

Understanding IT Security

Information Technology (IT) security includes multiple elements all designed to minimize losses. Digital security methods ensure that users are uniquely identified and authenticated before they are granted permission to access resources. Valuable data can be further protected with encryption. When disposing of media at the end of its life cycle, secure methods are used to erase the data. When necessary, the media is destroyed.

Exam 220-802 objectives in this chapter:

- 1.4 Given a scenario, use appropriate operating system features and tools.
 - Administrative
 - Users and groups
 - Local security policy
- 1.5 Given a scenario, use Control Panel utilities (the items are organized by “classic view/large icons” in Windows).
 - Common to all Microsoft Operating Systems
 - User accounts
- 1.8 Explain the differences among basic OS security settings.
 - User and groups
 - Administrator
 - Power user
 - Guest
 - Standard user
 - NTFS vs. Share permissions
 - Allow vs. deny
 - Moving vs. copying folders and files
 - File attributes
 - Shared files and folders
 - Permission propagation
 - Inheritance

- User authentication
 - Single sign-on
- 2.1 Apply and use common prevention methods.
 - Physical security
 - Lock doors
 - Biometrics
 - Badges
 - Key fobs
 - RFID badge
 - RSA token
 - Retinal
 - Digital security
 - User authentication/strong passwords
 - Directory permissions
 - User education
 - Principle of least privilege
- 2.3 Implement security best practices to secure a workstation.
 - Setting strong passwords
 - Requiring passwords
 - Restricting user permissions
 - Changing default user names
 - Disabling guest account
 - Screensaver required password
- 2.4 Given a scenario, use the appropriate data destruction/disposal method.
 - Low level format vs. standard format
 - Hard drive sanitation and sanitation methods
 - Overwrite
 - Drive wipe
 - Physical destruction
 - Shredder
 - Drill
 - Electromagnetic
 - Degaussing tool

Prevention

Security models commonly follow a prevent/detect/respond model. First, methods are implemented to prevent any security incidents from occurring. Incidents still occur, so other methods are used to detect them and respond as quickly as possible to contain the damage from an incident. Two methods that are important in the realm of prevention are user education and the principle of least privilege.

User Education

A core tenet of security is educating users about risks. The better users understand the risks, the more likely they are to comply with the security requirements.

User education might be done formally in gatherings or via online training sessions. Additionally, education is often done informally by an educated PC technician sharing knowledge with users. To share your knowledge, you first need to ensure that you have it.

Security-conscious PC technicians understand the different authentication methods and the importance of strong passwords and password management. They understand the importance of least privilege and how groups are often used in its implementation. They recognize the risks related to different types of malicious software (malware) and understand the importance of running up-to-date antivirus software on up-to-date computers. They are well aware of various methods used by attackers, including social engineering attacks, and are willing to share their knowledge.

MORE INFO CHAPTERS 15 AND 26

Chapter 15, “Configuring Windows Operating Systems,” covers Windows Update and patch management techniques. Chapter 26, “Recognizing Malware and Other Threats,” covers different types of malware, antivirus software, and social engineering.

Principle of Least Privilege



The principle of *least privilege* is an important security concept used in IT systems and networks of all sizes. Users should be given only the rights and permissions that they need to do their jobs and no more. This prevents them from accidentally causing problems such as accidentally deleting key system files. It also protects IT resources if a faithful worker becomes a disgruntled employee.

If usability is your only concern, you can give everyone full administrative access. Everyone will be able to access any resource and perform any task. In practice, this is rarely used because of the significant security risks. Instead, most organizations implement the principle of least privilege by identifying what privileges users need to perform their jobs and grant them only those privileges.



EXAM TIP

The principle of least privilege ensures that users are granted only enough privileges to perform their jobs and no more. Regular users rarely need administrative privileges, and membership in any type of administrative group should be limited.

Authentication



Authentication occurs when users prove their identity. The most common way this occurs is when a user claims an identity with a user name and proves the identity with a password. However there are several possible authentication methods, known as *authentication factors*. The three authentication factors are as follows:

- **Something you know.** This includes passwords or personal identification numbers (PINs).
- **Something you have.** This includes items you can physically hold, such as some types of badges and smart cards.
- **Something you are.** Biometric methods such as fingerprints or retinal scans are in this factor category.

Something You Know

Passwords are by far the most common method of authentication. They are also the weakest compared with the other factors. Ideally, users should create strong passwords so that they can't easily be guessed. This is common knowledge among IT professionals, but many regular users don't realize the importance of using a strong password or even how to create a strong password.

MORE INFO CREATING STRONG PASSWORDS

Microsoft hosts the Safety And Security Center, which provides a wealth of information about computer security, digital privacy, and online safety. It includes the following page, which provides information about creating strong passwords: <http://www.microsoft.com/security/online-privacy/passwords-create.aspx>. You can use the following page to test the strength of a password: <https://www.microsoft.com/security/pc-security/password-checker.aspx>.

Elements of Strong Passwords

Many systems apply a set of rules that users must follow when they create a password. This is commonly called a password policy, and it helps ensure that users create a strong password. If users don't follow the password policy rules, the password or password change is rejected.

A strong password includes the following elements, and any or all of these rules can be a part of a password policy:

- **Uses at least eight characters.** If you use a single lowercase alphabet letter password such as *a* or *b*, it only takes 26 guesses to discover it. If you use two characters, it takes 676 guesses (26^2). Guessing a password with eight lowercase alphabet letters requires over 208 billion guesses (26^8). Some people suggest a password should be 12 or more characters.
- **Uses all four character types.** Passwords should include uppercase letters, lowercase letters, numbers, and special characters such as \$ or @. Instead of just 26 possible characters, there are 95 possible characters—26 lowercase letters, 26 uppercase letters, 10 numbers, and 33 characters. An 8-character password using all four character types has over 6 quadrillion (95^8) possible combinations.
- **Does not use your name.** Passwords shouldn't include your user account name, your actual name, the name of your company, or other names that can be easily guessed.
- **Is different from other passwords.** If you have a password of IP@ssedA+, you shouldn't use another password that's similar, such as IP@ssedA+2 or IP@ssedA+3. After the first password is discovered, the others are easily guessed.



EXAM TIP

Strong passwords should be used with any desktop user account. Strong passwords use at least three character types, and four character types are commonly recommended.

Using Passphrases

A common method used to create a strong password is with a passphrase. There are multiple ways you can do this, such as the following:

1. Start with a sentence such as **I am A+ certified.**
2. Capitalize the first letter of each word—**I Am A+ Certified.**
3. Remove all the spaces—**IAmA+Certified.**
4. Replace some letters with characters (for example, replace *i* with *!*, or *a* with *@*)—**IAmA+Cert!f!ed.**
5. Add numbers or replace some letters with numbers (for example, replace *l* with *1* or *e* with *3*)—**1AmA+Cert!f!ed.**

At this point, you have a strong 12-character password that is easy to remember. Later in your IT career, you can replace it with **1AmNet+Cert!f!ed** and then **1AmSec+Cert!f!ed**.

REAL WORLD ATTACKS ARE EASY WHEN PASSWORDS ARE SIMPLE

Reports of attackers breaking into systems and stealing password database files are relatively common. For example, in June 2012, LinkedIn was attacked and a password database of 6.46 million users was stolen. The thieves cracked many of the simple passwords and posted the database online asking for help cracking the stronger passwords. All were eventually cracked.

The word *link* was reportedly the number one password in the database. While that might be an easy password to remember for a LinkedIn account, it's also quite easy to guess. The number two most used password was "1234."

On the surface, this might not seem like it's such a big deal. If someone discovers the LinkedIn password, they can log in to a LinkedIn account. So what? The real problem is that people who use simple passwords also commonly use the same password for all their online accounts, including banking and other financial websites. When an attacker gets one password, the attacker often gets them all.



Quick Check

1. What is the weakest type of authentication?
2. What is included in a strong password?

Quick Check Answers

1. Passwords.
2. At least eight characters and multiple character types.

Something You Have

All of the methods in the something-you-have authentication factor are items that you can hold in your hand. Often these items serve dual purposes. For example, a user can wear a badge when walking around the building and then use the badge to log on. In this case, the badge would also include smart-card components.

Badges and Smart Cards



A *smart card* is about the same size as a credit card. It includes data about the user and some cryptographic information to help keep it secure. Smart card readers are connected to a computer or part of the keyboard. When users want to log on, they insert the card into the reader and enter a PIN or password to authenticate.

A risk with smart cards is that they can be lost or misplaced. Anyone who finds the card can potentially use it to impersonate the user. However, by combining it with another method

of authentication, such as a PIN or password, the user reduces that risk. It's the same concept used with automated teller machine (ATM) cards and PINs.

NOTE MULTIFACTOR AUTHENTICATION

When more than one factor of authentication is used, it's called multifactor authentication. Multifactor authentication must include one element in two or more different factors. Using both a PIN and a password is not multifactor authentication because PINs and passwords are both in the something-you-know factor, but a PIN and a smart card is multifactor authentication.

In many cases, the smart card is also used as a badge. It includes the user's picture and other information about the user. Some organizations use stronger physical security within secure areas and require employees to wear these badges at all times except for when they use the badge to log on to their computer.



EXAM TIP

Device drivers for smart card readers often must be installed separately. If you add a keyboard that includes a smart card reader, you might need to install device drivers. If the smart card reader is part of the computer, it can often be enabled or disabled in the BIOS.

RFID Badges and Physical Security

One way you can provide physical security for a secure area is by keeping the entry doors locked. This is useful for smaller areas, such as a wiring closet that houses network devices like routers and switches. It isn't as useful for a high-traffic area where people frequently go in and out.

Radio Frequency Identification (RFID) badges are sometimes used to automatically open doors. Users simply wave their badge in front of a badge reader and the door unlocks. This is similar to how you can wave some credit cards in front of a credit card reader to purchase items.

Both use the same type of electronics. The card reader includes a special type of magnet, and when the card is passed close to the reader, the magnet charges the card, providing it with power. The card then broadcasts information received by the reader. For RFID badges, the broadcasted information can be a simple code to open the door. It can also include information about the user to record the user's access.

Key Fobs and RSA Tokens



A *key fob* is a small device that displays a number and can easily be attached to a key chain. The number changes periodically and is synchronized with an authentication server. Key fobs are most commonly used when authenticating with a website.

For example, a company can issue key fobs to traveling employees so that they can log on to a company website. Figure 25-1 shows how this works. The user accesses the company server over the Internet, and the server responds with a login page. The user enters a valid user name, password, and the number displayed in the key fob, and then the user clicks the Log In button. The server validates this data, and if everything is correct, the user is authenticated.

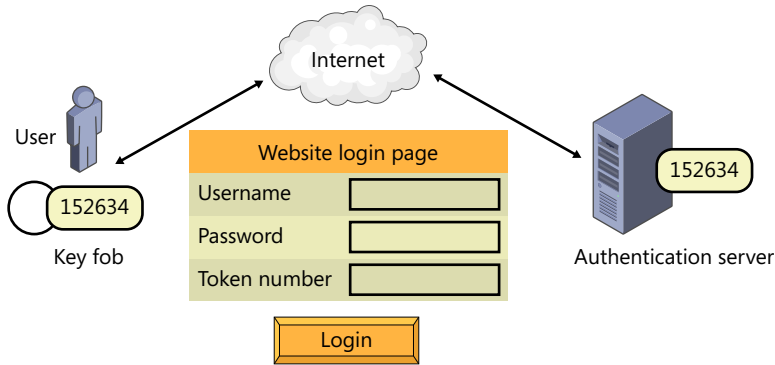


FIGURE 25-1 Authenticating with a key fob.

Typically, the number displayed in the key fob changes every 60 seconds. The authentication server knows what should be displayed in the key fob at any given time, so a number previously used won't work. Users must have the key fob in their possession. RSA SecureID is a popular key fob, and it is sometimes just called RSA token. These are sold by EMC Corporation.

NOTE RSA IS NOT AN ACRONYM

RSA is the name of a company that is now a security division of EMC Corporation. The letters are derived from the founders of RSA: Rivest, Shamir, and Adleman.

Something You Are



The third factor of authentication is something you are. This factor is proven with *biometrics*. The most common method uses fingerprints. Users register their fingerprints with the biometric system and authenticate later with the fingerprint.

Fingerprints can be used for both identification and authentication. For example, police use fingerprints for identification. If they find a fingerprint at a crime scene and can match it to another fingerprint, they can identify an individual.

Authentication systems can use fingerprints for authentication or identification. When used for authentication, a user enters a user name to claim an identity and then uses a fingerprint to prove the identity. This method is less susceptible to errors.

Retinal scans are the most accurate and often the most expensive form of biometrics. The retina is at the rear of the eye and includes a complex network of blood vessels. The pattern of these blood vessels is unique and normally stays the same for a person's entire lifetime. The retina is scanned with an infrared light as a person looks into an eyepiece.



EXAM TIP

Biometric authentication systems are susceptible to errors. They can falsely reject an authorized user and falsely accept an unauthorized user. Retinal biometric systems are the most accurate.

Other biometric methods used for authentication are iris scans (scanning the iris instead of the retina), facial recognition, and voice recognition.

Behavioral biometrics aren't used as often, but it is possible to identify individuals based on actions. This includes signature verification (identifying someone from their signature) and keystroke dynamics (measuring speed and pressure as an individual types).



Quick Check

1. What is displayed in a key fob?
2. What is the strongest type of biometric authentication?

Quick Check Answers

1. A number synchronized with an authentication server.
2. Retinal scans.

Single Sign-On

Single sign-on (SSO) technologies allow a user to log on once and access multiple resources without logging on again. Chapter 18, "Introducing Networking Components," compares workgroups and domains. Often, the reason an organization creates a domain instead of a workgroup is to support SSO.

Figure 25-2 compares a workgroup and a domain. In a workgroup, each computer has its own security accounts manager (SAM) database, which includes user names and passwords. Tom can log on to his computer because his user name and password are in the SAM on his computer. If Tom wants to log on to Kim's computer, the SAM on Kim's computer needs to have a separate account for Tom. If Tom needs to log on to all four computers, each SAM would have separate entries and he'd need to remember four separate user names and passwords.

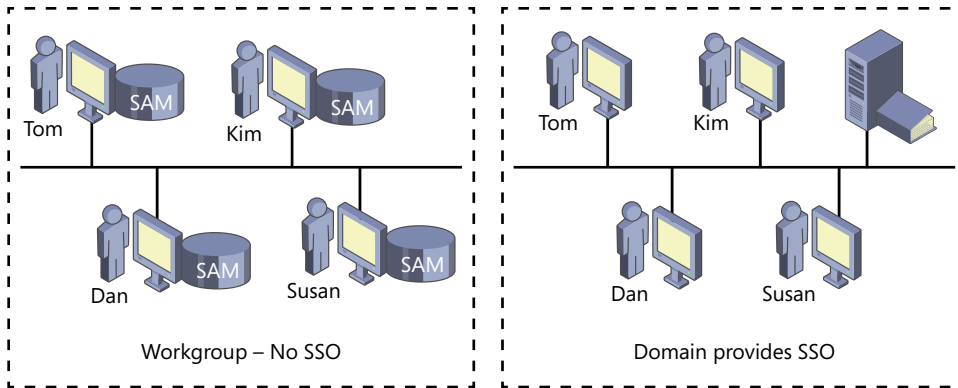


FIGURE 25-2 Authentication in workgroup and in domain.

In comparison, a Microsoft domain adds a domain controller running Active Directory Domain Services (ADDS). Each user has one account within ADDS and can use this account to log on once. For example, Tom can use his domain account to log on to any of the four computers.



EXAM TIP

Users have a single account to access multiple resources with SSO. When users are required to remember multiple passwords, they are more likely to write them down, decreasing overall security.

Requiring Password with the Screen Saver

Another security step you can take is to enable a password-protected screen saver on the computer. This requires users to log in after a screen saver starts.

Screen savers are designed to protect monitors from screen burn-in. For example, if the same image is displayed in a plasma monitor, the image can be burned in and remain visible even when the power is turned off. The screen saver starts after a period of inactivity and prevents the burn-in.

On Windows 7, you can enable the screen saver by right-clicking the desktop, selecting Personalize, and then clicking Screen Saver. Figure 25-3 shows the Screen Saver Settings page. After configuring the screen saver, select the On Resume, Display Logon Screen check box. After the screen saver starts, the user must enter credentials to get back into Windows.

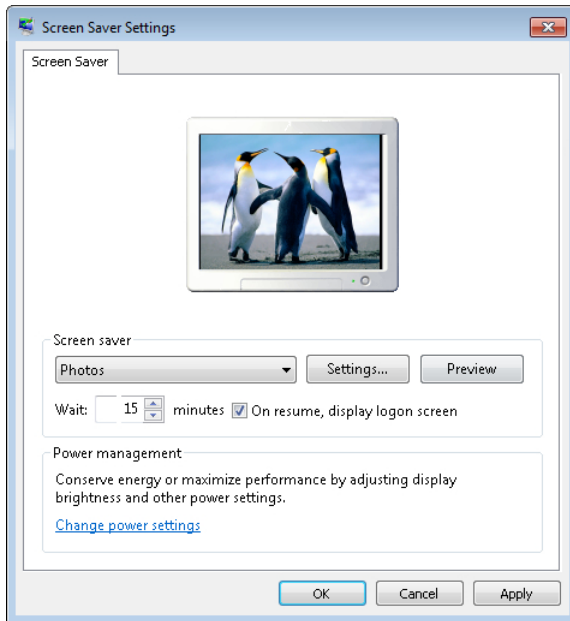


FIGURE 25-3 Enabling password protection with the screen saver.

It's not recommended, but it's possible to have a Windows user account without a password. If the user account isn't using a password, the screen saver doesn't require one.

IMPORTANT BEWARE OF VIRUSES

Windows includes several built-in screen savers, and you can find more online. However, many screen savers available online are infected with malware. When you install the screen saver, you're also installing the malware. Whenever malware is hidden within an apparently legitimate program, it's called a Trojan, or Trojan horse.

Local Security Policy

The Local Security Policy applet includes hundreds of settings that administrators commonly use to help secure a computer. Many of these settings aren't accessible anywhere else.

You can start it from the Administrative Tools group within Control Panel. You can also start it by entering **secpol.msc** from a command prompt or in the Start, Search text box.

Requiring Strong Passwords

One way the Local Security Policy is often used is to configure a password policy. When configured, it applies to all computer accounts on the local system and enforces the password policy.

Figure 25-4 shows the Local Security Policy open with Account Policies expanded and the Password Policy selected. These settings require users to change their password at least every 42 days and use a complex password at least 12 characters long. The last 24 passwords are remembered for the account, and the user must wait at least one day before changing the password again.

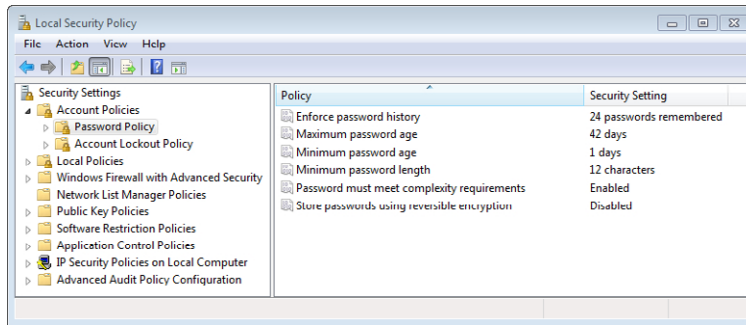


FIGURE 25-4 Using Local Security Policy to require a strong password.

NOTE POLICY SET BY DOMAIN POLICY IN A DOMAIN

Administrators commonly configure domain-wide policies that apply to all computers and users in the domain. If the computer is joined to the domain, domain policies take precedence over the policy set on the local computer.

Group Policy and Local Security Policy

Group Policy is a powerful tool used by administrators to configure a setting once and apply it to multiple computers in a domain. For example, if users need to use strong passwords, an administrator can configure one Group Policy setting and all users in the domain will be required to comply with the policy.

You can start the Group Policy editor for a local system by entering **gpedit.msc** from the command prompt or in the Start, Search text box. You can also create your own Microsoft Management Console (MMC) and add the Group Policy Object Editor snap-in by using procedures from Chapter 13, "Using Windows Operating Systems."

Figure 25-5 shows the Group Policy editor open on a Windows 7–based system. The dotted-line box is highlighting some key security settings, and if you compare them to those in Figure 25-4, you can see that they are the same settings available in the Local Security Policy tool.

Group Policy has thousands of configuration settings, including hundreds of security settings that can be accessed with the Local Security Policy. You certainly aren't expected to know all of the settings that are available in Group Policy, but it is valuable to know that it is commonly used to manage computers in a domain.

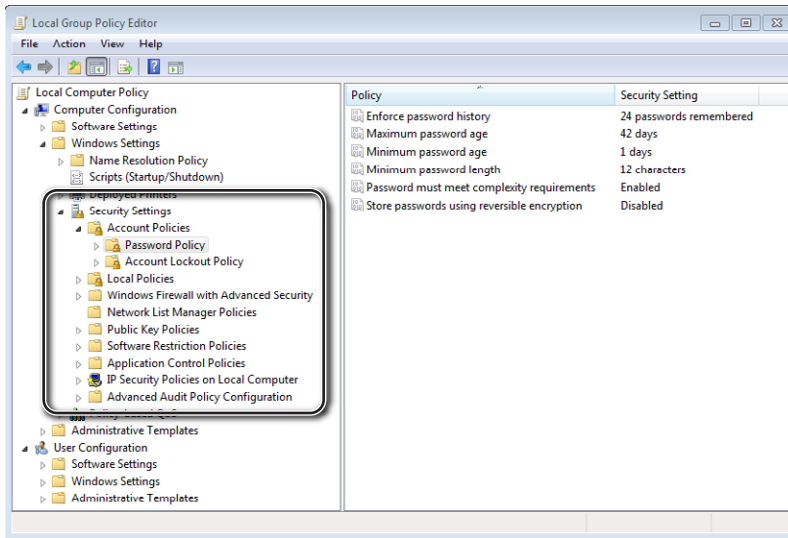


FIGURE 25-5 Viewing Security Settings in the Group Policy Editor.



Quick Check

1. What allows users to use a single user name and password?
2. What tool is used to force users to create strong passwords?

Quick Check Answers

1. Single sign-on (SSO).
2. Local Security Policy (or Group Policy in a domain).

Users and Groups

Microsoft systems support users and groups as a primary method of authentication and *authorization*. Users authenticate by providing a user name and password. They are then authorized to perform tasks based on rights and permissions granted to this account.

It's common to assign rights and permissions with groups. For example, you can add a user account to the Administrators group, granting the user full administrative privileges.

NOTE RIGHTS, PERMISSIONS, AND PRIVILEGES

Rights refer to the ability to take an action, such as the right to change the time. Permissions refer to the ability to access a resource, such as the permission to read or modify a file. Privileges include both rights and permissions. For example, administrative privileges imply that the account has full rights and permissions on a system.

User Accounts

When Windows is first installed, a user account is created for the primary user. There are additional user accounts created by default, and you can also add additional accounts with different tools.

When a user tries to access a resource, the operating system verifies that the user is authorized. Administrators often enable security logging to show when users access resources. These logs record the activity of the user based on the user account.

If someone else used your account and deleted data or modified entries, log entries recording the action would record that you did it. With this in mind, users should have individual user accounts with their own password. Additionally, users should never give out their password to anyone else.

Default User Accounts

Windows-based systems include default user accounts. The following two default user accounts, both disabled by default, are in Windows XP, Windows Vista, and Windows 7:

- **Administrator.** The Administrator account has full rights and permissions to do anything and everything on the system. It is often referred to as the local administrator account because when you use it, you can manipulate resources only on the local system, not on other computers.
- **Guest.** The Guest account is disabled by default and is created for temporary use only. For example, if you want to let someone use your computer to browse the Internet, you can enable the Guest account. The user can log on with this account and run basic applications, including a web browser. This way you don't have to create an account that you won't need after the user is done.



EXAM TIP

The Guest account provides a user with basic access to programs. It is disabled by default and should be kept disabled unless it's needed.

Windows XP also the following two additional user accounts by default. They are not in Windows Vista or Windows 7:

- **HelpAssistant.** This account is used for providing Remote Assistance.
- **SUPPORT_388945a0.** This is used for the Help And Support Service.

Standard User vs. Administrator

In Windows Vista and Windows 7, accounts are identified as standard user accounts or administrator accounts. The account created during the installation of Windows is an administrator account.

- **Standard user.** Users can run most software with this account, and they can modify some system settings that do not apply to other users. They cannot modify security settings.
- **Administrator.** Administrators have full privileges on the computer and can modify any settings.

In Windows XP, accounts are identified as limited or computer administrator. The limited account is similar to a standard user account, and a computer administrator account is the same as an administrator account in Windows Vista and Windows 7.

UAC and Access Tokens in Windows Vista and Windows 7

User Account Control (UAC) is used in Windows Vista and Windows 7 as a method to prevent unauthorized changes. For example, malware can sometimes make changes in Windows XP without the user's knowledge. UAC in Windows Vista and Windows 7 blocks this malware.

Anytime a user is logged on with an administrator account, the user is assigned two access tokens: a standard user access token and an administrator access token. These are directly related to the standard user and administrator account types.

Most of the time, only the standard user access token is used, and the user can do anything that a standard user can do. If the user tries to do something that requires administrative privileges, UAC switches into Admin Approval Mode. By default, UAC dims the screen and prompts the user to approve the action. The dimmed screen prevents software from automatically approving the action and requires the user to answer the prompt.

MORE INFO CHAPTER 11, "INTRODUCING WINDOWS OPERATING SYSTEMS"

Chapter 11 describes UAC in more depth and includes steps you can use to view and modify UAC settings.

User Accounts Applet

There are two ways you can create user accounts—with the User Accounts applet and with the Local Users And Groups snap-in that is a part of the Computer Management console. This section shows how to use the User Accounts applet, and Local Users And Groups is covered later.

You can start the User Accounts applet in Windows XP, Windows Vista, and Windows 7 by clicking Start and selecting Control Panel. Change the view to Classic View on Windows XP and Windows Vista, or Large Icons on Windows 7. Double-click User Accounts.

Figure 25-6 shows User Accounts in Windows XP on the left and Windows 7 on the right. In Windows XP, User Accounts shows all users, and you can click an individual account to change its settings. In Windows Vista and Windows 7, User Accounts starts with the focus on the currently logged in user's account settings, and you can click Manage Another Account to show all accounts.

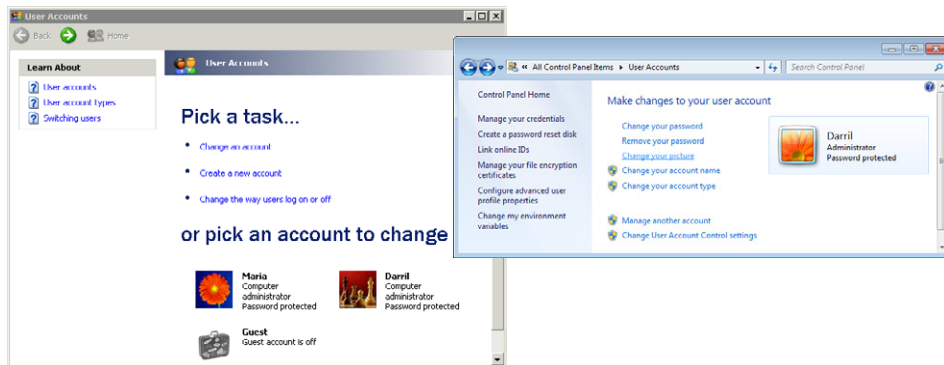


FIGURE 25-6 User Accounts applet in Windows XP and Windows 7.

Notice that the User Accounts applet tells you whether the account is an administrator type of account. When Computer Administrator or Administrator is not listed, it indicates that it is a limited or standard user type of account. If Password Protected is not included in the description, it indicates that a password is not configured.

You can use the User Accounts applet to create new accounts and to change the account type, passwords, and pictures. However, the Local Users and Groups applet provides more options.

Changing Default User Names

As a security best practice, it's recommended that you change the default user names. In Windows XP, Windows Vista, and Windows 7, the default accounts are Administrator and Guest. By changing the default user names, you make it more difficult for malware or an attacker to use these accounts.

For example, you can change the name of the Administrator account to Newadmin. If others try to log on by using Administrator, error messages will indicate that either the user

name or the password is wrong. No matter how many times they try to guess the password, they'll never succeed. Similarly, you can change the name of Guest to Newguest, making it more difficult to use this account.



EXAM TIP

Default user names should be changed when possible. Similarly, default passwords should also be changed. Wireless routers often include default administrator names and passwords. You can change the password, but you usually can't change the administrator name. In Windows, you can change both the name and the password.

Understanding Groups

Windows-based systems use groups to manage privileges and include some built-in groups. Instead of assigning privileges to an individual account, a best practice is to add a user to a group and assign the rights and permissions to the group.

Figure 25-7 shows user accounts for Holly and Joe. Holly's account is added to the Administrators group, and Joe's account is added to the Users group. The Administrators group has full access to the computer, so Holly can access the `\Windows\System32` folder. If Joe tried to do so, he would be blocked because neither his account nor the Users group has permission to access this folder.

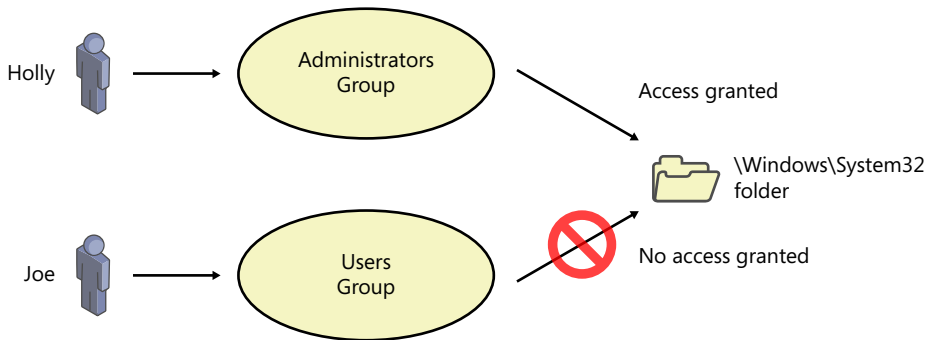


FIGURE 25-7 Granting privileges with group membership.

Default Groups

Windows-based systems include several default groups when Windows is first installed. Some of these built-in groups include the following:

- **Administrators.** This group has full privileges on the local computer. The administrator is a member of this group, which is how the administrator account gets its privileges. Similarly, when you create an administrator account on Windows Vista and Windows 7 or a computer administrator account on Windows XP, the account is placed into this group.

- **Power Users.** This group has more privileges than a regular user but not as many as an administrator. For example, users in this group can install a printer or add a different printer driver. However, administrative privileges are required to install applications and device drivers, and the Power Users group does not have these privileges.

NOTE POWER USERS GROUP NOT NEEDED IN WINDOWS VISTA AND WINDOWS 7

The Power Users group is needed in Windows XP so that users can run some legacy applications that require some advanced privileges. Due to how User Account Control (UAC) is used in Windows Vista and Windows 7, the Power Users group isn't needed in those operating systems, but it's kept for backward compatibility.

- **Users.** Regular users are in this group. They can run typical applications but don't have privileges to make system changes.
- **Backup Operators.** Users in this group can back up and restore files.
- **Remote Desktop Users.** Users in this group are authorized to connect to the system by using Remote Desktop.

There are additional groups in different operating systems. For example, Windows Vista and Windows 7 include the Event Log Readers and Performance Monitor Users groups, which give users privileges to use the Event Viewer and Performance Monitor.

If there is a default group that provides the appropriate privileges a user needs, the user account should be placed in that group. In large networks, administrators often create additional groups. They assign appropriate privileges to these groups and place the user accounts into the groups.

For example, a company might have a sales department with multiple salespeople. An administrator might create a group called Sales, assign it privileges needed by the salespeople, and add the salespeople user accounts to this group.

Using Local Users and Groups

The Local Users And Groups tool is available in Windows XP, Windows Vista, and Windows 7 as a snap-in in the Computer Management tool. You can start Computer Management by clicking Start, Control Panel, changing to Classic View or Large Icons, opening the Administrative Tools group, and double-clicking Computer Management.

Figure 25-8 shows Computer Management open on a Windows 7-based computer, with Users selected under Local Users And Groups. The Darril Gibson account was created when Windows 7 was first installed, and the other two accounts (Administrator and Guest) are default accounts.

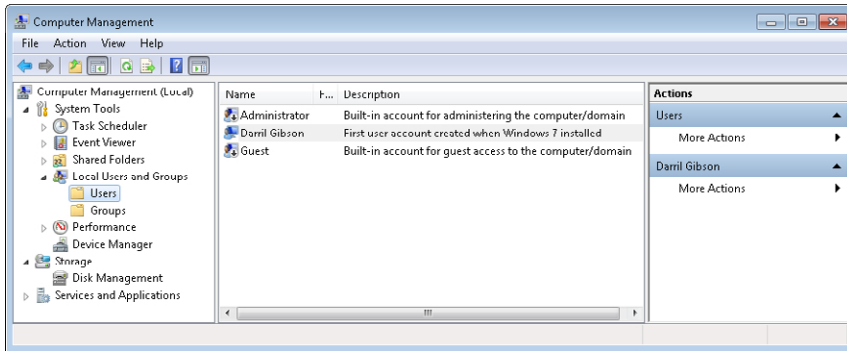


FIGURE 25-8 Local Users and Groups on Windows 7.

The Administrator and Guest accounts both have an icon of a down arrow in a circle. This is letting you know that these accounts are disabled, which is the default in Windows 7. On the right, you can see the Actions pane, which includes links to additional wizards. You can use these links to create new user accounts or to change passwords of existing accounts.

Figure 25-9 shows the three property tabs of an account. You can use the General tab to manipulate password rules and disable or enable an account. The Member Of tab shows group membership for a user account, and you can use it to view, add, or remove group membership. The Profile tab provides a method for changing the profile location.

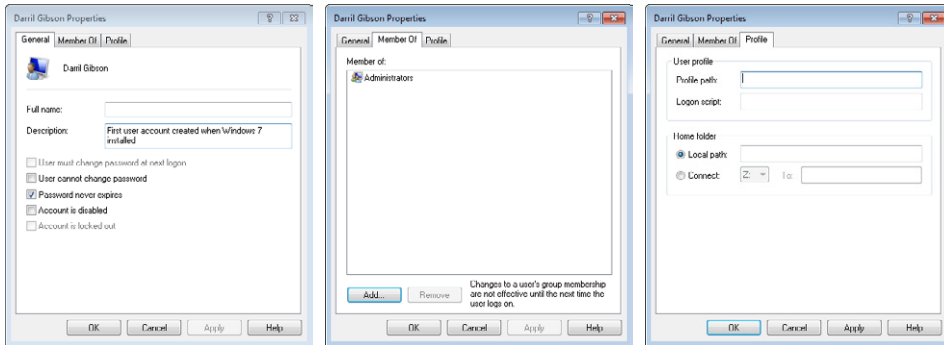


FIGURE 25-9 Viewing user properties from Local Users And Groups.

NOTE GROUP MEMBERSHIP CHANGES AREN'T REFLECTED IMMEDIATELY

A user's group membership is checked only when the user first logs on. If you make a change to the user's group membership, the user needs to log off and then back on before the changes apply to the account.

Figure 25-10 shows the groups within a Windows 7-based system with the Administrators group property page opened. You can double-click any group to view its properties. Using this property page, you can view, add, or remove individual users from a group.

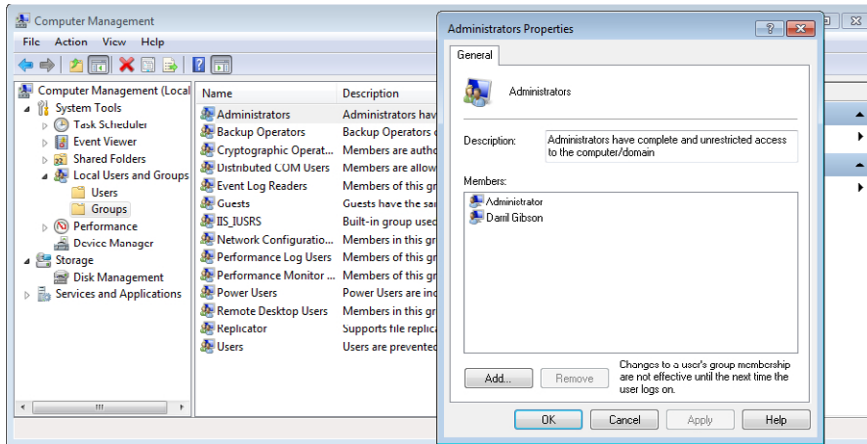


FIGURE 25-10 Viewing group properties in Local Users And Groups.

✓ Quick Check

1. What type of account has minimal privileges in Windows 7?
2. Name two tools used to modify user accounts in Windows-based systems.

Quick Check Answers

1. Standard user account.
2. User Accounts applet and Local Users And Groups in Computer Management.

Understanding Permissions

You can control who can access files and folders with permissions. Permissions are assigned to users or groups, and if users have permission from their user account or as a member of a group, they can access the resource.

For example, if you want someone to be able to read a file, you can grant read permission on the file. Permissions can be assigned to New Technology File System (NTFS) files, folders, or shares.

NOTE AUTHENTICATION VS. AUTHORIZATION

Users prove their identity with a password or some other method of authentication. This allows a user to log on. However, just because users can prove an identity doesn't mean they are automatically granted access to all resources. Instead, users are authorized access through rights and permissions assigned to their account or through group membership.

NTFS Permissions

NTFS permissions are available only on NTFS drives and not on file allocation table (FAT) drives. You can access the NTFS permissions for any file or folder through Windows Explorer by right-clicking the item, selecting Properties, and clicking the Security tab.

Figure 25-11 shows permissions assigned to a folder named A+ Study Notes on an NTFS drive. You can edit permissions by clicking the Edit button, and you'll see the dialog box shown on the right in the figure.

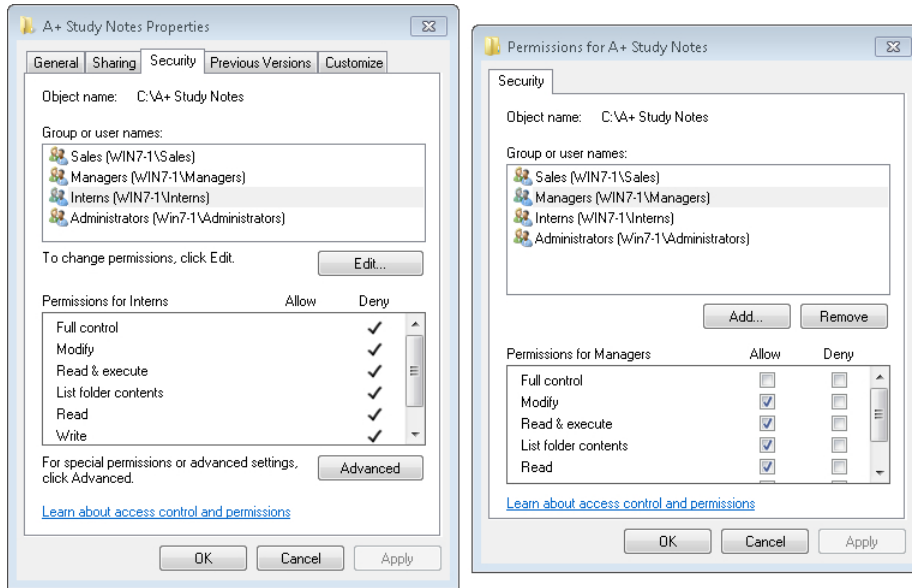


FIGURE 25-11 Viewing NTFS permissions.

NOTE ALLOW VS. DENY

Permissions can be assigned as Allow or Deny. In Figure 25-11, on the left, the Interns group is selected, and you can see that it is assigned Deny permissions on this folder so their access is blocked. On the right, the Managers group is selected, and you can see that it is assigned Allow permissions, granting access for members of this group.

The basic types of NTFS permissions are as follows:

- **Read.** Users can open files and read the contents. This does not give permission to save changes to a file.
- **Write.** Write allows a user to modify the contents of a file. It is normally assigned with the Read permission.
- **Read & Execute.** Programs require a user to have this permission to run them. It is not needed for files that are opened by a user.

- **Modify.** This is similar to read and write, with a significant addition: users can also delete files.
- **Full Control.** Full control allows the user to do anything and everything to the file. This includes the ability take ownership of files and change permissions on the files.

Combining NTFS Permissions

Permissions are most often assigned to groups, and a user can be a member of multiple groups. When this happens, the user is granted a combination of all the permissions assigned to all of the groups. This is commonly referred to as cumulative permissions.

For example, Maria is a sales manager within a company that has created groups called Sales and Managers. Maria is a member of both the Sales and Managers groups, and the permissions for a folder are assigned as follows:

- **Sales group.** Read.
- **Managers group.** Modify.

Because Maria is in both groups, she has both sets of permissions, allowing her to read and modify files within the folder.



EXAM TIP

Permissions are cumulative. When a user is granted permissions from multiple groups, the user has a combination of all the permissions.

Allow vs. Deny

In addition to granting permission with Allow, you can also explicitly block access by assigning Deny. If Deny is assigned for a user or group, it takes precedence and overrides allowed permissions.

For example, suppose a company hires sales interns and puts their user accounts in the Sales group. These users now have access to all the same data as anyone else in the Sales group. If the company wants to block the interns from accessing some files, it can assign the Deny permission for the Interns group. It would apply to users in the Interns group but to no one else.

If you look again at Figure 25-11, you'll see that the Interns group is assigned Deny for the A+ Study Notes folder. Even if one of the interns was added to the Managers group, which is granted access, the Deny takes precedence and will block the intern's access.

Permission Inheritance and Permission Propagation

Children inherit genes and sometimes huge fortunes from their parents. Permissions use inheritance as a metaphor to show that permissions assigned to parent folders are inherited by children folders and by any files within a parent folder.

Imagine that you create a folder named Study Notes. Any files or folders you create inside this folder are children, and any permissions you assign to the parent are automatically inherited by the children. This is also called permission propagation because the parent folder permissions are propagated to the children.

Figure 25-12 shows the A+ folder as a child of Study Notes and Network+ as another child of Study Notes. Similarly, the A+ folder includes several files that are children of the A+ folder. If you granted a group Full Control to the A+ folder, group members would automatically have access to all the files in that folder through permission inheritance.

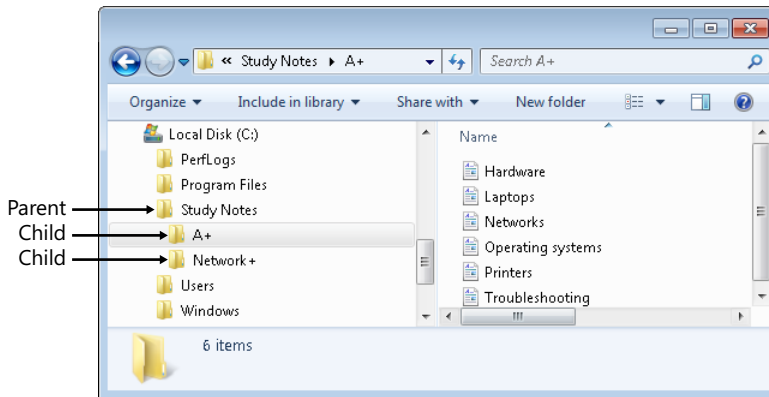


FIGURE 25-12 Inherited permissions from parent folder.

This does not give them access to the Network+ folder because the A+ and Network+ folders are both on the same level as children of the Study Notes folder. A brother doesn't inherit genes from a brother, and a child folder doesn't inherit permissions from another child folder.

What would you do if you wanted to give someone access to both the A+ and Network+ folders? One way is to assign permissions individually to each folder. An easier way is to assign permissions to the parent Study Notes folder. If you grant access to the Study Notes folder, access is granted to both the A+ and Network+ folders through inheritance.

Effect on Permissions When Copying and Moving Files

When you assign permissions directly to a file, it's important to understand how the operating system handles these permissions when you move or copy the file. For example, if you give Holly Read permission to a file named Study.doc, will she still have Read permission if you copy or move the file?

There is only one situation that results in the directly assigned permissions staying the same: when you move a file on the same partition or volume. Any other time, the permissions are inherited from the target location.



EXAM TIP

A short way to remember this is with either of the following phrases: “Move on same retains and everything else inherits” or “Move on same stays the same and everything else inherits.”

Figure 25-13 shows all of the following possibilities:

- When you move a file (drag and drop) from one folder to another folder on the same NTFS volume, the file retains the permissions. This is the only time the original permissions are retained.
- When you move a file from one NTFS volume to a folder on another volume, the file inherits the permissions of the destination folder.
- When you copy a file from a folder on an NTFS volume to another folder on the same volume, the file inherits the permissions of the destination folder.
- When you copy a file from a folder on an NTFS volume to a folder on another NTFS volume, the file inherits the permissions of the destination folder.









	Original location	New location	Effect on permissions
Move on same partition			Stay the same
Move to different partition			Inherited from new location
Copy on same partition			Inherited from new location
Copy to different partition			Inherited from new location

FIGURE 25-13 Effect on permissions when moving or copying files.



EXAM TIP

The only time that directly assigned permissions stay the same is when the file is moved on the same partition or volume. Remember that a partition and a volume refer to the same thing. Moving a file from C:\Data to C:\New can be referred to as moving a file on the same partition or moving a file on the same volume. Permissions are not supported on FAT volumes, so if you move or copy a file to a FAT volume, all permissions are lost.

File Attributes

Files have attributes that describe them such as hidden, read-only, and system. These work in conjunction with permissions, but they aren't the same.

For example, if a file is marked as read-only, the operating system prevents anyone from making modifications to the file. If you remove the read-only attribute, it can be modified.

In contrast, permissions are more selective. You can assign one group Read and Write permission for a file and assign another group only Read permission. Attributes apply to all users universally, but permissions can be applied to users and groups differently.

MORE INFO CHAPTER 14, “USING THE COMMAND PROMPT”

Chapter 14 shows how to use the `attrib` command to view and modify attributes from the command prompt.

Share Permissions

Shares are folders on other network computers that are accessible over the network. You can assign permissions to these shares, and they interact with NTFS to allow or block access.

MORE INFO CHAPTER 16, “UNDERSTANDING DISKS AND FILE SYSTEMS”

Chapter 16 covers shares in more depth, including administrative shares and regular shares. Only folders can be shared. When shared, all the files and subfolders within the share are accessible over the network by using a Universal Naming Convention (UNC) path in the format of `\\ServerName\ShareName`.

There are only three Share permissions, described in the following list, and each can be assigned as Allow or Deny:

- **Full Control.** This is the same as the NTFS Full Control permission. Users with full control permission can do anything with files within the share.
- **Change.** This is similar to the NTFS Modify permission. It allows users to read and modify files.
- **Read.** When a share is created, this is the default permission assigned.

Share permissions are cumulative, just as they are with NTFS. If a user is granted Read and Change permissions, the user has Change permission that includes Read. The permissions don't cancel each other.

The exception is when Deny is assigned. Just as Deny takes precedence in NTFS, Deny takes precedence with Share permissions. If a user is assigned Deny Read, it doesn't matter how many groups grant the user Allow Read. Deny overrides the Allow permission, and access is blocked.

Shares are accessed only over a network. If you access the folder on your local computer, you are accessing the folder, not the share. If you access the folder, the Share permissions do not apply.

Combining NTFS and Share Permissions

When you access a file within a share that is on an NTFS drive, both the NTFS and the Share permissions apply. In this case, the permissions are not cumulative. You can use the following three simple steps to determine what the ultimate permissions are for a file within the share:

- 1. Identify the combined NTFS permissions.** For example, if a user is a member of multiple groups and is granted Read permission as a member of one group and Full Control permissions as a member of the second group, the user is granted a combination of both Read and Full Control permissions. In this case, Full Control includes Read, so it's appropriate to say that the combined NTFS permissions are Full Control.
- 2. Identify the combined share permissions.** Similarly, if a user is a member of multiple groups granting the user Read as a member of one group and Change as a member of the second group, the user is granted a combination of both Read and Change permissions. In this case, Change includes Read so it's appropriate to say that the combined share permissions are Change.
- 3. Identify the lower permission of the two.** Which provides less access? Full Control from the combined NTFS permission or Change from the combined Share permissions? Change is less than Full Control, and that's the ultimate permission.

The default permission when you create a share is Read for the Everyone group. Unless you change this, users will be able to only read the files in the share. It doesn't matter what type of NTFS permissions they have. A user with Full Control NTFS permissions and Read share permissions is granted only Read permission when accessing files through the share.

NOTE LEAST RESTRICTIVE AND MOST RESTRICTIVE

Combining NTFS and Share permissions is often described as using the least restrictive and most restrictive permissions. First, you combine the NTFS permissions to identify the least restrictive NTFS permission, which is Full Control in the preceding explanation. Next, you combine the Share permissions to identify the least restrictive Share permission, which is Change in the explanation. Last, you identify which is most restrictive between the two. Change is more restrictive than Full Control, so Change is the applied permission.

Quick Check

1. What permissions will a user have when the user is a member of two groups?
2. When do permissions stay the same when a file is moved or copied?

Quick Check Answers

1. A combination of permissions from both groups.
2. Only when moved on the same partition or volume.

Understanding Encryption

Encryption is the process of converting plain text data into cipher text that is unreadable. Decryption converts cipher text back into plain text so that it is readable. The primary goal is to keep secret data secret. Security professionals refer to this as preventing loss of confidentiality by preventing unauthorized access.

The two primary times when encryption methods are applied are as follows:

- **Data at rest.** Whenever data is stored on media, it is at rest. This includes data stored on hard drives, optical media, and USB flash drives. You can encrypt individual files and folders with NTFS Encrypting File System (EFS). Similarly, you can encrypt entire partitions with BitLocker.
- **Data in motion.** When data is transferred over a network, it is in motion. Network protocols such as Secure Shell (SSH), Secure Sockets Layer (SSL), and Transport Layer Security (TLS) are used to encrypt data in motion. Wireless networks also use encryption to protect some transmitted data.

The Advanced Encryption Standard (AES) is commonly used in many different security applications to encrypt both data at rest and data in motion. It has replaced the older Data Encryption Standard (DES), which is no longer considered secure.

MORE INFO CHAPTER 20 AND CHAPTER 23

Chapter 20, “Understanding Protocols,” covers encryption protocols. For example, SSH is used with Secure File Transfer Protocol (SFTP) and Secure Copy (SCP) to encrypt data sent over a network. Chapter 23, “Exploring Wireless Networking,” covers the wireless protocols used to encrypt data.

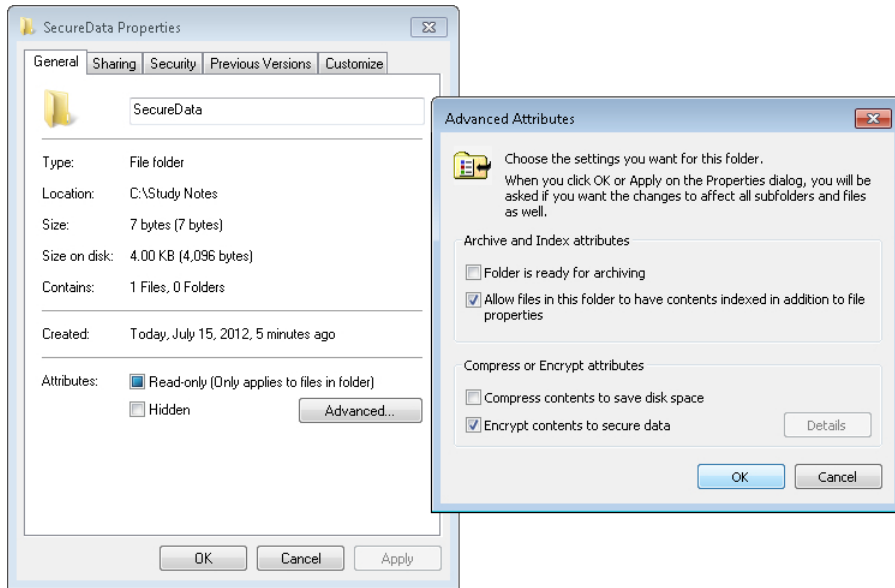
Encrypting Files with EFS



Windows operating systems using NTFS include *Encrypting File System (EFS)*, which you can use to encrypt files and folders. When an authorized user accesses an encrypted file, the operating system automatically decrypts the file and opens it. When a user saves a file that was originally encrypted, the operating system automatically encrypts it again.

You can use the following steps to encrypt a folder on a Windows 7 NTFS drive:

1. Open Windows Explorer by clicking Start, Computer.
2. Browse to the drive and folder that you want to encrypt.
3. Right-click the folder you want to encrypt and select Properties. If necessary, click the General tab.
4. Click Advanced. Select Encrypt Contents To Secure Data. Your display will look similar to the following graphic. Click OK.



NOTE ENCRYPT OR COMPRESS

Files and folders can be encrypted or compressed, but they cannot be encrypted and compressed at the same time. Only one choice is allowed at a time.

5. Click OK again. On the Confirm Attribute Changes dialog box, ensure that Apply Changes To This Folder, Subfolders And Files is selected and click OK. This ensures that all folders within the folder will also be encrypted.

The folder appears green in color. Any new files you create in this folder and any files that you copy or move into it will also be encrypted. If you set compression instead of encryption, the folder will be blue. Files can be green, indicating that they're encrypted, or blue, indicating that they are compressed, but they can't be both green and blue at the same time. More specifically, they can't be compressed and encrypted at the same time.

EFS uses certificates in the encryption and decryption process. The operating system automatically creates a certificate the first time a user encrypts a file, and this certificate includes cryptographic keys. The certificate is accessible only to the user, and when the user opens a file, the operating system retrieves the certificate to decrypt it.

This brings up an important point. If you move encrypted files from one computer to another, they can't be decrypted unless you also move the user's certificate. You need to export the certificate from the original computer and then import it on the new computer.

On Windows 7, you can use the User Accounts applet and click Manage Your File Encryption Certificates to access wizards to help with the process. Technet includes an article, "Manage Certificates," which includes information about exporting a certificate from one

computer and importing it on another computer. You can access it here: <http://technet.microsoft.com/library/cc771377>.



EXAM TIP

NTFS uses certificates for encryption. If encrypted files are moved, the certificates must also be moved to ensure that the files are accessible on the target system.

Offline Files Encryption

The Offline Files feature allows users to access files even when users are away from the network, and it is useful for laptop users. Imagine that Server1 hosts files within a share, and Holly uses her laptop computer to access the files when her laptop computer is connected to the work network.

When the Offline Files feature is enabled, the files are also copied onto Holly's laptop. She can access these files even when she's away from work and not connected to the network.

If these files include sensitive data, they can be protected with encryption. If the user's laptop is lost or stolen, encryption helps prevent unauthorized individuals from viewing the data.

The Offline Files feature includes the ability to encrypt offline files but requires different steps to access them on different operating systems.

- On Windows XP, start the Folder Options applet from the Control Panel. Click the Offline Files tab and click Encrypt Offline Files To Secure Data.
- On Windows Vista, start the Offline Files applet from the Control Panel. Click the Encryption tab and click Encrypt.
- On Windows 7, start the Sync Center from the Control Panel and click Manage Offline Files. Click the Encryption tab and click Encrypt.

BitLocker Drive Encryption

BitLocker Drive Encryption is a Windows feature that can encrypt the entire volume. This makes it difficult for unauthorized individuals to access data if they are able to steal a hard drive.

If you protect files on a drive by using NTFS permissions, they can't easily be accessed. However, an administrator can take ownership of the files and change the permissions. With this in mind, a thief can be an administrator on a computer he owns. He can install a stolen hard drive as a second drive on his computer, take ownership of the files, and change their permissions.

Disk drives protected with BitLocker Drive Encryption are protected from this type of attack. When the drive is moved to another system, they remain encrypted and unreadable.

BitLocker uses a Trusted Platform Module (TPM) when available. A TPM is a chip on the motherboard, and it often needs to be enabled in the BIOS. If a TPM is not available,

BitLocker can be used with a PIN that the user enters when the computer starts or with a USB flash drive that includes a startup key and is inserted when the computer is started.

BitLocker To Go is a feature available in Windows 7 that allows you to encrypt data on removable disks, such as a USB flash drive. It uses AES and provides strong encryption.

MORE INFO BITLOCKER

If you want to dig a little deeper into BitLocker, check out the following links:

- BitLocker Drive Encryption: <http://windows.microsoft.com/en-us/windows-vista/BitLocker-Drive-Encryption-Overview>.
- Windows BitLocker Drive Encryption Step by Step Guide: <http://go.microsoft.com/fwlink/?LinkId=53779>.
- BitLocker and BitLocker To Go video: <http://technet.microsoft.com/en-us/windows/bitlocker-and-bitlocker-to-go.aspx>.

Quick Check

1. What is used to encrypt individual files?
2. What is required to support BitLocker?

Quick Check Answers

1. EFS, which is part of NTFS.
2. A TPM. As an alternative, you can use a PIN or a USB.

Destruction and Disposal of Data and Media

When media such as hard drives, backup tapes, CDs, and DVDs reach the end of their life cycle, they should be destroyed or disposed of properly. This includes when a computer is donated, recycled, returned to the vendor at the end of a lease, or simply thrown away. The primary goal is to ensure that the data doesn't fall into the wrong hands.



Sanitization is the process of removing all usable data from media. The ultimate form of sanitization is physical destruction.

There are many different methods of sanitizing media, and organizations commonly have procedures in place for destruction and disposal. The sensitivity of the data often dictates which method is used. For example, you might need to destroy a disk drive that has highly classified material but only need to erase data from another drive.

Hard Drive Sanitization

If you need to dispose of a hard drive, you should ensure that it does not have any data that could be valuable to someone else. In some cases, you can use software tools to sanitize a hard drive. Software tools overwrite the drive to remove all remnants of the data. Hardware tools are used to destroy the drive.

Deleting Files

It's relatively easy to delete files in Windows. You can browse to the file by using Windows Explorer, right-click the file, and select Delete. However, even though you've selected Delete, the file isn't actually deleted.

Most people know about the Recycle Bin available in Windows. If you accidentally delete a file, you can go into the Recycle Bin, locate the file, right-click it, and select Restore.

However, even when it's deleted from the Recycle Bin, the file is not actually totally deleted. File systems use a table to identify the location of files. When you delete a file, you're deleting only the entry in the table. This is similar to the index in the back of a book that you can use to find a topic. If the index entry is deleted, the topic still remains in the book; it's just a little harder to find.

Many undelete tools are available that can locate deleted files and add them back to the file system table. If you have data that you don't want anyone else to access, you need to do more than just delete it. Other tools are available to completely remove the files.

Overwrite and Drive Wipe Tools



Data is written as magnetized fields on a hard drive, and even when a file is deleted and overwritten, some magnetism of the original data remains. This is often called data *remanence*. Specialized forensics tools can locate and recover this data.

Software tools are available that will overwrite deleted files to remove all data remnants. For example, Unix includes a utility called *shred* that can overwrite individual files or entire disk drives. It overwrites the file at least three times with multiple patterns.

Some tools write a pattern of 1s and 0s (such as 1001 1100) in the first pass and then write the complement of the pattern (0110 0011 in this example) in a second pass. The last pass writes random bits.



EXAM TIP

Deleting a file doesn't truly erase it. Overwriting a file multiple times with different bit patterns is a secure method of deleting a file.

Low-Level Format vs. Standard Format

Hard drives start as platters with ferromagnetic material that isn't organized in any way. Manufacturers perform a low-level format of the hard drives at the factory to define the positions of the tracks and sectors. Later, users perform a standard format to prepare the disk with a file system like NTFS.

It's unlikely that you'll ever perform a true low-level format of a hard disk drive. However, the process of writing zeros onto the disk will erase the disk and is often referred to as a low-level format.

A zero-fill program sanitizes a disk drive by filling every sector with zeros. The `dd` command in Unix is used for copying data at the bit level, and it can be used as a zero-fill program.

NOTE LOW-LEVEL FORMAT VS. WRITING ZEROS

Over 20 years ago, end users occasionally needed to perform low-level formats due to disk aging problems. These problems never occur on current disks, so the low-level format performed at the factory never needs to be repeated. However, applications that write zeros (zero-fill programs) are sometimes referred to as low-level format programs. These are not the same as the factory low-level format, but they will erase all data on the drive.

Hard drive manufacturers often provide hard drive utilities that include a zero-fill utility. For example, Western Digital offers utilities that work with its drives. The knowledge base article titled "How to low level format or write zeros (full erase) to a WD hard drive or Solid State drive" describes the full process and includes download links. You can view it here: http://wdc.custhelp.com/app/answers/detail/a_id/1211.

A standard format prepares the hard drive for file storage and is performed by users within an operating system. For example, you can format a hard drive by using Disk Management or the `format` command.

MORE INFO CHAPTER 16, "UNDERSTANDING DISKS AND FILE SYSTEMS"

Chapter 16 provides steps for formatting a disk drive by using Disk Management and the `format` command. A standard format can be either quick or full. The full format checks the sectors and marks faulty sectors as bad so that they aren't used. It is not a low-level format.

Just as there are undelete tools that can undelete files, there are also unformat tools that can unformat hard drives. An important point to realize is that a standard format is not an effective method of sanitizing a drive.

Physical Destruction

Although many of the methods for sanitizing media can be effective, they are all susceptible to problems or errors. For example, an undetected software bug might prevent the complete erasure of data or the person running the program might make a mistake.

When media holds extremely sensitive or top secret data, an organization often chooses to eliminate any of these risks. Instead of using tools to erase the data, the organization destroys the media.

Shredder

Shredders are commonly used to destroy paper and can also be used to destroy some media. Some small shredders used in small offices/home offices (SOHOs) might be able to shred a CD, but they are rarely good enough to shred a thicker DVD or Blu-ray disc.

Some companies, such as Shred-it, have mobile trucks with industrial-sized shredders inside the truck and they can shred materials at the customer's location. In addition to paper, these companies can also shred any type of hard drive from desktop and laptop computers, magnetic tapes, floppy disks, and optical media.

NOTE CROSSCUT SHREDDERS

A simple strip shredder cuts paper into strips and is not suitable for destruction. A dumpster diver can retrieve the strips from the garbage and put them back together. Crosscut or confetti shredders cut in more than one direction to create small pieces of paper similar to confetti. Higher-quality crosscut shredders create extremely small particles of paper.

Degaussing Tool (Magnet and Electromagnetic)



Hard drives store data by magnetizing ferromagnetic material on the platters. A *degaussing tool* exposes the drive to a strong magnetic field, scrambling the data. Similarly, degaussing tools erase data from magnetic tapes. There are two types of degaussing tools:

- **Permanent magnet.** A strong permanent magnet is used to create the magnetic field.
- **Electromagnetic.** Electricity is sent through a coil to generate strong magnetic fields.

Degaussing is an effective method of sanitizing damaged hard drives, but you shouldn't use it on a drive that you want to use again. The magnetic fields that erase the data will also destroy the hard drive.



EXAM TIP

Degaussing is an effective method of sanitizing hard drives and tapes, but it has no effect on non-magnetic media. You cannot use it on optical media such as CDs and DVDs.

Drilling, Sanding, and Grinding

Drills, sanders, and grinders are sometimes used to destroy media. Drilling several holes through the platters makes a disk unusable and is sometimes considered a suitable method of destroying the media. Electric sanders and grinders completely remove all of the magnetic material, ensuring that there is nothing left on the disk.



Quick Check

1. What type of format erases data on a disk?
2. Name two methods of physical destruction.

Quick Check Answers

1. A low-level format or writing zeros.
2. Shredding, degaussing, and drilling are possible answers.

Chapter Summary

- Security methods attempt to prevent incidents, detect them when they occur, and respond to quickly contain them. User education is an important prevention method.
- The principle of least privilege ensures that users are granted only the privileges they need for their job.
- Users prove who they are with authentication. Passwords are used most often but are the weakest form of authentication. Tools such as the Local Security Policy ensure that users create strong passwords with multiple character types.
- Badges and smart cards provide strong authentication when combined with another authentication method, such as a PIN or a password. Biometric authentication is the strongest method, and retinal scans are the strongest form of biometric authentication.
- Single sign-on allows users to log on once and access multiple resources without logging on again.
- Windows XP includes a limited user account and a computer administrator account. Similarly, Windows Vista and Windows 7 use a standard user account and an administrator account.
- You can create and modify accounts with the User Accounts applet or the Local Users And Groups snap-in available in Computer Management.
- Privileges are granted to users when the account is added to a group. Users can be in multiple groups and have a combination of all the privileges assigned to the groups.

- NTFS permissions are assigned on NTFS volumes. When assigned to a folder, the folder is the parent and the permissions are inherited by files and subfolders with the parent folder.
- Permissions can be assigned as Allow or Deny. When a user is assigned multiple Allow permissions, the result is a combination of all. When Deny is assigned, it takes precedence and blocks any Allow permission.
- Share permissions apply to shared folders only when the share is accessed over the network. They do not apply when the folder is accessed locally.
- Files and folders can be encrypted with EFS. An encrypted file appears green. If EFS files are copied to another computer, the EFS certificate should also be copied.
- BitLocker Drive Encryption encrypts entire hard drives. It can be used with a TPM, a PIN, or a USB flash drive.
- Media should be sanitized prior to disposal. One method of sanitizing media is by using programs that overwrite it with repeating patterns of bits. Media can also be destroyed by using shredders, by using degaussing tools, and by drilling holes in the media.

Chapter Review

Use the following questions to test your knowledge of the information in this chapter. The answers to these questions, and the explanations of why each answer choice is correct or incorrect, are located in the “Answers” section at the end of this chapter.

1. Which one of the following passwords is the strongest?
 - A. apluscertified
 - B. IPassedAPlus
 - C. IPa\$\$ed!!
 - D. IPa\$\$ed801
2. Which of the following provides the strongest authentication?
 - A. Strong passwords
 - B. Retinal scans
 - C. Smart cards
 - D. RSA tokens

- 3.** A user was first assigned as a member of the Sales group and later added to the Managers group. What are the effective permissions of the user?
 - A.** Only permissions assigned to the Sales group.
 - B.** Only permissions assigned to the Managers group.
 - C.** A combination of permissions from both groups.
 - D.** Only permissions granted to both groups.

- 4.** Of the following choices, when will directly assigned permissions stay the same?
 - A.** When a file is copied to a new location on a volume.
 - B.** When a file is copied to a different volume.
 - C.** When a file is moved to a new location on a volume.
 - D.** When a file is moved to a different volume.

- 5.** What is the benefit of encrypting data with NTFS?
 - A.** It helps prevent unauthorized users from viewing it.
 - B.** It helps prevent unauthorized users from copying it.
 - C.** It ensures that the data stays hidden.
 - D.** It ensures that the data is not modified.

- 6.** Which of the following methods provides the strongest sanitization of a hard disk?
 - A.** Formatting the disk with the format command.
 - B.** Low-level format writing zeros.
 - C.** Physical destruction.
 - D.** Deletion of individual files.

Answers

This section contains the answers to the chapter review questions in this chapter.

- 1. Correct Answer: D**
 - A. Incorrect:** `apluscertified` uses only one character type (lowercase) and is the weakest.
 - B. Incorrect:** `IPassedAPlus` uses only two character types.
 - C. Incorrect:** `IPa$$ed!!` uses only three character types.
 - D. Correct:** `IPa$$ed801` is the strongest because it uses all four character types (uppercase, lowercase, special characters, and numbers).

- 2. Correct Answer: B**
 - A. Incorrect:** Passwords are the weakest form of authentication.
 - B. Correct:** A retinal scan is a biometric method of authentication, and it is the strongest.
 - C. Incorrect:** Smart cards are strong when combined with a second method but are not very strong when used alone.
 - D. Incorrect:** RSA tokens are strong when combined with a second method but are not very strong when used alone.

- 3. Correct Answer: C**
 - A. Incorrect:** It does not matter when permissions are granted. The fact that the user was added to the Sales group first is not relevant.
 - B. Incorrect:** Permissions are not limited to just one group.
 - C. Correct:** When a user is a member of multiple groups, the user has a combination of permissions from all groups.
 - D. Incorrect:** Permissions are not limited if a user is added to another group.

- 4. Correct Answer: C**
 - A. Incorrect:** Permissions are inherited from the new location when a file is copied to a new location.
 - B. Incorrect:** Permissions are inherited from the new location when a file is copied to a different volume.
 - C. Correct:** The only time directly assigned permissions stay the same is when files are moved on the same volume.
 - D. Incorrect:** Permissions are inherited from the new location when a file is moved to a different volume.

5. Correct Answer: A

- A. Correct:** Encryption scrambles data so that unauthorized users are unable to view it.
- B. Incorrect:** Encryption doesn't prevent copying.
- C. Incorrect:** Encryption doesn't hide data.
- D. Incorrect:** Encryption doesn't stop authorized users from modifying data.

6. Correct Answer: C

- A. Incorrect:** An operating system format does not sanitize a drive because the process can be reversed.
- B. Incorrect:** A low-level format writing zeroes is a strong method of sanitization but not as strong as destruction.
- C. Correct:** Physical destruction is the ultimate form of sanitization.
- D. Incorrect:** Deleting files isn't reliable unless a tool is used to overwrite the files multiple times.