt can be made. This can be set from 0 to 99,999 minutes. If set to 0, an administrator will need to manually unlock the account; no automatic unlocking will occur.
- **Account lockout threshold:** This setting determines the number of failed logons permitted before account lockout occurs. This can be set from 0 (no account lockouts) to 999 attempts before lockout.
- **Reset account lockout counter after:** This setting determines the period of time, in minutes, that must elapse before the account lockout counter is reset to 0 bad logon attempts. If an account lockout threshold is set, the reset account lockout threshold must be less than or equal to the account lockout duration.

Usually account lockout settings range from three to ten attempts, with account lockout duration and reset account lockout counter after set anywhere from 30 to 60 minutes. Although some users complain when they don't get as many attempts to log in as they need, this is a critical configuration to set to ensure your environment remains secure.

Looking at Password Length

The length of a password is a key component of its strength. Password length is the number of characters used in a password. A password with two characters is considered highly insecure, because there is a very limited set of unique passwords that can be made using two characters. Therefore, a two-character password is considered easy to guess.

On the other side of the spectrum is the 14-character password. Although extremely secure relative to a two-character password, a 14-character password is difficult for most users to remember. When passwords become this long, users often start breaking out the note paper and writing their passwords down, which defeats any security benefits you may have gotten from requiring a 14-character password in the first place.

As these scenarios illustrate, the trick to setting a minimum password length is balancing usability with security. Microsoft permits you to set a minimum password length ranging from one to 14 (a setting of 0 means no password is required, which is never appropriate in a production environment). The generally accepted minimum password length is eight characters.

Using Password History to Enforce Security

Password history is the setting that determines the number of unique passwords that must be used before a password can be re-used. This setting prevents users from recycling the same passwords through a system. The longer the period of time a password is used, the greater the chances it can be compromised.

Microsoft allows you to set the password history value between 0 and 24. Ten is a fairly common setting in standard environments, although Windows Server 2008 defaults to 24 on domain controllers.

Setting the Time between Password Changes

The final password setting you should be familiar with is the time between password changes. This setting actually consists of two settings:

- **Minimum Password Age:** The minimum password age setting controls how many days users must wait before they can reset their password. This setting can be a value from one to 998 days. If set to 0, passwords can be changed immediately. Although this seems to be a fairly innocent setting, too low a value could allow users to defeat your password history settings. For example, if you set this value to 0 and your password history is set to 10, all users have to do is reset their password 10 times in a row, and then they can go back to their original password. This setting must be set to a lower value than the maximum password age, unless the maximum password age is set to 0, which means passwords never expire. Ten days or greater is usually a good setting, although this can vary widely depending on administrator preferences.
- **Maximum Password Age:** The maximum password age setting controls the maximum

period of time that can elapse before you are forced to reset your password. This setting can range from one to 999 days, or it can be set to 0 if you never want passwords to expire. A general rule for this setting is 90 days for user accounts; although for administrative accounts, it's generally a good idea to reset passwords more frequently. In high-security areas, 30 days is not an uncommon setting.

TAKE NOTE*

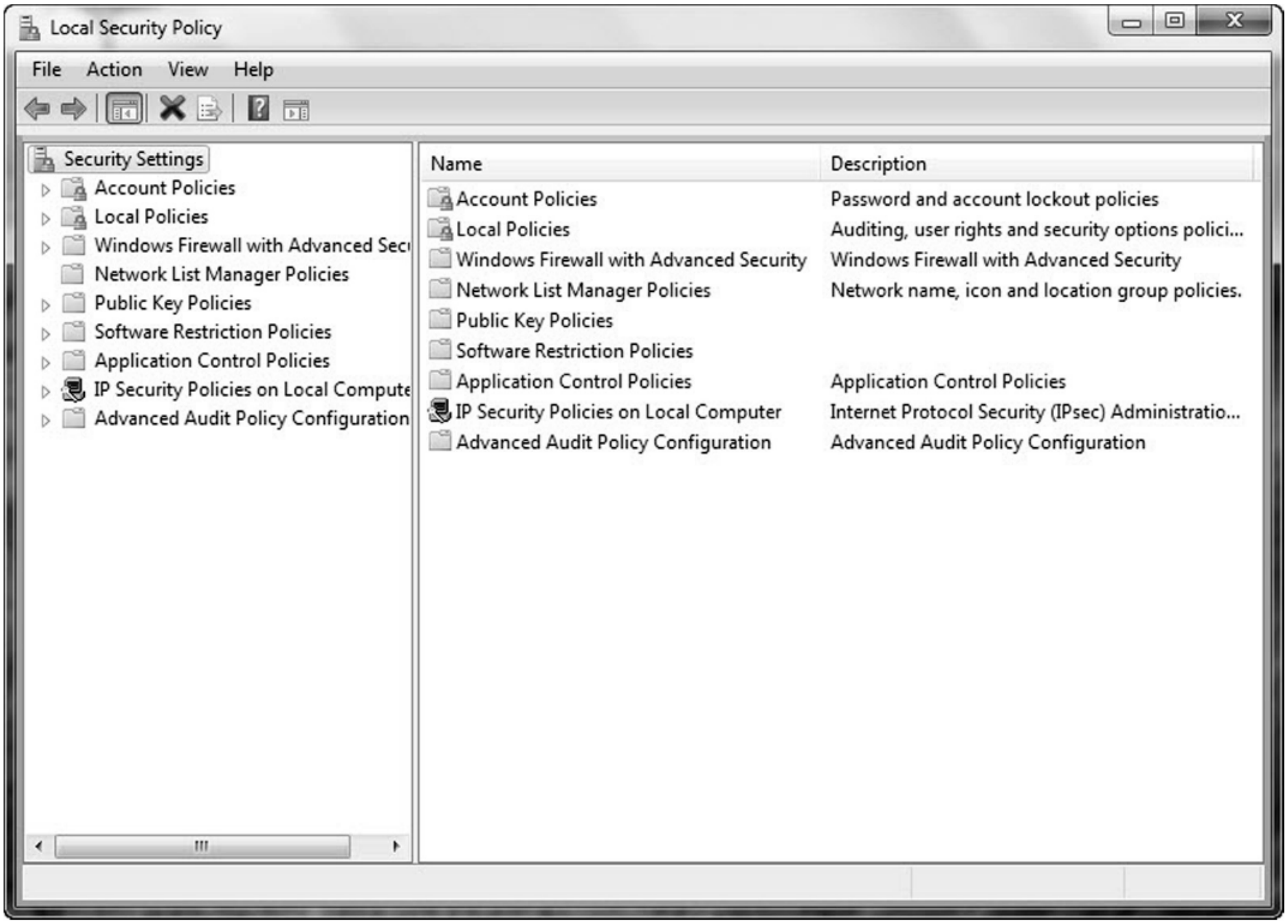
Passwords should always expire, except in extremely unique circumstances, such as service accounts for running applications.

Although this may add additional administrative overhead to some processes, passwords that don't expire can be a serious security issue in virtually all environments.

We have discussed the different settings you can use to ensure the best password security for your environment. Now, let's look at how to review those settings on a Windows 7 workstation.

REVIEW THE PASSWORD SETTINGS ON A WINDOWS 7 WORKSTATION

GET READY. Before you begin these steps, be sure to launch the **Local Security Policy** snap-in from the **Administrative Tools** menu (see Figure 3-1).

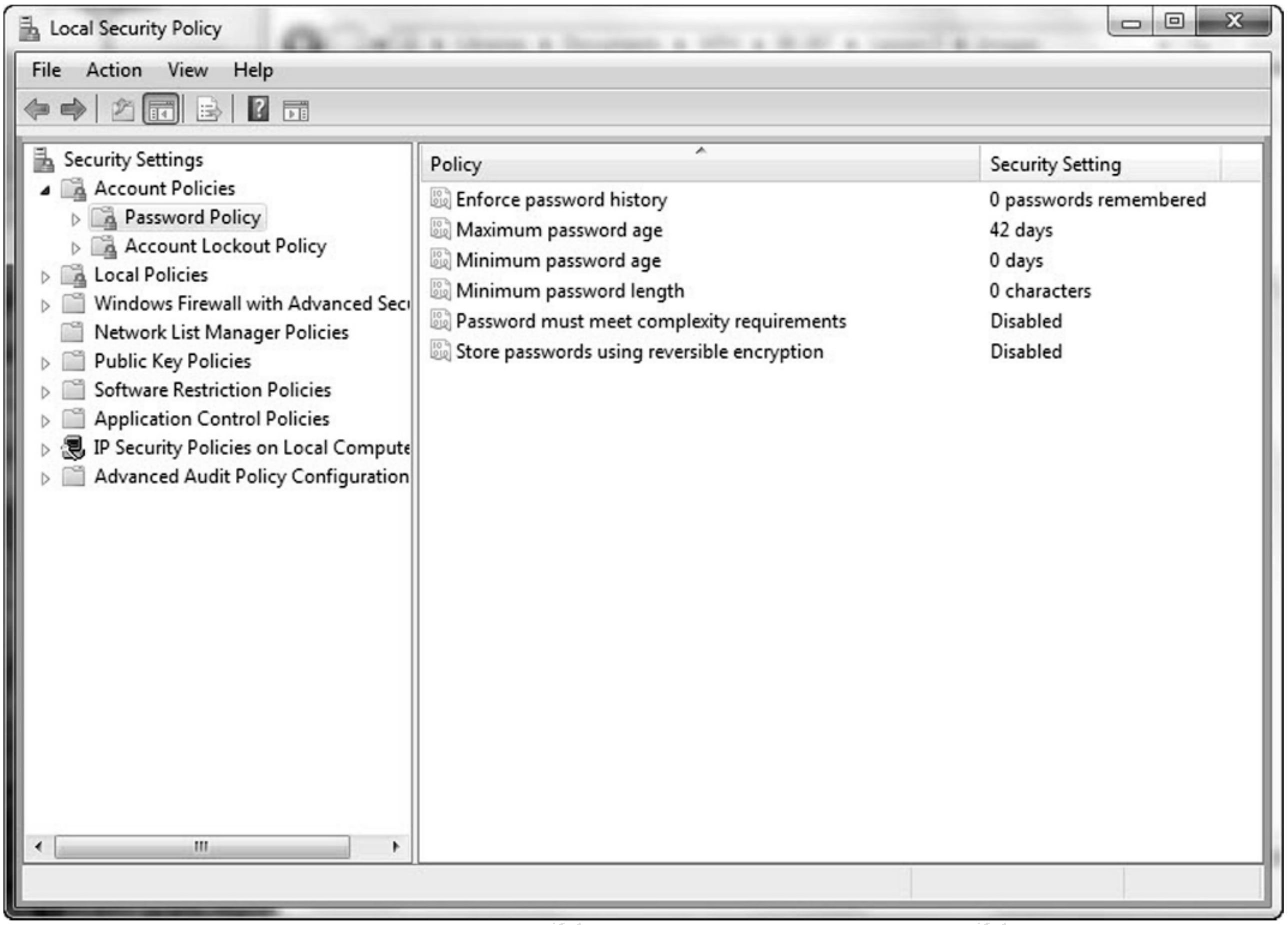

Local Security Policy
File
Action
View
Help
Security Settings
Account Policies
Local Policies
Windows Firewall with Advanced Secu
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Compute
Advanced Audit Policy Configuration

Name	Description
Account Policies	Password and account lockout policies
Local Policies	Auditing, user rights and security options polici...
Windows Firewall with Advanced Security	Windows Firewall with Advanced Security
Network List Manager Policies	Network name, icon and location group policies.
Public Key Policies	
Software Restriction Policies	
Application Control Policies	Application Control Policies
IP Security Policies on Local Computer	Internet Protocol Security (IPsec) Administratio...
Advanced Audit Policy Configuration	Advanced Audit Policy Configuration

Figure 3-1 Local Security Policy window

1. In the **Local Security Policy** snap-in, click on **Account Policies**.

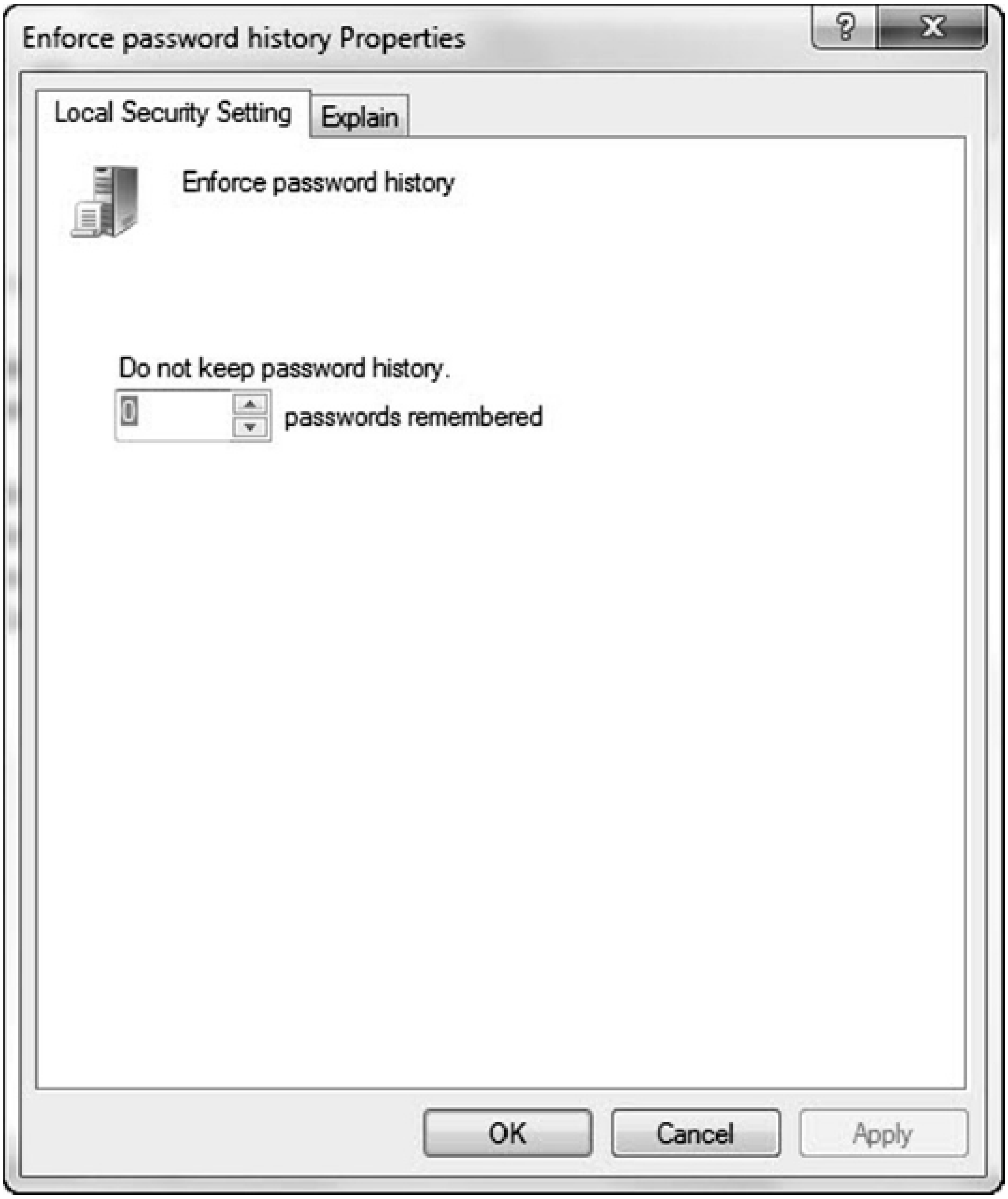
2. Click on **Password Policy**. You should see the password settings we've discussed in the right window. See Figure 3-2.


Local Security Policy
File
Action
View
Help
Security Settings
Account Policies
Password Policy
Account Lockout Policy
Local Policies
Windows Firewall with Advanced Secı
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Compute
Advanced Audit Policy Configuration

Policy	Security Setting
Enforce password history	0 passwords remembered
Maximum password age	42 days
Minimum password age	0 days
Minimum password length	0 characters
Password must meet complexity requirements	Disabled
Store passwords using reversible encryption	Disabled

Figure 3-2 Password Policy security settings

3. Click on each of the password settings (see Figures 3-3, 3-4, 3-5, 3-6, and 3-7 for the different settings).



Enforce password history Properties

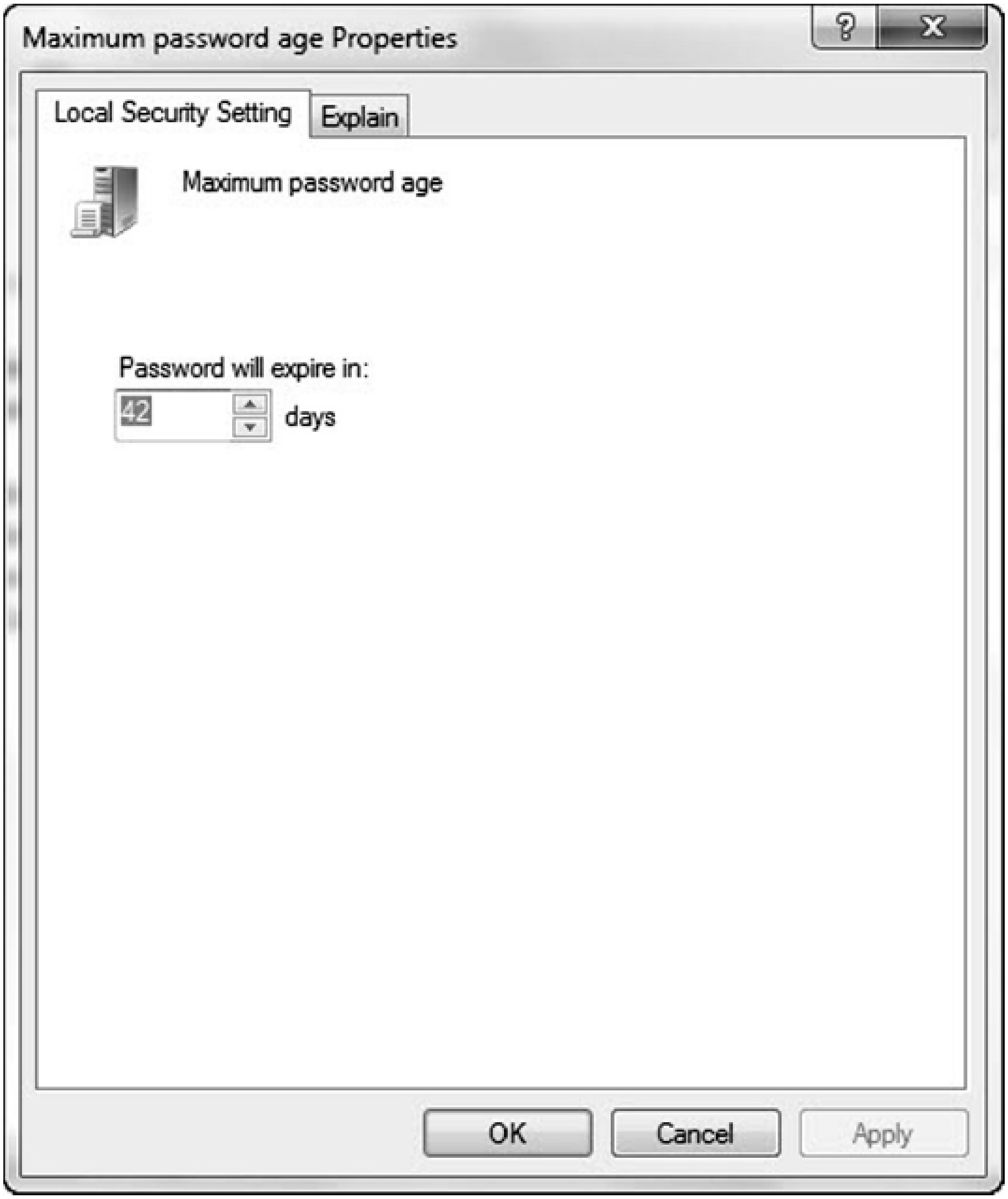
Local Security Setting | Explain

Enforce password history

Do not keep password history.

0 passwords remembered

Figure 3-3 Enforce password history

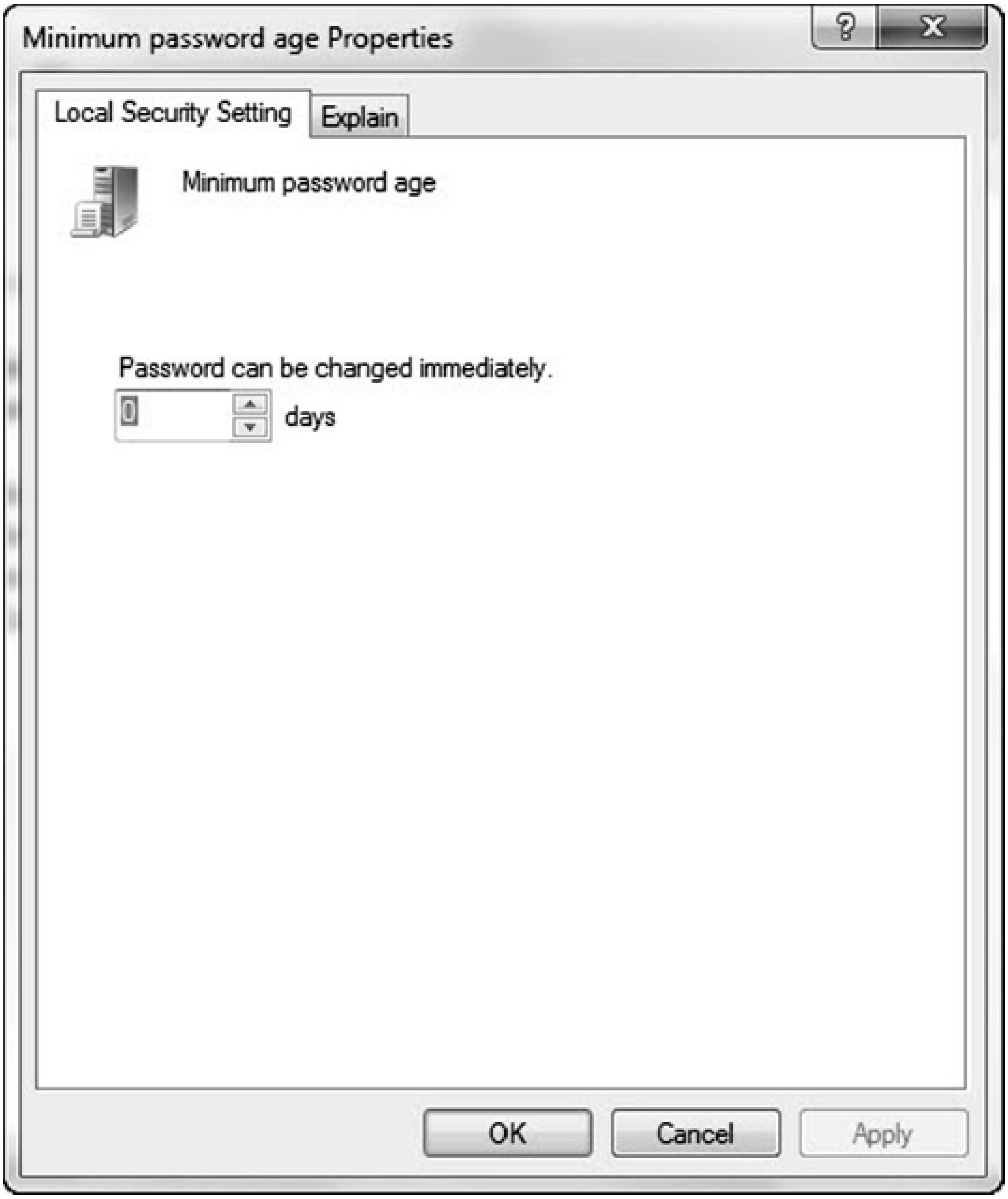


Maximum password age Properties

Maximum password age

Password will expire in:
42 days

Figure 3-4 Maximum password age

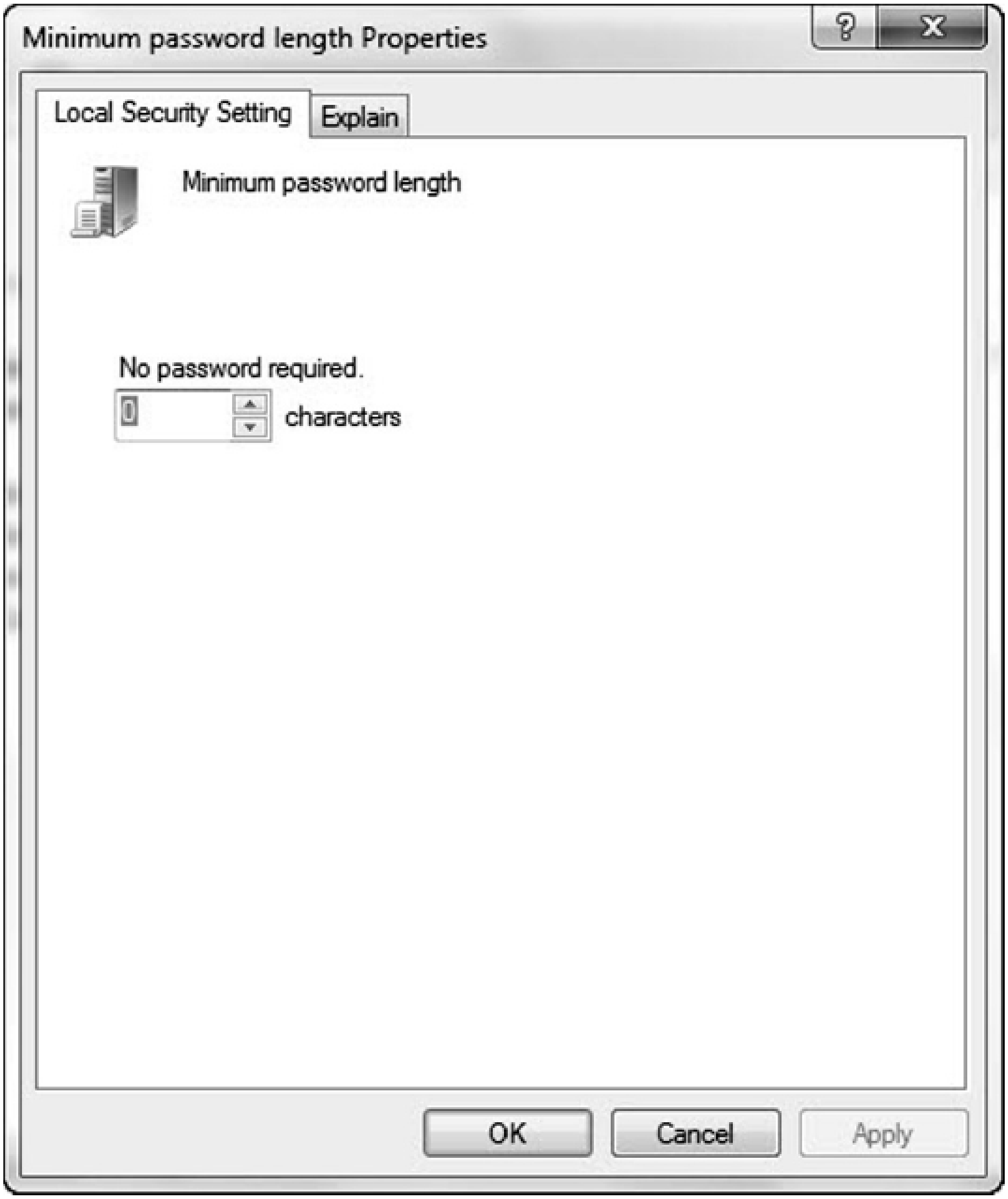


Minimum password age

Password can be changed immediately.

0 days

Figure 3-5 Minimum password age



Minimum password length Properties

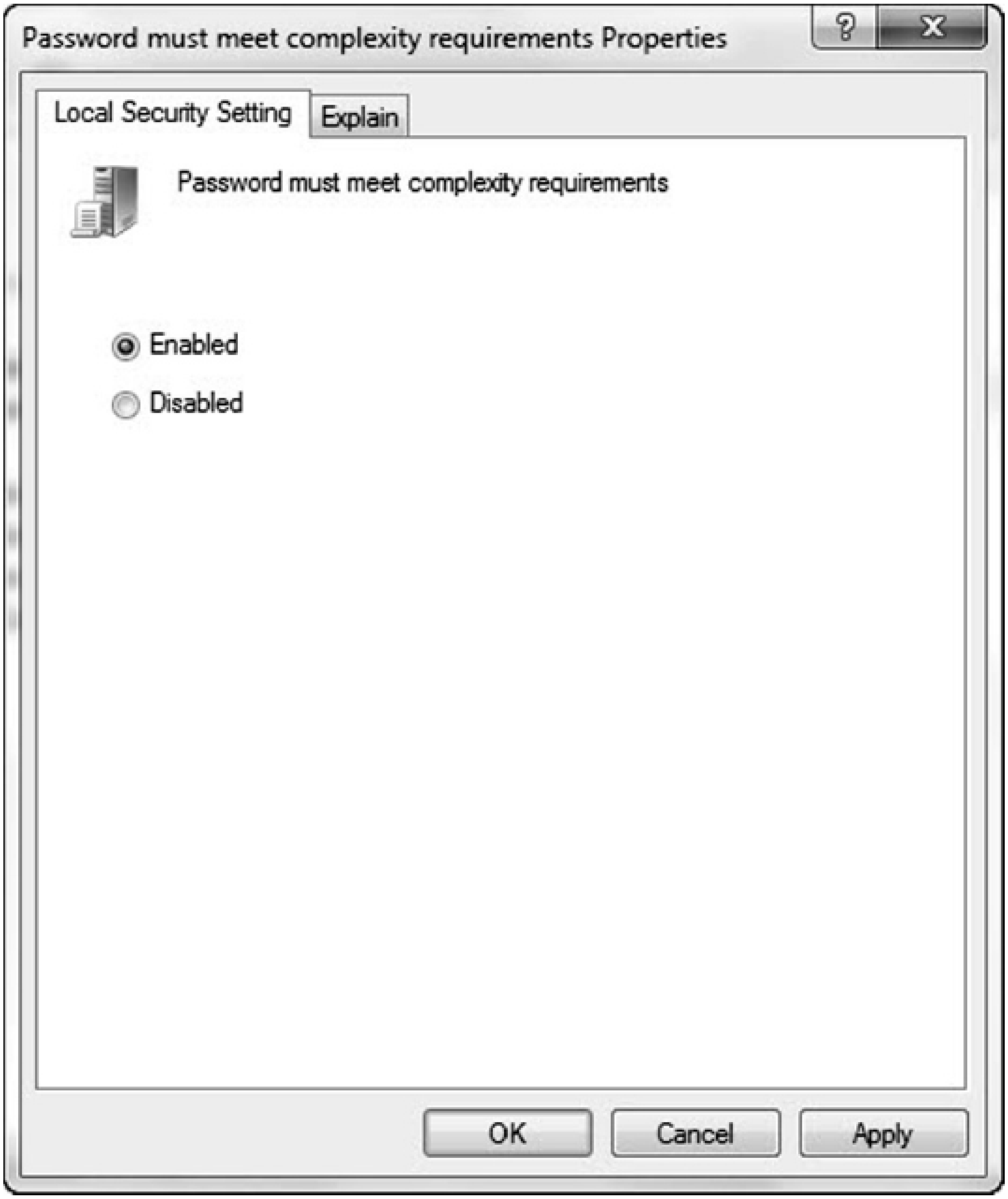
Local Security Setting

Minimum password length

No password required.

0 characters

Figure 3-6 Minimum password length



Password must meet complexity requirements Properties

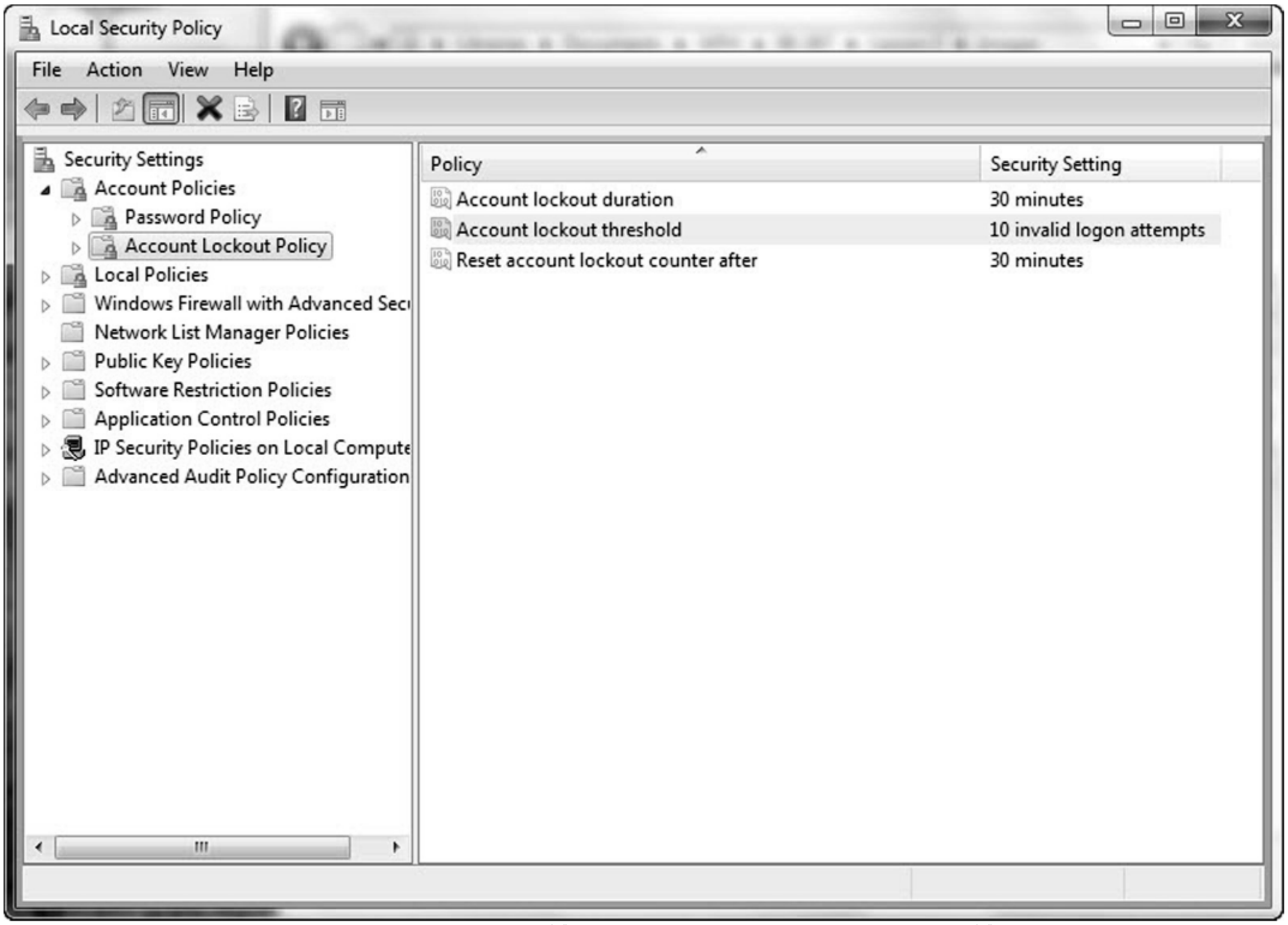
Password must meet complexity requirements

● Enabled

○ Disabled

Figure 3-7 Enforcing password complexity

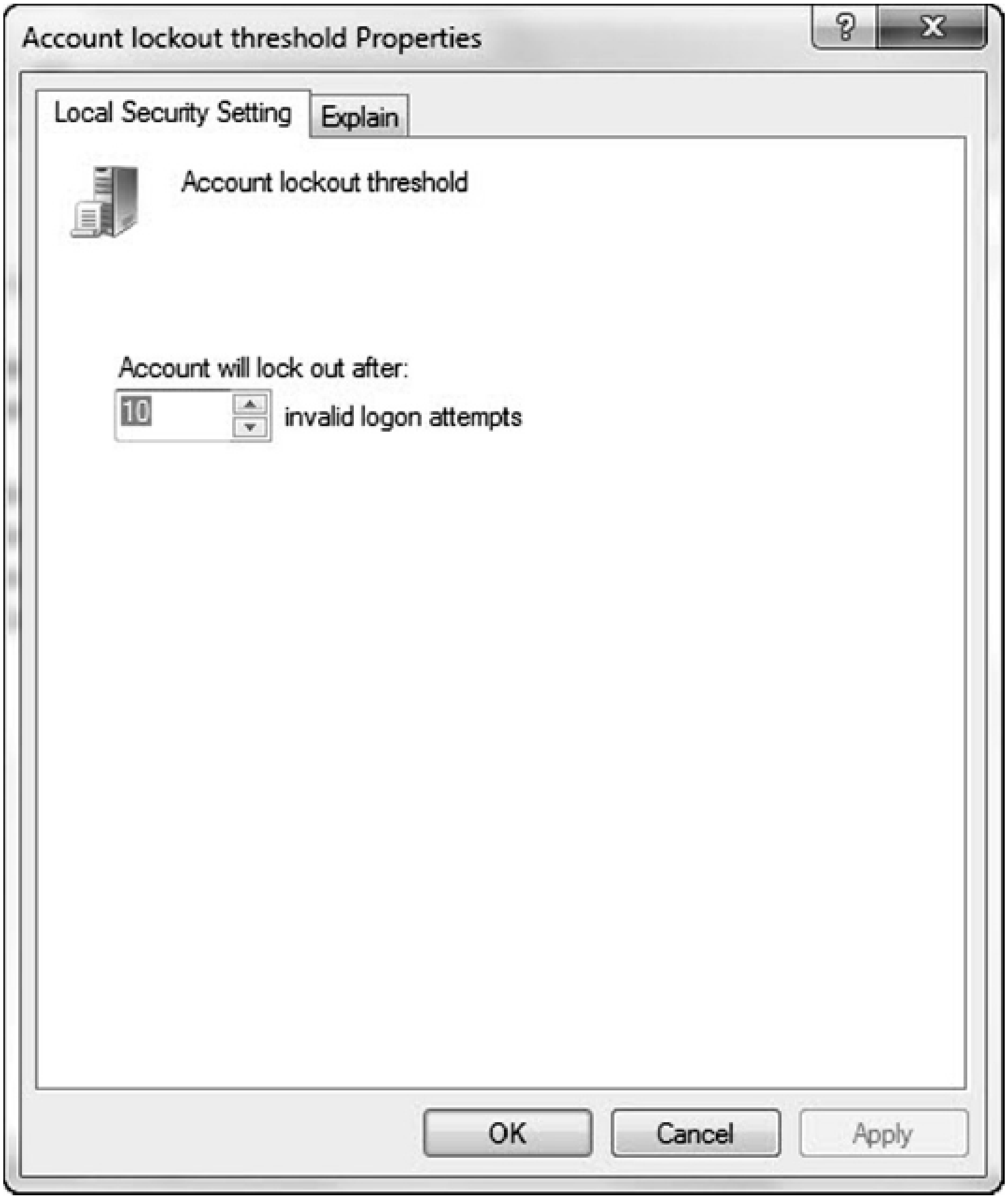
4. Click on **Account Lockout Policy**. You should see the account lockout settings we've discussed in the right window. See Figure 3-8.


Local Security Policy
File
Action
View
Help
Security Settings
Account Policies
Password Policy
Account Lockout Policy
Local Policies
Windows Firewall with Advanced Secu
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Compute
Advanced Audit Policy Configuration

Policy	Security Setting
Account lockout duration	30 minutes
Account lockout threshold	10 invalid logon attempts
Reset account lockout counter after	30 minutes

Figure 3-8 Account Lockout Policy settings

5. Click on each of the account lockout settings as discussed above (see Figures 3-9, 3-10, and 3-11 for the different settings).

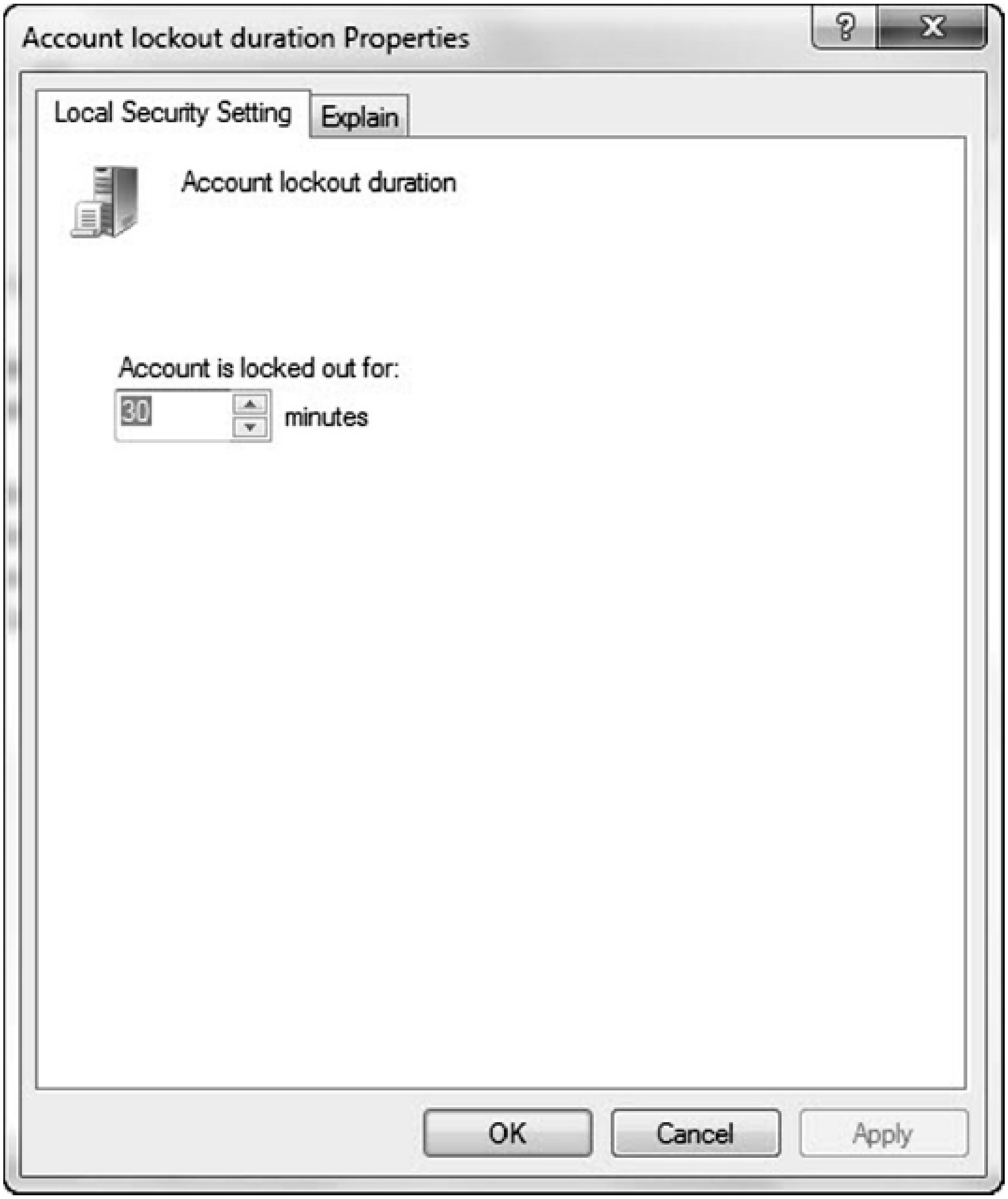


Account lockout threshold Properties

Account lockout threshold

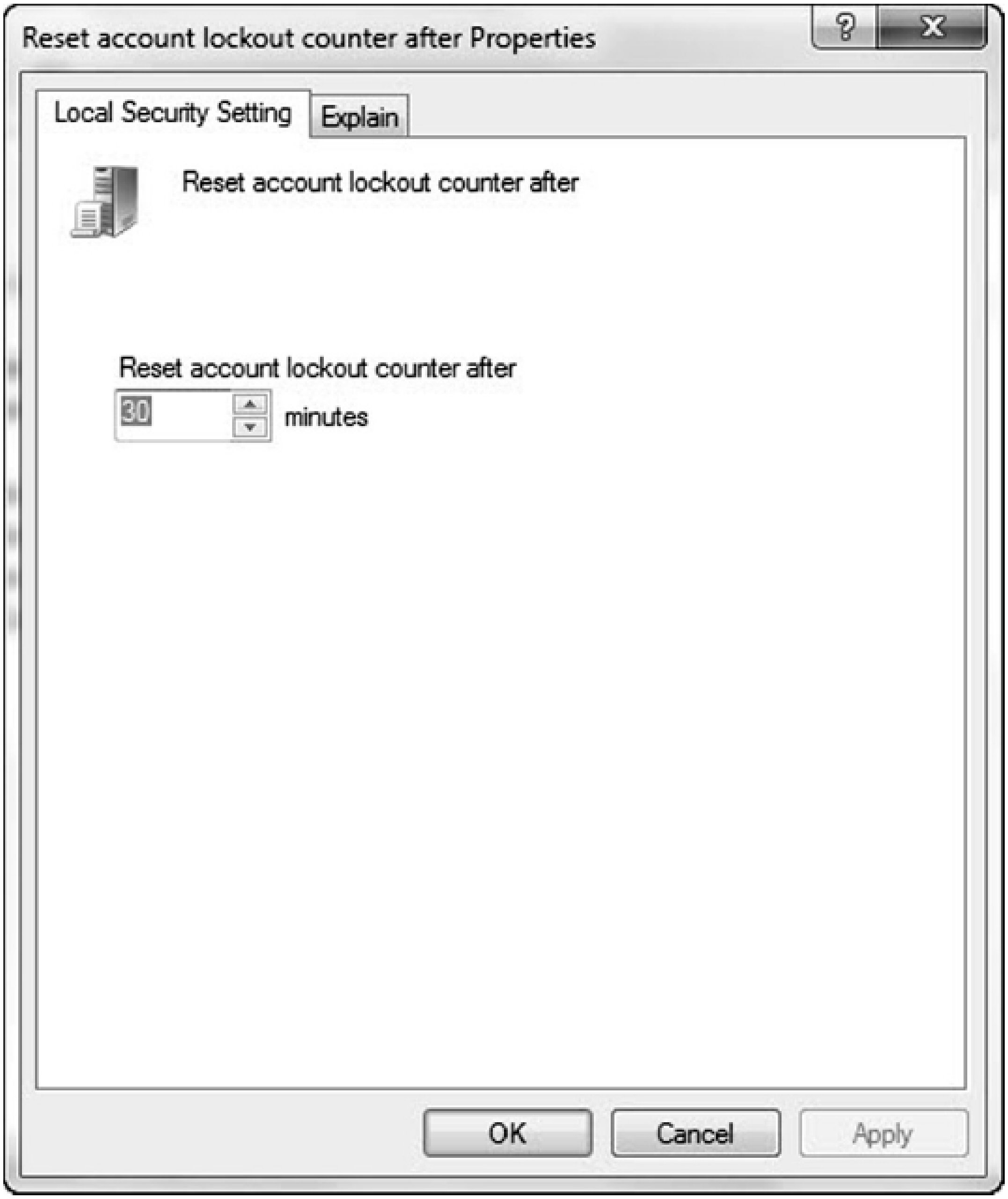
Account will lock out after: 10 invalid logon attempts

Figure 3-9 Account lockout threshold



Account is locked out for:
30 minutes

Figure 3-10 Account lockout duration



Reset account lockout counter after Properties

Reset account lockout counter after

Reset account lockout counter after

30 minutes

Figure 3-11 Reset account lockout timer

TAKE NOTE*
The password settings for a Windows 2008 domain are configured differently than for a stand-alone host or client. In this example, we are reviewing current password settings. We'll look at changing these settings using a Group Policy Object (GPO) in the next section.

Now that we have looked at setting password policies on a local client, let's take a look at how Group Policies can be used to set these properties for the members of a domain.

Using Password Group Policies to Enforce Security

Before we look at using Group Policies to enforce password settings, we should describe exactly what a Group Policy (also known as a Group Policy Object) is.

A ***Group Policy Object (GPO)*** is a set of rules that allow an administrator granular control over the configuration of objects in Active Directory (AD), including user accounts, operating systems, applications, and other AD objects. GPOs are used for centralized management and configuration of the Active Directory environment.

Now that you have a better idea of what a GPO is, let's look at how you can use one to enforce password controls in Active Directory.

USE A GROUP POLICY TO ENFORCE PASSWORD CONTROLS ON DOMAIN SYSTEMS

GET READY. Before you begin these steps, be sure to launch the **Active Directory Users and Computers** snap-in from the **Administrative Tools** menu.

1. Right-click the root container for the domain and select **Properties**.
2. In the **Properties** dialog box for the domain, click the **Group Policy** tab.
3. Click **New** to create a new GPO in the root container. Type "**Password Policy**" as the name of the new policy, and then click **Close**.
4. Right-click the root container for the domain, and then click **Properties**.
5. In the **Properties** dialog box, click the **Group Policy** tab, and then select your newly created GPO (named Password Policy.)
6. Click **Up** to move your new GPO to the top of the list.
7. Click **Edit** to open the **Group Policy Object Editor** for the GPO you just created.
8. Under **Computer Configuration**, navigate to the **Windows Settings\Security Settings\Account Policies\Password Policy** folder.
9. From here, you can set the policies as we did in the earlier exercise. Open each policy in turn, change the setting, and click **OK** to return to the main dialog box.

TAKE NOTE*
Windows Server 2008 fundamentally changes the mechanism for setting password attributes in Active Directory. We will look both at the legacy GPO model for enforcing password controls as well as a high-level example of how to perform a similar function in a Windows Server 2008 Active Directory.

10. Once you have configured the settings as desired, close the **Group Policy Object Editor**.
11. Click **OK** to close the domain properties dialog box.
12. Exit **Active Directory Users and Computers**.

You have now set a GPO to enforce password settings. This process works great with Windows Server 2003. However, with Windows Server 2008, the most current release of the Windows Server operating system, setting these policies requires a slightly different process.

In particular, Windows Server 2008 permits you to store what Microsoft calls password group policies. These policies allow you to set different password policies on different containers in the Active Directory. In order to support this new functionality, Windows Server 2008 includes two new object classes:

> **TAKE NOTE***
> When you are working with GPOs, you may find your changes cause unexpected consequences. If a new GPO causes problems, disable it until you have a better idea of what's causing the issue.

- Password Settings Container
- Password Settings Object

The Password Settings Container (PSC) is created by default under the System container in the domain. You can view it by using the Active Directory Users and Computers snap-in, but you will need to enable the advanced features to get to it. The PSC stores the Password Settings Objects (PSOs) for the domain.

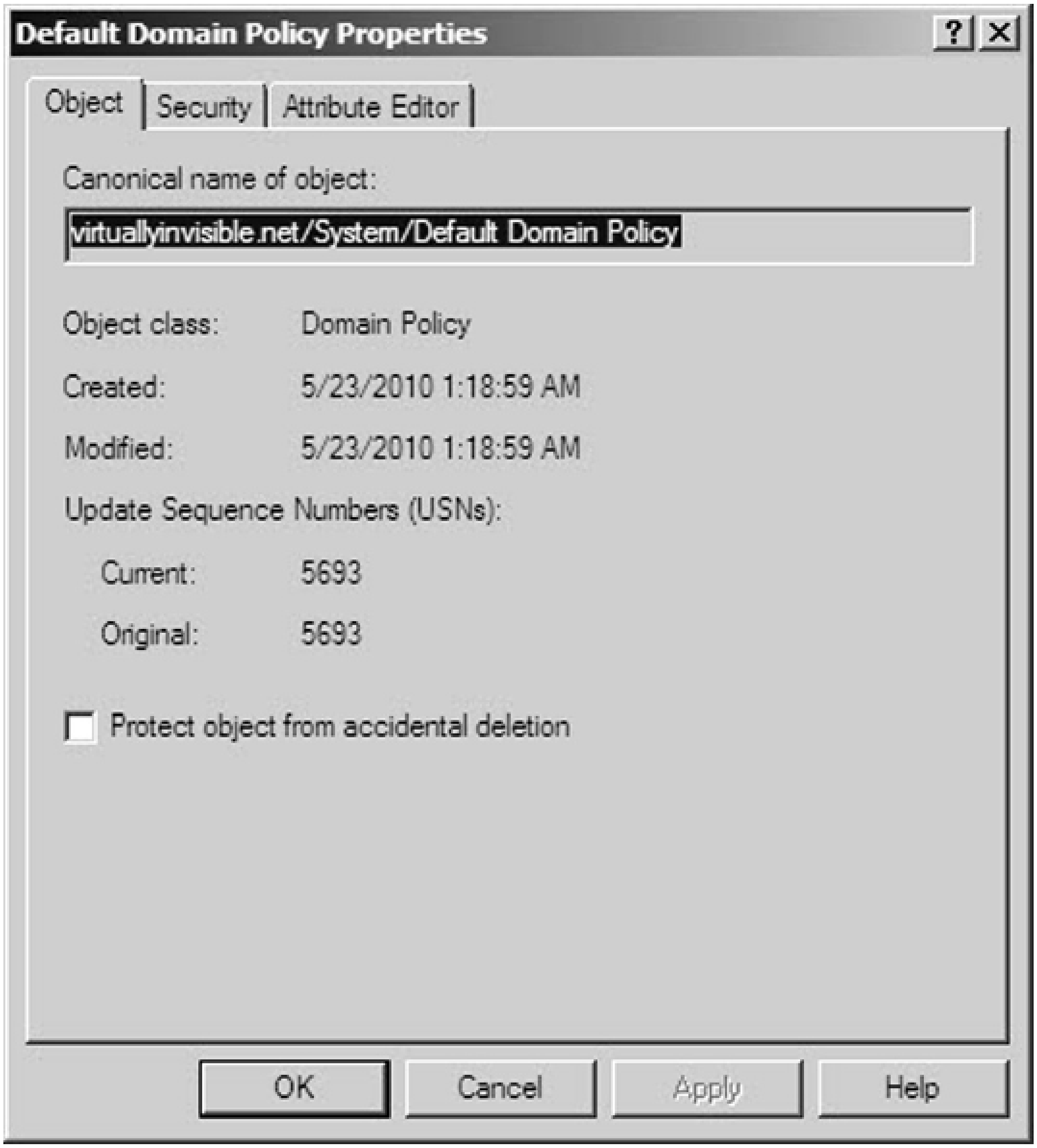
If no fine-grained password policies are configured, the Default Domain Policy, also accessible through the Active Directory Users and Computers snap-in, applies to all accounts in the domain.

Let's take a look at how to modify the Default Domain Policy to achieve an implementation that is similar to the use of the GPO in earlier versions of Active Directory.

USE THE DEFAULT DOMAIN POLICY TO ENFORCE PASSWORD CONTROLS ON DOMAIN SYSTEMS

> **GET READY.** Before you begin these steps, be sure to launch the **Active Directory Users and Computers** snap-in with the **Advanced Features** enabled from the **Administrative Tools** menu.

1. Expand the domain to show the default folders.
2. Double-click **System**. The list of default objects under the System container should be visible.
3. Right-click the **Default Domain Policy** and select **Properties**. The **Default Domain Policy Properties** dialog box will open (See Figure 3-12).



Canonical name of object:
virtuallyinvisible.net/System/Default Domain Policy

Object class: Domain Policy

Created: 5/23/2010 1:18:59 AM

Modified: 5/23/2010 1:18:59 AM

Update Sequence Numbers (USNs):

Current: 5693

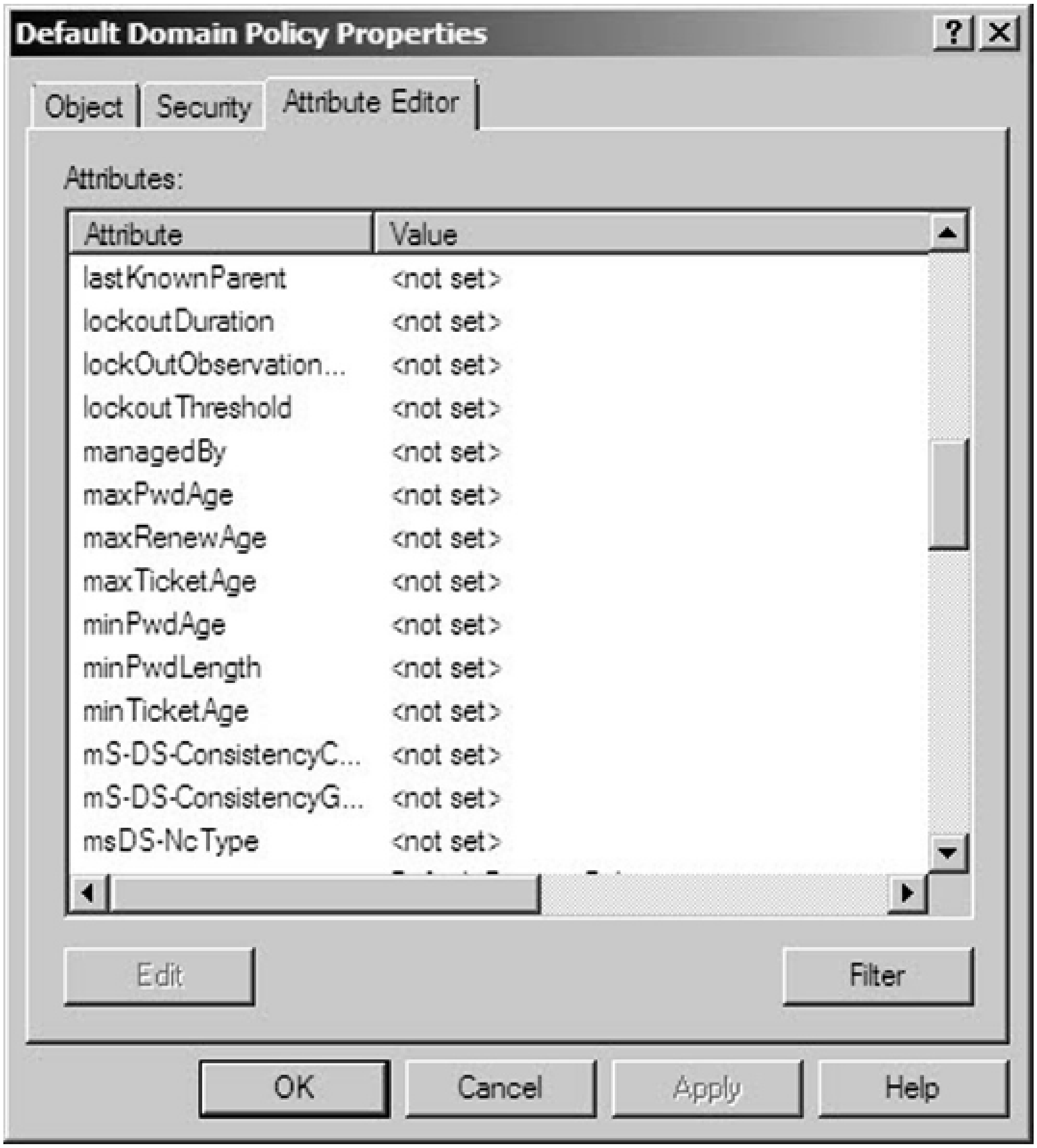
Original: 5693

□ Protect object from accidental deletion

Figure 3-12 Default Domain Policy Properties Object tab

ent belongs to VICTOR D AZULA (@hotmail.com) uthorized copies allowed!

4. Click on the **Attribute Editor** tab, and scroll down to the **Password Attributes** (see Figure 3-13).



Default Domain Policy Properties

Object | Security | Attribute Editor

Attributes:

Attribute	Value
lastKnownParent	<not set>
lockoutDuration	<not set>
lockOutObservation...	<not set>
lockoutThreshold	<not set>
managedBy	<not set>
maxPwdAge	<not set>
maxRenewAge	<not set>
maxTicketAge	<not set>
minPwdAge	<not set>
minPwdLength	<not set>
minTicketAge	<not set>
mS-DS-ConsistencyC...	<not set>
mS-DS-ConsistencyG...	<not set>
msDS-NcType	<not set>

Figure 3-13 Default Domain Policy Properties Attribute Editor tab

5. Double-click the attribute you want to change.

6. When you have completed your desired changes, click **OK** to close the **Default Domain Policy Properties** dialog box.

7. Exit **Active Directory Users and Computers**.

Now that you know some ways to set password attributes on the client, both in a Windows Server 2003 Active Directory and in the current version of Active Directory, we need to discuss some of the most common attack methods you might encounter in the real world.

Understanding Common Attack Methods

Passwords have long been recognized as one of the weak links in many security programs. Although tokens, smart cards, and biometrics are gaining traction in the business world for securing key systems and data, a significant amount of confidential and private data is still being secured with passwords. Passwords are considered a weak link for two main reasons.

First, you are completely reliant on users in the selection of passwords. Even though many users will select strong passwords in line with your standards, and even though you have some tools to enforce password attributes like complexity and minimum length, there will still be users who continue to select weak passwords. Attackers are aware of this and will try to exploit those individuals.

> **TAKE NOTE***
> The new functionality of Windows Server 2008 provides significant benefits to experienced Active Directory administrators, but it can create significant complexity for someone new to AD.
> Make changes with caution.

Second, even strong passwords are vulnerable to attack through a variety of different mechanisms.

EXAMINING DICTIONARY AND BRUTE FORCE ATTACKS

A ***dictionary attack*** uses a dictionary containing an extensive list of potential passwords that the attacker then tries in conjunction with a user ID in an attempt to guess the appropriate password. This is known as a dictionary attack because the earliest versions of this attack actually used lists of words from the dictionary as the basis of their login attempts. Today, custom dictionaries with likely passwords are available for download from the Internet, along with applications that can use these possible passwords against your systems.

Another, more crude type of attack—called a brute force attack—doesn't rely on lists of passwords, but rather tries all possible combinations of permitted character types. Although this type of attack was historically considered ineffective, improvements in processor and network performance have made it more useful, although not nearly as effective as a dictionary attack.

These types of attacks tend to be most successful when a password's length is seven characters or less. Each additional character adds a significant number of possible passwords. These attacks are often successful because users sometimes use common words with the first letter capitalized and then append a number to meet the complexity guidelines. These are the easiest passwords for users to remember, but they are also the easiest for an attacker to compromise.

The Account Lockout settings discussed earlier in the lesson are a critical defense against this type of attack, because an Account Lockout will either slow or even stop a brute force attack in its tracks after the configured number of incorrect logon attempts is reached.

LOOKING AT PHYSICAL ATTACKS

Anytime your computer can be physically accessed by an attacker, that computer is at risk. Physical attacks on your computer can completely bypass almost all security mechanisms, such as by capturing the passwords and other critical data directly from the keyboard when a software or hardware ***keylogger*** is used. In fact, if your encryption key passes through a keylogger, you might find that even your encrypted data is jeopardized.

> **XREF**
> Lesson 1 contains more details on keylogging.

Some other physical attacks may include the use of a hidden camera to tape your keystrokes, or even the removal and duplication (or direct theft) of your hard drive. Although not specifically a password attack, if attackers remove your hard drive, they can frequently bypass password controls by mounting the drive remotely and accessing your data directly from the drive, without an intervening operating system.

EXAMINING LEAKED AND SHARED PASSWORDS

Another challenge you'll encounter when dealing with users in an office environment is leaked or shared passwords. Users tend to trust their co-workers. After all, everyone works for the same company, and in many cases, they have access to similar company information. As a result, users can easily be convinced to share their passwords with co-workers who feel they "need" this information. This practice is especially problematic in environments with high turnover, because there is no way to tell who in the last crop of terminated employees still has a friend's user ID and password and thus has continued access to the network.

Even if users don't deliberately provide their password to another employee, the casual work environment frequently makes it easy for employees to watch as their co-workers key in their user IDs and passwords.

Finally, spouses, children, and other relatives may end up with access to your computing environment because of their close relationship with your employees.

User awareness is the best way to combat this type of attack. Providing users with a greater understanding of the risks and impact of these types of behaviors can go a long way in keeping passwords under the control of only authorized users. In addition, the minimum and maximum password age settings, as well as the password history setting, can help mitigate this risk. Here, even if someone obtains a password he or she shouldn't have, when the maximum password age limit is hit, it will force a reset of all passwords, including shared ones.

LOOKING AT CRACKED PASSWORDS

A ***cracked password*** frequently relies on more than just a password attack. In a password crack attack, the attacker gets access to an encrypted password file from a workstation or server. Once he or she has access, the attacker starts running password cracking tools against the file, with an eye toward breaking as many passwords as possible and leveraging them to further compromise the company's network and systems.

Passwords that are stored in an encrypted state are harder to break than passwords that are stored in clear text or in a hashed state. However, with today's computing power, even encrypted password stores are being compromised by password cracking attacks.

If you ever become aware that your password store has been compromised, you need to have all employees with an account on the compromised system change their passwords immediately.

You can also use the same tools that potential attackers might use to audit the security of your password stores. Trying to crack your own password file is a fairly common practice, as it not only allows you to test the security of your password store, but if any passwords are compromised and/or weak, it gives you the ability to have users change them to more secure passwords.

EXAMINING NETWORK AND WIRELESS SNIFFERS

If an attacker can access your internal network, your wireless network, or even an Internet access point used by your employees, then he or she has the ability to use a specialized tool known as a sniffer to try to intercept unencrypted passwords. Although applications have gotten much better in recent years, there are still a number of them that pass sensitive information like passwords across networks in clear text—which means this information can be read by anyone with the ability to view data as it traverses the network.

Sniffers are specially designed software (and in some cases hardware) applications that capture network packets as they traverse a network, displaying them for the attacker. Sniffers are valid forms of test equipment, used to identify network and application issues, but the technology has been rapidly co-opted by attackers as an easy way to grab logon credentials.

In addition to sniffers that are used to attack wired networks, there are now sniffers that have the ability to capture wireless data as well. Whenever you are connected to your business wireless, perhaps while at the local coffee shop or even while attending a meeting at a hotel, you are potentially at risk of having your data literally pulled out of the air and made available to an attacker. The use of encryption remains the best mechanism for combating this type of attack.

Another area of concern with sniffers is wireless keyboards. At its core, a wireless keyboard is a broadcast technology that sends keystrokes from the keyboard to a receiver connected to the computer. If you can get a receiver tuned to the same frequency close enough to the computer, you can capture every keystroke entered into the wireless keyboard—without needing to install a keylogger. Most wireless keyboards now support additional security, such as encrypted connections, but they are still broadcasting all information that the user types, so as long as people continue to enter the majority of their data via keyboard, this will be a significant potential source for attackers to exploit. In fact, many companies only permit their employees to use wired keyboards in order to mitigate this risk.

XREF
Sniffing is discussed in more detail in Lesson 4.

LOOKING AT GUESSED PASSWORDS

Although not as prevalent an issue as it was in years past, the possibility still exists that someone could sit down at your computer and guess your password. As we have seen in countless movies, an attacker may be familiar with the person whose system they are trying to compromise, or they may look around and see a postcard from a trip or pictures of an employee’s kids with their names listed and ascertain a password from these items. Indeed, if a user does not follow corporate rules requiring a strong, not easily guessable password, but instead selects a password based on a spouse’s, child’s, or pet’s name and birthday, an attacker could more easily guess the password and access the employee’s data.

That being said, this type of attack is almost never seen these days. With the widespread availability of password cracking tools, the type of individual targeting required to guess someone’s password is seldom worth the effort. It is generally much easier to leverage an attack using one of the other methods currently available. Typically, only co-workers or close friends will try to guess a user’s password.

SKILL SUMMARY

IN THIS LESSON YOU LEARNED:

- The strength of a password can be determined by looking at the password’s length, complexity, and randomness.

- A complex password uses characters from at least three of the following categories: uppercase, lowercase, numeric characters, and nonalphanumeric characters.

- Account lockout refers to the number of incorrect logon attempts permitted before a system will lock an account.

- The Minimum Password Age setting controls how many days users must wait before they can reset their password.

- The Maximum Password Age setting controls the maximum period of time that can elapse before users are forced to reset their password.

- A Group Policy Object (GPO) is a set of rules that allow an administrator granular control over the configuration of objects in Active Directory (AD), including user accounts, operating systems, applications, and other AD objects.

- Passwords have long been recognized as one of the weak links in many security programs.

- During a dictionary attack, the attacker tries an extensive list of potential passwords in conjunction with a user ID to try to guess the appropriate password.

- Brute force attacks try all possible combinations of permitted character types in an attempt to determine a user’s password.

- Physical attacks on a computer can completely bypass almost all security mechanisms, such as by capturing passwords and other critical data directly from a keyboard when a software or hardware keylogger is used.

- In a password crack attack, attackers get access to an encrypted password file from a workstation or server. Once they have access to this file, attackers start running password cracking tools against it.

- If an attacker can gain access to your internal network, your wireless network, or even an Internet access point used by your employees, he or she has the ability to use a specialized tool known as a sniffer to intercept unencrypted passwords.

- Although not as prevalent an issue as it was in years past, the possibility still exists that someone could sit down at your computer and guess your password.

Knowledge Assessment

Multiple Choice

Circle the letter or letters that correspond to the best answer or answers.

1. Which of the following are not valid password controls? (Choose all that apply.)

a. Minimum Password Age

b. Maximum Password Age

c. Maximum Password Length

d. Account Lockout Threshold

e. Password History

2. Which of the following would be an acceptable password on a Windows 7 Professional system with Password Complexity enabled and Minimum Password Length set to eight? (Choose all that apply.)

a. Summer2010

b. $$Thx17

c. ^^RGood4U

d. Password

e. St@rTr3k

3. What is the maximum setting for Minimum Password Age?

a. 14

b. 999

c. 998

d. 256

4. You are setting up your first secure Windows 7 Professional workstation and you are setting the password history. What are the minimum and maximum settings you can use? (Choose the best answer.)

a. 0, 14

b. 1, 14

c. 0, 24

d. 1, 24

e. 0, 998

5. Which of the following are common types of password attacks? (Choose two answers)

a. Cracking

b. Man in the middle

c. Smurf

d. Spoofing

e. Brute force

6. One form of brute force password attack uses an extensive list of predefined passwords. What is this form of brute force attack called? (Choose the best answer.)

a. Bible attack

b. Cracking attack

c. Guessing attack

d. Dictionary attack

7. As the Chief Security Officer for a small medical records processing company, you suspect that a competitor will be attacking your network soon. Having worked in the business for a while, you're pretty sure that this competitor will try to run a dictionary attack against one of your Windows application servers. You want to be sure your competitor can't get into the server using this attack method. Which setting should you adjust in order to ensure this attack has a limited chance at success? (Choose the best answer.)

a. Minimum Password Length

b. Account Lockout Threshold

c. Password History

d. Maximum Password Age

8. You are the head of the corporate security department, and the Microsoft team has asked you for some assistance in setting the password controls on their new stand-alone server. Which Administrative Tool should you use to configure these settings?

   a. Active Directory Users and Computers

   b. Computer Management

   c. Security Service

   d. Local Security Policy

9. What are the two new features introduced in Windows Server 2008 that permit the use of fine-grained password policies? (Choose all that apply.)

   a. Global Policy Object

   b. Password Settings Container

   c. Password Settings Object

   d. Password Policy

10. Why would you use a minimum password age?

   a. To ensure that someone does not guess a password

   b. To stop someone from trying over and over to guess a password

   c. To make sure a user does not reset a password multiple times until he or she can reuse his or her original password

   d. To automatically reset a password

Fill in the Blank

1. A set of rules that allows an administrator granular control over the configuration of objects in Active Directory (AD), including user accounts, operating systems, applications, and other AD objects, is known as a(n) _____________.

2. The number of incorrect logon attempts permitted before a system will lock an account is known as the _____________.

3.

The setting that determines the number of unique passwords that must be used before a password can be re-used is the _______________.

4. The type of attack that uses an extensive list of potential passwords is known as a(n) _______________.

5. When you use special software to read data as it is broadcast on a network, you are _______________ the network.

6. The _______________ needs to be less than or equal to the Account Lockout Duration.

7. The highest setting that Account Lockout Duration can use is _______________.

8. In a Windows Server 2008 Active Directory, the _______________ automatically applies in the event you have not set a fine-grained password policy.

9. The three configuration settings for account lockout are _______________, _______________, and _______________.

10. A _______________ account is one type of account you can configure so that the password does not expire.

Competency Assessment

Scenario 3-1: Understanding Long Passwords

a. Let’s say you have a PIN that is four digits long. Each digit can be 0, 1, 2, 3, 4, 5, 6, 7, 8, or 9, giving you a total of 10 possible digits. How many different PINs are possible?

b. Let’s say you have a four-letter password, and each character in the password must be a lowercase letter (a–z). There are 26 letters in the alphabet. How many different passwords are possible?

c. Let’s say you have a six-letter password, and each character in the password must be a lowercase letter (a–z). How many different combinations are possible?

d. Let’s say you have an eight-letter password, and each character in the password must be a lowercase letter (a–z). How many different combinations are possible?

e. Let’s say you have an eight-letter password, and each character in the password must be either a lowercase letter (a–z) or an uppercase letter (A–Z). How many different combinations are possible?

f. Let’s say you have an eight-letter password, and each character in the password must be a lowercase letter (a–z), an uppercase letter (A–Z), a digit (0–9), or a special character (~`!@#$%^&*()_-+={[}]|\:;”’<,>.? or /). How many different combinations are possible?

Scenario 3-2: Changing Passwords

Imagine that you work for the Contoso Corporation. Your CIO tells you that he just got a message on his computer saying that he has to change his password. He wants to know why he must not only use such a relatively long password, but also why he must change that password on a regular basis. What should you tell him?

Proficiency Assessment

Scenario 3-3: Managing Users

Log in to a computer running Windows 7 and create an account for John Adams (JAdams) using the Control Panel. Then add JAdams to the Administrator group. Set the password for JAdams to Password01. Verify the groups that JAdams is a member of using the Computer Management Control.

Scenario 3-4: Configuring a Local Security Policy

On a computer running Windows 7, open Group Policy Management to access the Local Group Policy. View the Password Policy and Account Lockout Policy.

Workplace Ready

Understanding Group Policies

Group Policies is one of the most powerful features included with Active Directory. Besides being used to configure password policies and account lockout policies, it can be used to assign user rights that define what an individual can do on a computer. It can also be used to install software, prevent software from being installed, lock down a computer, standardize a working environment, and preconfigure Windows. When you look deeper in Group Policies, you will see that there are literally thousands of settings.