LESSON 2

# Understanding Authentication, Authorization, and Accounting

## OBJECTIVE DOMAIN MATRIX

| Skill/Concept | Exam Objective | Objective Number |
|---|---|---|
| Starting Security with Authentication | Understand user authentication | 2.1 |
| Introducing Directory Services with Active Directory | Understand user authentication | 2.1 |
| Comparing Rights and Permissions | Understand permissions | 2.2 |
| Understanding NTFS | Understand permissions | 2.2 |
| Sharing Drives and Folders | Understand permissions | 2.2 |
| Introducing the Registry | Understand permissions | 2.2 |
| Using Encryption to Protect Data | Understand encryption | 2.5 |
| Understanding IPsec | Understand protocol security | 3.3 |
| Introducing Smart Cards | Understand user authentication | 2.1 |
| Configuring Biometrics, Windows Hello, and Microsoft Passport | Understand user authentication | 2.1 |
| Using Auditing to Complete the Security Picture | Understand audit policies | 2.4 |

## KEY TERMS

**access control list (ACL)**
**accounting**
**Active Directory**
**administrative share**
**asymmetric encryption**
**auditing**
**authentication**
**authorization**
**biometrics**
**BitLocker To Go**
**brute force attack**
**built-in group**
**certificate chain**
**certificate revocation list (CRL)**
**computer account**
**decryption**
**dictionary attack**
**digital certificate**
**digital signature**
**domain controller**
**domain user**

**effective permissions**
**encryption**
**explicit permission**
**group**
**hash function**
**inherited permission**
**IP Security (IPsec)**
**Kerberos**
**key**
**local user account**
**member server**
**Microsoft Passport**
**multifactor authentication**
**nonrepudiation**
**NTFS**
**NTFS permissions**
**NTLM**
**organizational unit (OU)**
**owner**
**password**
**permission**
**personal identification number (PIN)**
**public key infrastructure (PKI)**
**registry**
**right**
**Secure Sockets Layer (SSL)**
**Security Account Manager (SAM)**
**security token**
**share permissions**
**shared folder**
**single sign-on (SSO)**
**smart card**
**symmetric encryption**
**Syslog**
**Trusted Platform Module (TPM) chip**
**user account**
**virtual private network (VPN)**
**virtual smart card (VSC)**
**Windows Biometric Framework (WBF)**
**Windows Hello**

The CIO for your company wants to discuss security. He asks which system is in place to ensure that users can access only what they need to access and nothing else. You respond by saying that the security model was built using the three A's—authentication, authorization, and accounting. He wants to know more about this model.

## ■ Starting Security with Authentication

THE BOTTOM LINE

In the realm of IT security, the AAA (Authentication, Authorization, and Accounting) acronym is a model for access control. ***Authentication*** is the process of identifying an individual, usually based on a user name and password. After a user is authenticated, the user can access network resources based on the user's authorization. ***Authorization*** is the process of giving individuals access to system objects based on their identity. ***Accounting***, also known as ***auditing***, is the process of keeping track of a user's activity while accessing the network resources, including the amount of time spent in the network, the services accessed while there, and the amount of data transferred during the session.

***Nonrepudiation*** prevents one party from denying actions they carry out. If proper authentication, authorization, and accounting have been established, a person cannot deny their own actions.

Before any user can access a computer or a network resource, the user will most likely log on to prove their identity and to see if they have the required rights and permissions to access the network resources.

**CERTIFICATION READY**
Which methods are used for authentication?
Objective 2.1

A logon is the process whereby a user is recognized by a computer system or network so that they can begin a session. A user can authenticate using one or more of the following methods:

- What a user knows, such as a password or personal identification number (PIN)
- What a user owns or possesses, such as a passport, smart card, or ID card
- Who a user is, based on biometric factors such as fingerprints, retinal scans, voice input, or other forms

When two or more authentication methods are used to authenticate someone, a ***multifactor authentication*** system is being implemented. A system that uses two authentication methods such as smart cards and a password can be referred to as a two-factor authentication.

## Authentication Based on What a User Knows

The most common method of authentication with computers and networks is the password. A ***password*** is a secret series of characters that enables a user to access a file, computer, or program.

### USING PASSWORDS

Hackers will try to crack passwords by first trying obvious passwords, including the name of spouse/partner or children, birthdays, keywords used by the user, hobbies of the user, and common passwords. Then hackers will try ***brute force attacks***, which consist of trying as many combinations of characters as time and money permit. A subset of the brute force attack is the ***dictionary attack***, in which all words in one or more dictionaries are tested. Lists of common passwords are also typically tested.

To make a password more secure, choose a password that nobody can guess. It should be lengthy and should be considered a strong or complex password. For more information about creating strong passwords, visit the following website:

https://blogs.microsoft.com/microsoftsecure/2014/08/25/create-stronger-passwords-and-protect-them/

Because today's computers are much more powerful, some people recommend that passwords should be at least 14 characters in length. However, for some people, remembering long passwords is cumbersome, so they may start writing their passwords on a piece of paper near their desk. In these situations, you should start looking for other forms of authentication, such as a smart card or biometrics.

Remember to change passwords regularly, so that if a password is revealed to someone else, it will have been changed before they can attempt to use it. In addition, this shortens the time that someone has to guess a password, because they will need to try all over again.

Microsoft includes password policy settings within group policies to enforce a minimum number of characters, specify if the password is a complex password, suggest how often a user must change his password, state how often a user can reuse a password, and so on.

While passwords are the easiest method of authentication to implement and are the most popular authentication method, passwords have significant disadvantages because they can be stolen, spoofed, forgotten, and so on. A hacker may use social engineering where he calls the IT department for support and pretends to be someone else, so that the IT department will reset the password for the hacker. Therefore, establish a secure process to reset passwords for users.

One method of establishing a self-service password service is where a user's identity is verified by asking questions and comparing the answers to previously stored responses, such as the person's birthday, name of their favorite movie, name of a pet, and so on. However, these can be relatively easily guessed by an attacker, discovered though low-effort research or social engineering.

When resetting passwords, there must be a method to identify the user asking for a password to be changed. Don't send the password through email, because if the password is compromised, the new password may be read, and if the user does not know the password, she would still not be able to retrieve it. Meeting with the person and asking for identification is a possible solution. Unfortunately, with large networks and networks that contain multiple sites, this may not be plausible. Another solution would be to call back and leave the password on a person's voice mail, so that a user will need to provide a PIN to access, or the password could be sent to a user's manager or administrative assistant. In either case, the user should reset the password immediately after they log on.

### USING A PERSONAL IDENTIFICATION NUMBER (PIN)

A ***personal identification number (PIN)*** is a secret numeric password shared between a user and a system that can be used to authenticate the user to the system. Because it only consists of digits and is relatively short (usually four digits), it is used for relatively low security scenarios like gaining access to the system or in combination with another method of authentication.

## Authentication Based on What a User Owns or Possesses

Another type of authentication is based on what a user owns or possesses. The most common examples are the digital certificate, smart card, and security token.

The ***digital certificate*** is an electronic document that contains an identity such as a user or organization and a corresponding public key. Because a digital certificate is used to prove a person's identity, it can be used for authentication. Think of a digital certificate as a driver's license or passport that contains a user's photograph and thumbprint, so that there is no doubt about the user's identity.

A ***smart card*** is a pocket-sized card with embedded integrated circuits consisting of non-volatile memory storage components, and perhaps, dedicated security logic. Non-volatile memory is memory that does not forget its contents when power is discontinued. Smart cards can contain digital certificates to prove the identity of someone carrying the card and may also contain permissions and access information. Because a smart card can be stolen, some smart cards will not have any markings on them, so that they cannot be easily identified as to what they can open. In addition, many organizations will use a password or PIN in combination with the smart card.

A ***security token*** (or sometimes a hardware token, hard token, authentication token, USB token, cryptographic token, or key fob) is a physical device that an authorized user of computer services is given to ease authentication. Hardware tokens are typically small enough to be carried in a pocket and are often designed to attach to a user's keychain. Some of these security tokens include a USB connector, RFID functions, or Bluetooth wireless interface to enable transfer of a generated key number sequence to a client system. Some security tokens may also include additional technology such as a static password or digital certificate built into the security token, much like a smart card. Other security tokens may automatically generate a second code that will have to be entered to get authenticated.

## Authentication Based on a User's Physical Traits

***Biometrics*** is an authentication method that identifies and recognizes people based on voice recognition or a physical trait such as a fingerprint, face recognition, iris recognition, or retina scan. Many mobile computers include a fingerprint scanner, and it is relatively easy to install biometric devices at doors and cabinets to ensure that only authorized people will enter a secure area.

Biometric devices require a biometric reader or scanning device, software that converts the scanned information into digital form and compares match points, and a database that stores the biometric data for comparison.

To initially use the biometric system, set up an enrollment station where an administrator enrolls each user, which includes scanning the biometric feature to be used for authentication. When selecting a biometric method, consider its performance, difficulty, reliability, acceptance, and cost. In addition, look at the following issues:

- **False rejection rate (false negative):** Authorized users who are incorrectly denied access
- **False acceptance rate (false positive):** Unauthorized users who are incorrectly granted access

## Introducing RADIUS and TACACS+

Remote Authentication Dial-In User Service (RADIUS) and Terminal Access Controller Access-Control System Plus (TACACS+) are two protocols that provide centralized authentication, authorization, and accounting management for computers to connect to and use a network service.

The RADIUS or TACACS+ server resides on a remote system and responds to queries from clients such as VPN clients, wireless access points, routers, and switches. The server then authenticates a user name/password combination (authentication), determines if a user can connect to the client (authorization), and logs the connection (accounting).

RADIUS is a mechanism that allows authentication of dial-in and other network connections including modem dial-up, wireless access points, VPNs, and web servers. As an Internet Engineering Task Force (IETF) standard, RADIUS has been implemented by most of the major operating system manufacturers, including Microsoft Windows.

In Windows Server 2008, Network Policy Server (NPS) can be used as a Remote Authentication Dial-In User Service (RADIUS) server to perform authentication, authorization, and accounting for RADIUS clients. It can be configured to use a Microsoft Windows NT Server 4.0 domain, an Active Directory Domain Services (AD DS) domain, or the local Security Accounts Manager (SAM) user accounts database to authenticate user credentials for connection attempts. NPS uses the dial-in properties of the user account and network policies to authorize a connection.

Another competing centralized AAA server is TACACS+, which was developed by Cisco. When designing TACACS+, Cisco incorporated much of the existing functionality of RADIUS and extended it to meet their needs. From a feature viewpoint, TACACS+ can be considered an extension of RADIUS.

## Running Programs as an Administrator

Because administrators have full access to a computer or the network, it is recommended that a standard non-administrator user should perform most tasks, such as reading reports and sending email. Then, to perform administrative tasks, use the runas command or built-in options that are included with the Windows operating system.

Before Windows Vista, an administrator account was needed to do certain things, such as changing system settings or installing software. When logged on as a limited user, the runas command eliminated the need to log off and then log back on as an administrator. For example, to run the widget.exe as the admin account, execute the following command:

```
runas /user:admin /widget.exe
```

In newer versions of Windows, including Windows 10 and Windows Server 2016 R2, the runas command has been changed to Run as administrator. With User Account Control (UAC), the Run as administrator command is rarely used, because Windows automatically prompts for an administrator password when needed.

**MORE INFORMATION**

Refer to Lesson 5 for a more detailed discussion of User Account Control (UAC).

### RUN A PROGRAM AS AN ADMINISTRATOR

**GET READY.** To run a program as an administrator, perform the following steps.

1. Right-click the program icon or file that you want to open and choose **Run as administrator**. If you want to right-click an item in the Start menu, right-click the program's icon, choose **More**, and then click **Run as administrator**. See Figure 2-1.

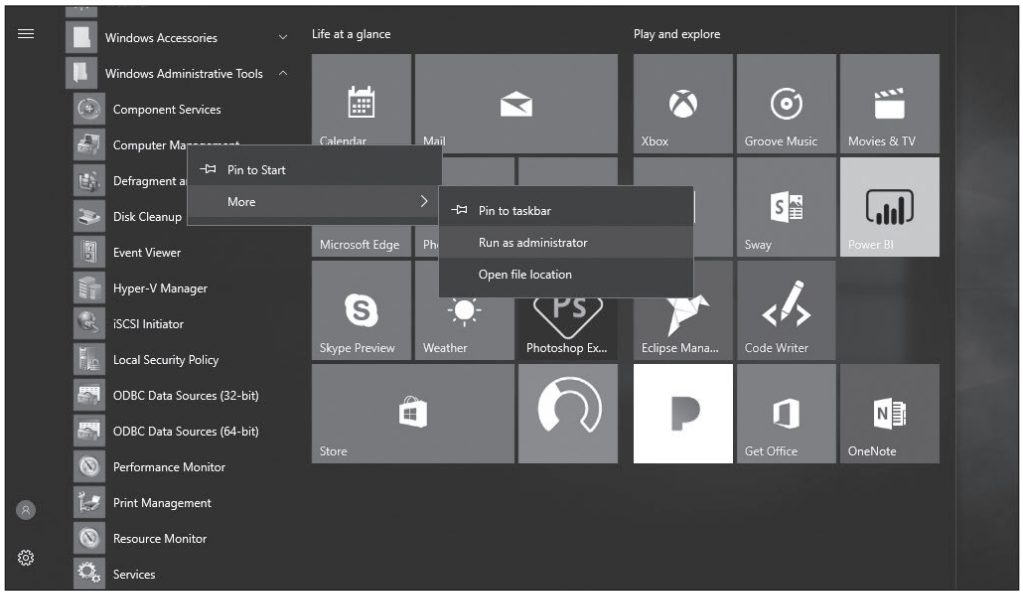



**Figure 2-1**

Using the Run as administrator option

2. Select the administrator account that you want to use, type the password, and then click **Yes**.

# ■ Introducing Directory Services with Active Directory

THE BOTTOM LINE

A directory service stores, organizes, and provides access to information in a directory. It is used for locating, managing, and administering common items and network resources, such as volumes, folders, files, printers, users, groups, devices, telephone numbers, and other objects. A popular directory service used by many organizations is Microsoft's Active Directory.

**CERTIFICATION READY**
What is the Active Directory primary method for authentication?
Objective 2.1

***Active Directory*** is a technology created by Microsoft that provides a variety of network services, including the following:

- Lightweight Directory Access Protocol (LDAP)
- Kerberos-based and single sign-on authentication
- Directory services, including DNS-based naming
- Central location for network administration and delegation of authority

The Lightweight Directory Access Protocol (LDAP) is an application protocol for querying and modifying data using directory services running over TCP/IP. Within the directory, the set of objects is organized in a logical hierarchical manner so that the objects can easily be located and managed. The structure can reflect geographical or organizational boundaries, although it tends to use DNS names for structuring the topmost levels of the hierarchy. Deeper inside the directory might appear entries representing people, organizational units, printers, documents, groups of people, or anything else that represents a given tree entry (or multiple entries). LDAP uses TCP port 389.

***Kerberos*** is the default computer network authentication protocol, which allows hosts to prove their identity over a non-secure network in a secure manner. It can also provide mutual authentication so that both the user and server verify each other's identity. To make it secure, Kerberos protocol messages are protected against eavesdropping and replay attacks.

***Single sign-on (SSO)*** allows a user to log on once and access multiple, related, but independent software systems without having to log on again. When a user logs on with Windows using Active Directory, the user is assigned a token, which can then be used to sign on to other systems automatically.

Lastly, Active Directory provides directory services that allow you to organize and name all of the network resources, including users, groups, printers, computers, and other objects, so that passwords, permissions, rights, and so on, can be assigned to the identity that needs them. A person who manages a group of objects can also be assigned. To help find resources, Active Directory is closely tied to DNS.

## Understanding Domain Controllers

A ***domain controller*** is a Windows server that stores a replica of the account and security information of the domain and defines the domain boundaries. To make a computer running Windows Server 2016 a domain controller, it is necessary to first install the Active Directory Domain Services. Then, execute the dcpromo (short for dc promotion) command to make the server a domain controller.

After a computer has been promoted to a domain controller, there will be several MMC snap-in consoles available to manage Active Directory. These include:

- **Active Directory Users and Computers:** Used to manage users, groups, computers, and organizational units.

- **Active Directory Domains and Trusts:** Used to administer domain trusts, domain and forest functional levels, and user principal name (UPN) suffixes.
- **Active Directory Sites and Services:** Used to administer the replication of directory data among all sites in an Active Directory Domain Services (AD DS) forest.
- **Active Directory Administrative Center:** Used to administer and publish information in the directory, including managing users, groups, computers, domains, domain controllers, and organizational units. The Active Directory Administrative Center was introduced in Windows Server 2008 R2.
- **Group Policy Management Console (GPMC):** Provides a single administrative tool for managing Group Policy across the enterprise. GPMC is automatically installed in Windows Server 2008 and higher domain controllers and needs to be downloaded and installed on Windows Server 2003 domain controllers.

While these tools are installed on domain controllers, they can also be installed on client PCs so that Active Directory can be managed without logging on to a domain controller.

Active Directory uses multimaster replication, which means that there is no master domain controller, commonly referred to a primary domain controller, as was found on Windows NT domains. However, because there are certain functions that can only be handled by one domain controller at a time, domain controllers can take on separate roles.

One role is the PDC Emulator, which provides backwards compatibility for NT4 clients and is becoming very uncommon. However, it also acts as the primary domain controller for password changes and acts as the master time server within the domain.

A server that is not running as a domain controller is known as a ***member server***. To demote a domain controller to a member server, run the dcpromo program again.

## Understanding NTLM

While Kerberos is the default authentication protocol for today's domain computers, ***NT LAN Manager (NTLM)*** is the default authentication protocol for Windows NT stand-alone computers that are not part of a domain, or when authenticating to a server using an IP address. It also acts a fallback authentication if it cannot complete Kerberos authentication, such as when blocked by a firewall.

NTLM uses a challenge-response mechanism for authentication, in which clients are able to prove their identities without sending a password to the server. After a random 8-byte challenge message is sent to the client from the server, the client uses the user's password as a key to generate a response back to the server using an MD4/MD5 hashing algorithm and DES encryption.

## Understanding Kerberos

With Kerberos, security and authentication is based on secret key technology, where every host on the network has its own secret key. The Key Distribution Center maintains a database of secret keys.

When a user logs on, the client transmits the user name to the authentication server, along with the identity of the service the user desires to connect to, such as a file server. The authentication server constructs a ticket, which randomly generates a key that is encrypted with a file server's secret key, and sends it to the client as part of its credentials, which includes the session key encrypted with the client's key. If the user enters the correct

password, then the client can decrypt the session key, present the ticket to the file server, and use the shared secret session key to communicate between them. Tickets are time stamped, and typically have an expiration time of only a few hours.

For all of this to work and to ensure security, the domain controllers and clients must have the same time. Windows operating systems include the Time Service tool (W32Time service). Kerberos authentication will work if the time interval between the relevant computers is within the maximum enabled time skew. The default setting is five minutes. Another option is to turn off the Time Service tool and then install a third-party time service. Of course, if there are problems with authentication, make sure that the time is correct for the domain controllers and the client having the problem.

## Using Organizational Units

As mentioned previously, an organization could have thousands of users and thousands of computers. With Windows NT, the domain could only handle so many objects before some performance issues appeared. With later versions of Windows, the size of the domain was dramatically increased. While several domains can be used with Windows NT to define an organization, there could be one domain to represent a large organization. However, if there are thousands of such objects, a method is needed to organize and manage them.

To help organize objects within a domain and minimize the number of domains, use ***organizational units***, commonly expressed as OUs. OUs can be used to hold users, groups, computers, and other organizational units. See Figure 2-2. An organizational unit can only contain objects that are located in a domain. While there are no restrictions on the number of nested OUs (an OU inside of another OU), a shallow hierarchy should be designed for better performance.

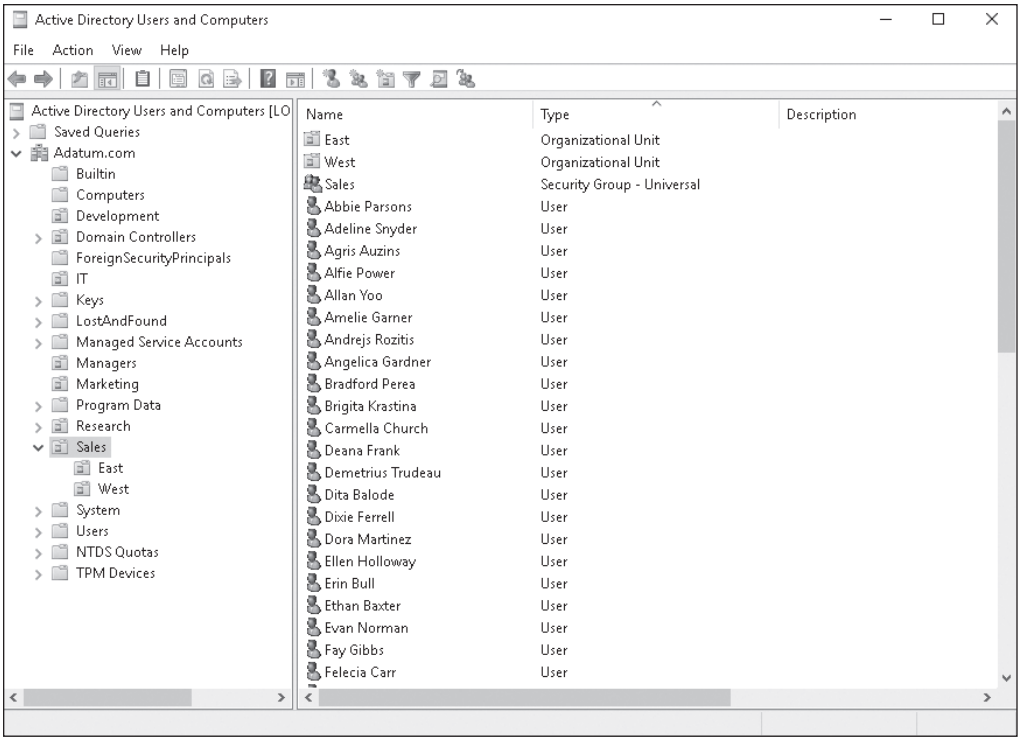



**Figure 2-2**

Active Directory organizational unit

When Active Directory is first installed, there are several organizational units already created. These include computers, users, domain controllers, and built-in OUs. Different from OUs that you create, these OUs do not allow anyone to delegate permissions or assign group policies to them. Group policies will be explained later in this lesson. Containers are objects that can store or hold other objects. They include the forest, tree, domain, and organizational unit. To help manage objects, delegate authority to a container, particularly an organizational unit.

For example, let's say that a domain is divided by physical location. Assign a site administrator authoritative control to the OU that represents the physical location. The user will only have administrative control to the objects within the OU. Also, structure the OUs by function or areas of management. For example, create a Sales OU to hold all of the sales users. In addition, create a Printers OU to hold all of the printer objects and assign a printer administrator.

Similar to NTFS and the registry, permissions can be assigned to users and groups over an Active Directory object. However, control would normally be delegated to the user or group. Basic administrative tasks can be assigned to regular users or groups, and domain-wide and forest-wide administration can be assigned to members of the Domain Admins and Enterprise Admins groups. By delegating administration, groups within your organization can be allowed to take more control of their local network resources. Help secure the network from accidental or malicious damage by limiting the membership of administrator groups.

Delegate administrative control to any level of a domain tree by creating organizational units within a domain and delegating administrative control for specific organizational units to particular users or groups.

### DELEGATE CONTROL

**GET READY.** To delegate control of an organizational unit, perform the following steps.

1. Open **Active Directory Users and Computers**.
2. In the console tree, right-click the organizational unit for which you want to delegate control.
3. Choose **Delegate control** to start the Delegation of Control Wizard and follow the instructions.

## Understanding Objects

An object is a distinct, named set of attributes or characteristics that represent a network resource. Common objects used within Active Directory are computers, users, groups, and printers. Attributes have values that define the specific object. For example, a user could have the first name John, the last name Smith, and the logon name as jsmith, all of which identify the user.

When working with objects, administrators will use names of the object such as user names. However, Active Directory objects are assigned a 128-bit unique number called a security identifier (SID), sometimes referred to as globally unique identifier (GUID) to uniquely identify an object. If a user changes his name, you can change the name and he will still be able to access all objects and have all the same rights as before, because they are assigned to the GUID.

GUIDs also provide some security where, if a user is deleted, a new user account cannot be created with the same user name and expect to have access to all of the objects and all of the rights that the previous user had. If someone within the organization is let go and will be replaced, disable the account, hire the new person, rename the user account, change the password, and re-enable the account. The new hire will be able to access all resources and have the same rights that were assigned to the previous user.

The schema of Active Directory defines the format of each object and the attributes or fields within each object. The default schema contains definitions of commonly used objects such as user accounts, computers, printers, and groups. For example, the schema defines that the user account has the first name, last name, and telephone numbers.

To allow the Active Directory to be flexible so that it can support other applications, extend the schema to include additional attributes. For example, add badge numbers or employee identification to the user object. When installing some applications such as Microsoft Exchange, it will extend the schema, usually by adding additional attributes or fields so that it can support the application.

## USERS

A ***user account*** enables a user to log on to a computer and domain. As a result, it can be used to prove the identity of a user, which can then be used to determine what kind of access that user will have (authorization). It can be used for auditing, so that if there is a security problem and something was accessed or deleted, the user account can indicate who accessed or deleted the object.

On today's Windows networks, there are two types of user accounts:

- The local user account
- The domain user account

A user account allows a user to log on and gain access to the computer where the account was created. The ***local user account*** is stored in the ***Security Account Manager (SAM)*** database on the local computer. The only Windows computer that does not have a SAM database is the domain controller. The administrator local user account is the only account that is created and enabled by default in Windows. While the administrator local user account cannot be deleted, it can be renamed.

The only other account created by default is the guest account. It was created for the occasional user who needs access to network resources on a low-security network. Using the guest account is not recommended and it is disabled by default.

A ***domain user*** is an account that is stored on the domain controller and allows the user to gain access to resources within the domain, assuming they have been granted permissions to access those objects. Like the computer local administrator account, the domain computer local administrator user account is the only account that is created and enabled by default in Windows when a domain is first created. While this domain administrator user account cannot be deleted, it can be renamed.

When creating a domain user account, supply a first name, last name, and a user's logon name. The user's logon name must be unique within the domain. See Figure 2-3. After the user account is created, open the user account properties and configure a person's user name, logon hours, which computers a user can log on to, telephone numbers and addresses, what groups the person is a member of, and so on. You can also specify if a password expires, if the password can be changed, and if the account is disabled. Lastly, on the Profile tab, define the user's home directory, logon script, and profile path. See Figure 2-4.

**Figure 2-3**

A user account in Active Directory

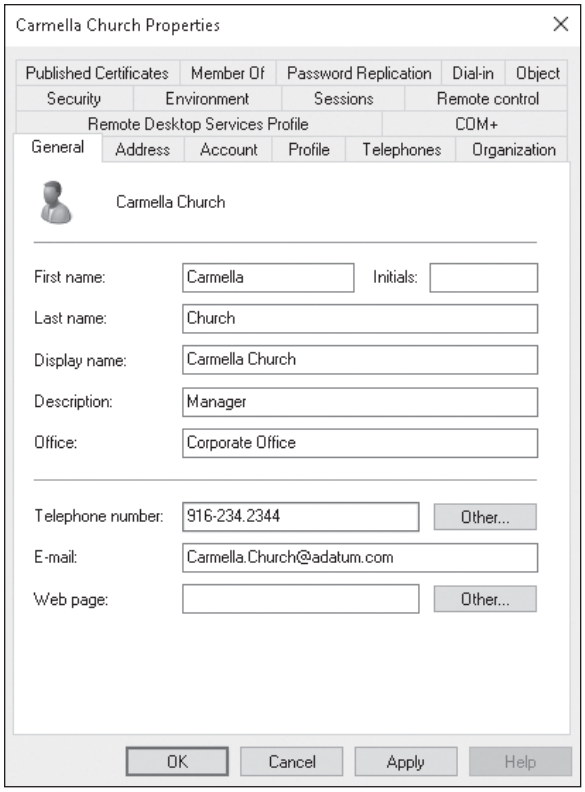
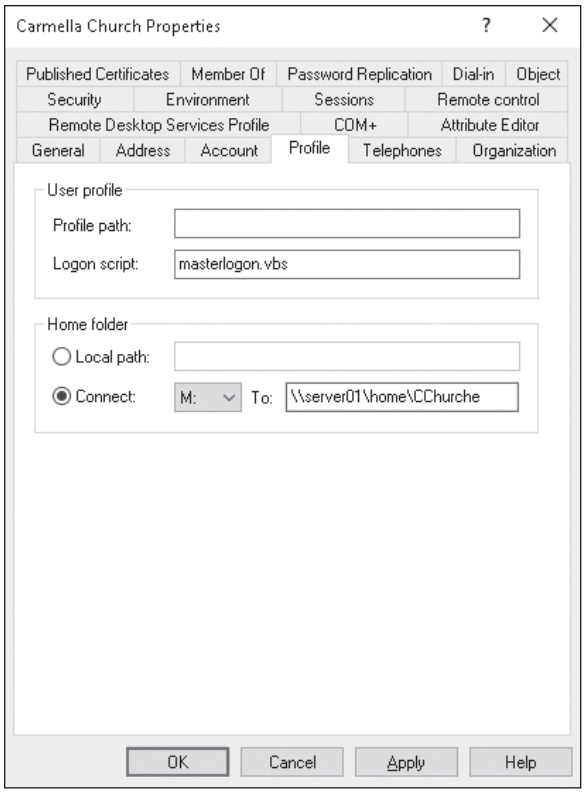



**Figure 2-4**

The Profile tab

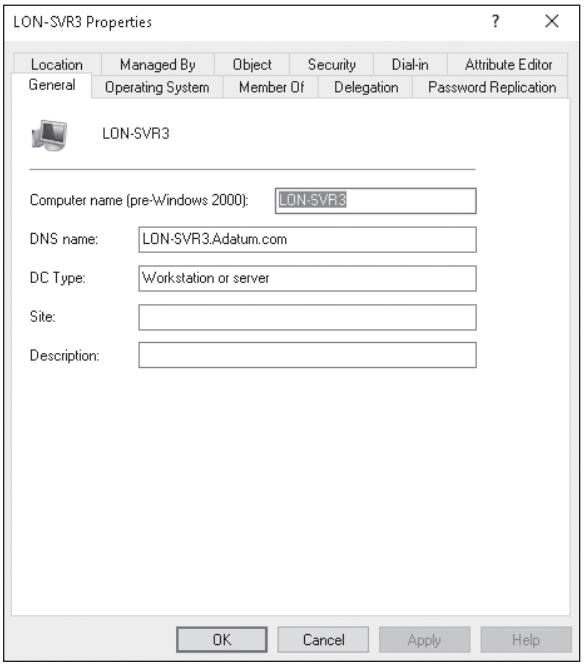


### COMPUTERS

Like user accounts, Windows ***computer accounts*** provide a means for authenticating and auditing the computer's access to a Windows network and its access to domain resources. Each Windows computer to which you want to grant access to resources must have a unique computer account. It can also be used for auditing purposes, specifying what system was used when something was accessed. See Figure 2-5.

**Figure 2-5**

A computer account




## Using Groups

A ***group*** is a collection or list of user accounts or computer accounts. Different from a container, the group does not store the user or computer, it just lists them. The advantage of using groups is to simplify administration, especially when assigning rights and permissions.

A group is much like it sounds; it is used to group users and computers together so that when rights and permissions are assigned, they are assigned to the group rather than to each user individually. Users and computers can be members of multiple groups, and in some instances, a group can be assigned to another group.

### GROUP TYPES

In Windows Active Directory, there are there are two types of groups—security and distribution. The security group is used to assign rights and permissions and gain access to a network resource. It can also be used as a distribution group. A distribution group is only for non-security functions such as email distribution and cannot be assigned rights and permissions to any resources.

## GROUP SCOPES

Any group, whether it is a security group or a distribution group, is characterized by a scope that identifies the extent to which the group is applied in the domain tree or forest. The three group scopes, also detailed in Table 2-1, are:

- **Domain local group:** Contain global groups and universal groups and can contain user accounts and other domain local groups. It is usually in the domain where the intended resources are located.
- **Global group:** Designed to contain user accounts. Global groups can contain user accounts and other global groups. Global groups are designed to be "global" for the domain. After placing user accounts into global groups, the global groups are typically placed into domain local groups or local groups.
- **Universal group:** This group scope is designed to contain global groups from multiple domains. Universal groups can contain global groups, other universal groups, and user accounts. Because global catalogs replicate universal group membership, limit the membership to global groups. This way, if a member within a global group is changed, the global catalog will not have to replicate the change.

When assigning rights and permissions, always try to group the users and assign the rights and permissions to the group instead of the individual users. To effectively manage the use

**Table 2-1**

Group Scopes

| Scope | Group can include as members. . . | Group can be assigned permissions in. . . | Group scope can be converted to. . . |
|---|---|---|---|
| Universal | Accounts from any domain within the forest in which this universal group resides<br>Global groups from any domain within the forest in which this universal group resides<br>Universal groups from any domain within the forest in which this universal group resides | Any domain or forest | Domain local<br>Global (as long as no other universal groups exist as members) |
| Global | Accounts from the same domain as the parent global group<br>Global groups from the same domain as the parent global group | Member permissions can be assigned in any domain | Universal (as long as it is not a member of any other global groups) |
| Domain Local | Accounts from any domain, global groups from any domain, universal groups from any domain, and domain local groups, but only from the same domain as the parent domain local group | Member permissions can be assigned only within the same domain as the parent domain local group | Universal (as long as no other domain local groups exist as members) |

of groups when assigning access to a network resource using global groups and domain local groups, remember AGDLP (Accounts, Global, Domain Local, Permissions):

- Add the user account (A) into the global group (G) in its domain where the user exists.
- Add the global group (G) from the user domain into the domain local group (DL) in the resource domain.
- Assign permissions (P) on the resource to the domain local group (DL) in its domain.

If you are using a universal group, the mnemonic is expanded to AGUDLP:

- Add the user account (A) into the global group (G) in its domain where the user exists.
- Add global groups (G) from the user domain into the universal group (U).
- Add universal group (U) to the domain local group (DL).
- Assign permissions (P) on the resource to the domain local group (DL) in its domain.

### BUILT-IN GROUPS

Like the administrator and guest accounts, Windows has default groups called ***built-in groups***. These default groups have been granted the essential rights and permissions to get you started with groups. Some of the built-in groups include the following:

- **Domain Admins:** Can perform administrative tasks on any computer within the domain. The default, the Administrator account, is a member.
- **Domain Users:** Windows automatically adds each new domain user account to the Domain Users group.
- **Account Operators:** Can create, delete, and modify user accounts and groups.
- **Backup Operators:** Can backup and restore all domain controllers by using Windows Backup.
- **Authenticated Users:** Includes all users with a valid user account on the computer or in Active Directory. Use the Authenticated Users group instead of the Everyone group to prevent anonymous access to a resource.
- **Everyone:** All users who access the computer with a valid user account.

For more information on the available groups, visit the following website:

https://technet.microsoft.com/en-us/library/dn579255(v=ws.11).aspx

## Understanding Web Server Authentication

When a person accesses a web server such as those running on Microsoft's Internet Information Server (IIS), several methods of authentication can be used.

When authenticating to a web server, IIS provides a variety of authentication schemes:

- **Anonymous (enabled by default):** Anonymous authentication gives users access to the website without prompting them for a user name or password. Instead, IIS uses a special Windows user account called IUSR_*machinename* for access. By default, IIS controls the password for this account.
- **Basic:** Basic authentication prompts the user for a user name and password. However, while the user name and password is sent as Base64 encoding, it is basically sent in plain text. If it is necessary to encrypt the user name and password while using basic authentication, use digital certificates so that it is encrypted with https.
- **Digest:** Digest authentication is a challenge/response mechanism, which sends a digest or hash using the password as the key instead of sending the password over the network.

- **Integrated Windows authentication:** Integrated Windows authentication (formerly known as NTLM authentication and Windows NT Challenge/Response authentication) can use either NTLM or Kerberos V5 authentication.
- **Client Certificate Mapping:** Uses a digital certificate that contains information about an entity and the entity's public key, which is used for authentication.

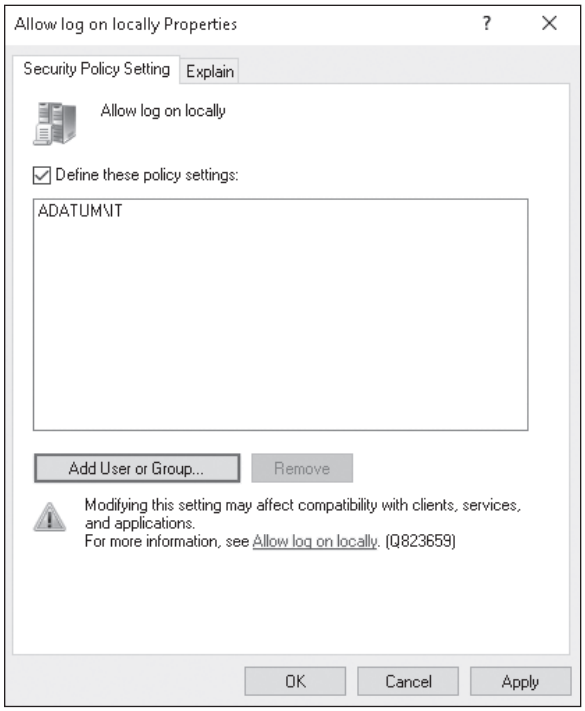
## ■ Comparing Rights and Permissions

**THE BOTTOM LINE** Specifying what a user can do on a system, or to a resource, is determined by two things: rights and permissions.

**CERTIFICATION READY**
Can you describe how permissions are stored for an object?
Objective 2.2

A ***right*** authorizes a user to perform certain actions on a computer, such as logging on to a system interactively, or backing up files and directories on a system. User rights are assigned through local policies or Active Directory group policies. See Figure 2-6.

**Figure 2-6**
Group policy user rights assignment




A ***permission*** defines the type of access that is granted to an object (an object can be identified with a security identifier) or object attribute. The most common objects assigned permissions are NTFS files and folders, printers, and Active Directory objects. To keep track of which user can access an object and what the user can do with that object, refer to the ***access control list (ACL)***. The ACL lists all users and groups that have access to the object.

**MORE INFORMATION**
NTFS and printer permissions will be discussed in Lesson 3.

## ■ Understanding NTFS

THE BOTTOM LINE

The file system is a method of storing and organizing computer files and the data they contain to make it easy to find and access them. It also maintains the physical location of the files so that the files can be found and accessed in the future. Like earlier Windows operating systems, Windows Server 2016 supports FAT16, FAT32, and NTFS file systems on hard drives.

**CERTIFICATION READY**
What is used to protect files on a drive when they are accessed directly and remotely?
Objective 2.2

After partitioning a disk, the next step is to format the disk as FAT16, FAT32, or NTFS. Out of these three options, NTFS is the preferred file system to be used in today's operating systems.

FAT16, sometimes referred to generically as File Allocation Table (FAT), is a simple file system that uses minimum memory and has been used with DOS. Originally, it supported the 8.3 naming scheme which allowed up to 8-character file names and 3-character file name extensions. Later, it was revised to support long file names. Unfortunately, FAT can only support volumes up to 2 GB.

FAT32 was introduced with the second major release of Windows 95. While the file system can support larger drives, today's Windows versions typically support volumes up to 32 GB. FAT32 also supports long file names.

NTFS is the preferred file system because it supports large volumes up to 16 exabytes (EB) and long file names. In addition, it is more fault tolerant than previous file systems used in Windows, because it is a journaling file system. A journaling file system ensures that a disk transaction is written to disk properly before being recognized. Lastly, NTFS offers better security through permissions and encryption.

### Using NTFS Permissions

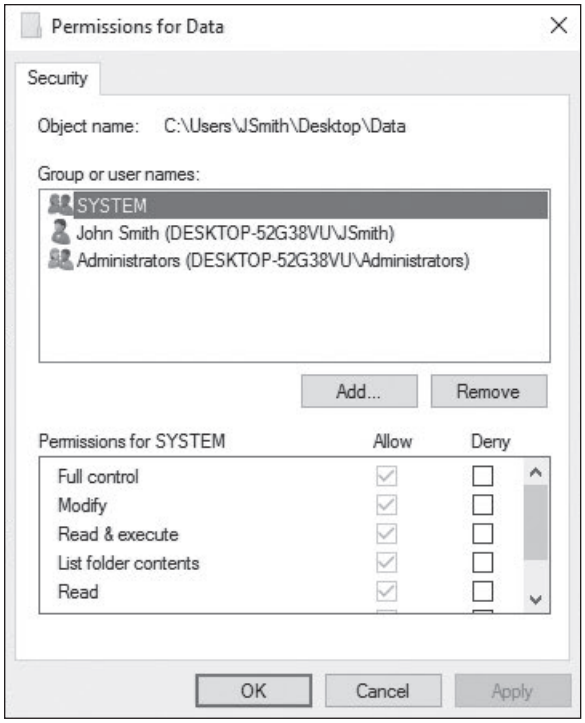
***NTFS permissions*** allow you to control which users and groups can gain access to files and folders on an NTFS volume. The advantage with NTFS permissions is that they affect local users as well as network users.

Usually, when assigning NTFS permissions, an administrator would assign the following NTFS Standard permissions:

- **Full Control:** Read, write, modify, and execute files in the folder; change attributes and permissions; and take ownership of the folder or files within.
- **Modify:** Read, write, modify, and execute files in the folder; and change attributes of the folder or files within.
- **Read & Execute:** Display the folder's contents; display the data, attributes, owner, and permissions for files within the folder; and run files within the folder.
- **List Folder Contents:** Display the folder's contents; display the data, attributes, owner, and permissions for files within the folder.
- **Read:** Display the file's data, attributes, owner, and permissions.
- **Write:** Write to the file, append to the file, and read or change its attributes.

To manage NTFS permissions, right-click a drive, folder, or file; choose Properties; and then click the Security tab. As shown in Figure 2-7, the group and users who have been given NTFS permissions and their respective standard NTFS permissions appear. To change the permissions, click the Edit button.

**Figure 2-7**
NTFS permissions




Groups or users granted Full Control permission on a folder can delete any files in that folder regardless of the permissions protecting the file. In addition, List Folder Contents is inherited by folders but not files, and it should only appear when viewing folder permissions. In Windows Server 2016, the Everyone group does not include the Anonymous Logon group by default, so permissions applied to the Everyone group do not affect the Anonymous Logon group.

To simplify administration, it is recommended to grant permissions using groups. By assigning NTFS permissions to a group, permissions are granted to one or more people, reducing the number of entries in each access list and reducing the amount of effort to configure when multiple people need access to the files or folders.

## Understanding Effective NTFS Permissions

The folder/file structure on an NTFS drive can be very complicated with many folders and many nested folders. In addition, because it is recommended to assign permissions to groups, and permissions can be assigned at different levels on an NTFS volume, figuring out the effective permissions of a particular folder or file for a particular user can be tricky.

There are two types of permissions used in NTFS:

- ***Explicit permission*:** Permissions granted directly to the file or folder
- ***Inherited permission*:** Permissions granted to a folder (parent object or container) that flow into child objects (subfolders or files inside the parent folder)

When assigning permissions to a folder, by default the permissions apply to the folder being assigned and the subfolders and files of the folder. To stop permission from being inherited, select the "Replace all existing inheritable permissions on all descendants with inheritable

permissions from this object" in the Advanced Security Settings dialog box and respond to the confirmation message. If the "Allow inheritable permissions from parent to propagate to this object" check box is cleared, the Security dialog box opens. When you click the Copy button, the explicit permission will be copied from the parent folder to the subfolder or file. Then, change the subfolder's or file's explicit permissions. If you click the Remove button, it will remove the inherited permission altogether.

By default, objects within a folder inherit the permissions from that folder when the objects are created. However, explicit permissions take precedence over inherited permissions. So, if different permissions are granted at a lower level, the lower level permissions take precedence.

For example, there is a folder called Data. Under the Data folder, there is a folder named Folder1, and under Folder1, there is Folder2. If Allow Full Control is granted to a user account, the Allow Full Control Permission will flow down to the subfolders and files under the Data folder.

| Object | NTFS Permissions |
|---|---|
| Data | Grant Allow Full Control (Explicit) |
| Folder1 | Allowed Full Control (Inherited) |
| Folder2 | Allowed Full Control (Inherited) |
| File1 | Allowed Full Control (Inherited) |

If Allow Full Control is granted on the Data folder to a user account, the Allow Full Control permission would normally flow down to Folder1. But if Allow Read permission is granted to Folder1 to the same user account, the Allow Read permission will overwrite the inherited permissions and it will then inherit down to Folder2 and File1.

| Object | NTFS Permissions |
|---|---|
| Data | Grant Allow Full Control (Explicit) |
| Folder1 | Allowed Read (Explicit) |
| Folder2 | Allowed Read (Inherited) |
| File1 | Allowed Read (Inherited) |

If a user has access to a file, the user will still be able to gain access to a file even if she does not have access to the folder containing the file. Of course, because the user doesn't have access to the folder, the user cannot navigate or browse through the folder to get to the file. Therefore, a user would have to use the universal naming convention (UNC) or local path to open the file.

When viewing the permissions, the status will be one of the following:

- **Checked:** Permissions are explicitly assigned.
- **Cleared (unchecked):** No permissions are assigned.
- **Shaded:** Permissions are granted through inheritance from a parent folder.

Besides granting the Allow permissions, you can also grant the Deny permission. The Deny permission always overrides the permissions that have been granted, including when a user or group has been given Full Control. For example, if the group has been granted Read and Write permissions, yet a person has been denied the Write permission, the user's effective rights would be the Read permission.

When you combine applying Deny versus Allowed with Explicit versus Inherited permissions, the hierarchy of precedence of permissions are:

1. Explicit Deny
2. Explicit Allow
3. Inherited Deny
4. Inherited Allow

Because users can be members of several groups, it is possible for them to have several sets of explicit permissions to a folder or file. When this occurs, the permissions are combined to form the ***effective permissions***, which are the actual permissions when logging on and accessing a file or folder. They consist of explicit permissions plus any inherited permissions.

When calculating the effective permissions, first calculate the explicit and inherited permissions for an individual group and then combine them. When combining user and group permissions for NTFS security, the effective permission is the cumulative permission. The only exception is that deny permissions always apply.

For example, there is a folder called Data. Under the Data folder, there is a folder named Folder1, and under Folder1, there is Folder2. User 1 is a member of Group 1 and Group 2. If you assign Allow Write permission to the Data folder to User 1, the Allow Read permission to Folder1 to Group 1, and the Allow Modify Permission to Folder2 to Group 2, the user's effective permissions would be shown as:

| Object | User 1 NTFS Permissions | Group 1 Permissions | Group 2 Permissions | Effective Permissions |
|---|---|---|---|---|
| Data | Allow Write Permission (Explicit) | | | Allow Write Permission |
| Folder1 | Allow Write Permission (Inherited) | Allow Read Permission (Explicit) | | Allow Read and Write Permission |
| Folder2 | Allow Write Permission (Inherited) | Allow Read Permission (Inherited) | Allow Modify Permission* (Explicit) | Allow Modify Permission* |
| File1 | Allow Write Permission (Inherited) | Allow Read Permission (Inherited) | Allow Modify Permission* (Inherited) | Allow Modify Permission* |

* The Modify permission includes the Read and Write permissions.

As another example, there is a folder called Data. Under the Data folder, there is a folder named Folder1, and under Folder1, there is Folder2. User 1 is a member of Group 1 and Group 2. If you assign Allow Write permission to the Data folder to User 1, the Allow Read permission to Folder1 to Group 1, and the Deny Modified permission to Folder2 to Group 2, the user's effective permissions would be shown as:

| Object | User 1 NTFS Permissions | Group 1 Permissions | Group 2 Permissions | Effective Permissions |
|---|---|---|---|---|
| Data | Allow Write Permission (Explicit) | | | Allow Write Permission |
| Folder1 | Allow Write Permission (Inherited) | Allow Read Permission (Explicit) | | Allow Read and Write Permission |
| Folder2 | Allow Write Permission (Inherited) | Allow Read Permission (Inherited) | Deny Modify Permission (Explicit) | Deny Modify Permission |
| File1 | Allow Write Permission (Inherited) | Allow Read Permission (Inherited) | Deny Modify Permission (Inherited) | Deny Modify Permission |

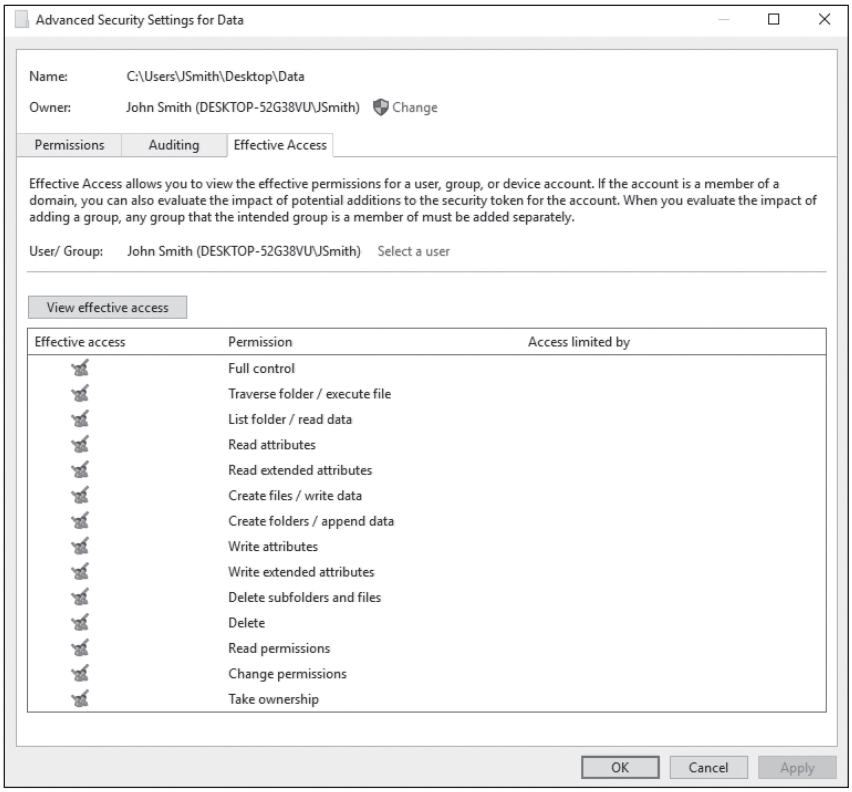
## VIEW NTFS EFFECTIVE PERMISSIONS

**GET READY.** To view the NTFS effective permissions granted to a user for a file or folder, perform the following steps.

1. Right-click the file or folder and choose **Properties**.
2. Click the **Security** tab.
3. Click the **Advanced** button.
4. Click the **Effective Access** tab.
5. Click the **Select a user** option and type the name of the user or group you want to view.
6. Click the **View effective access** button, as shown in Figure 2-8.
7. Click **OK**.

**Figure 2-8**

Showing Effective NTFS permissions



## Copying and Moving Files

When copying or moving files from one location to another, it is important to understand what happens to the NTFS permissions.

When copying and moving files, there are three scenarios:

- If copying a file or folder, the new folder and file will automatically acquire the permissions of the drive or folder to which the folder and file is being copied.
- If the folder or file is moved within the same volume, the folder or file will retain the same permissions that were already assigned.
- If the folder or file is moved from one volume to another volume, the folder or file will automatically acquire the permissions of the drive or folder to which the folder and file is being copied.

## Using Folder and File Owners

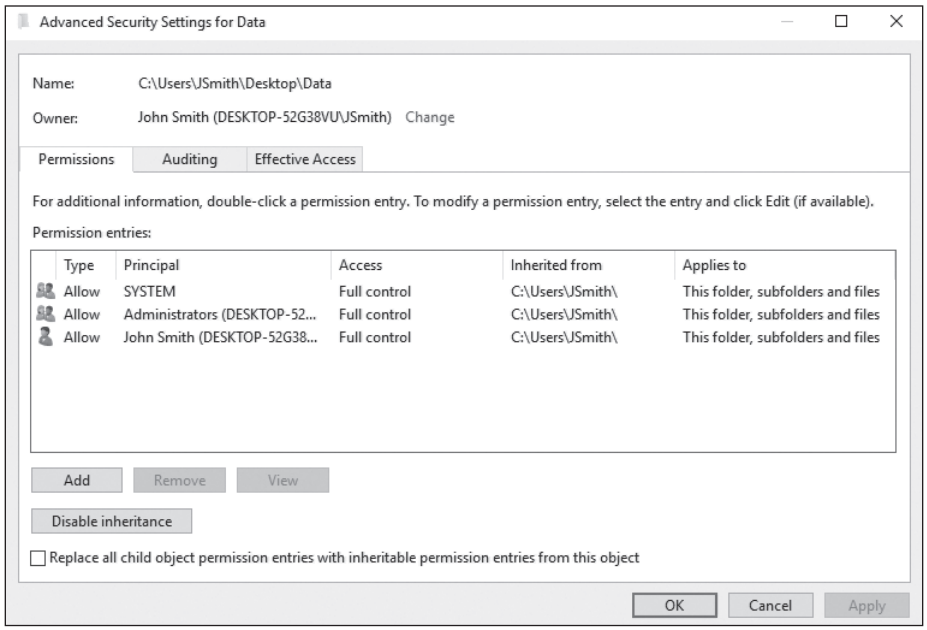
The ***owner*** of the object controls how permissions are set on the object and to whom permissions are granted. If, for some reason, access to a file or folder has been denied and the permissions need to be reset, take ownership of a file or folder and modify the permissions. All administrators automatically have the Take Ownership permission of all NTFS objects.

### TAKE OWNERSHIP OF A FILE OR FOLDER

**GET READY.** To take ownership of a file or folder, perform the following steps.

1. Open **File Explorer** and locate the file or folder for which you want to take ownership.
2. Right-click the file or folder, choose **Properties**, and then click the **Security** tab.
3. Click **Advanced**, as shown in Figure 2-9.

**Figure 2-9**
The Permissions tab



4. In the Owner section, click **Change**.
5. In the Select User or Group dialog box, in the Enter the object name to select text box, type the name of the user, such as **JSmith**, and click **OK**.
6. To close the Advanced Security Settings for Data dialog box, click **OK**.
7. To close the Properties dialog box, click **OK**.

## ■ Sharing Drives and Folders

**THE BOTTOM LINE**

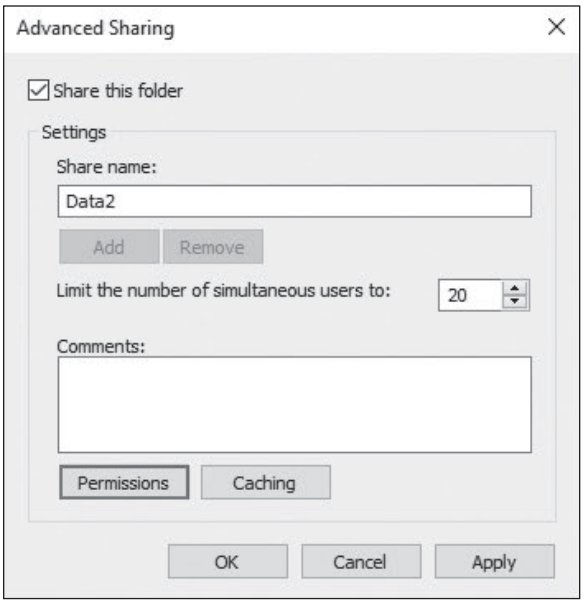
Most users are not going to log on to a server directly to access their data files. Instead, a drive or folder will be shared (known as a ***shared folder***), and they will access the data files over the network. To help protect against unauthorized access, use ***share permissions*** along with NTFS permissions (if the shared folder is on an NTFS volume). When a user needs to access a network share, they would use the UNC, which is \\servername\sharename.

### SHARE A FOLDER

**GET READY.** To share a folder, perform the following steps.

1. In Windows Server 2016, right-click the drive or folder, choose **Properties**, click the **Sharing** tab, and then click the **Advanced Sharing** button.
2. Select the **Share this folder** check box.
3. In the Advanced Sharing dialog box, in the Share name text box, type the name of the shared folder, such as **Data2** (see Figure 2-10).

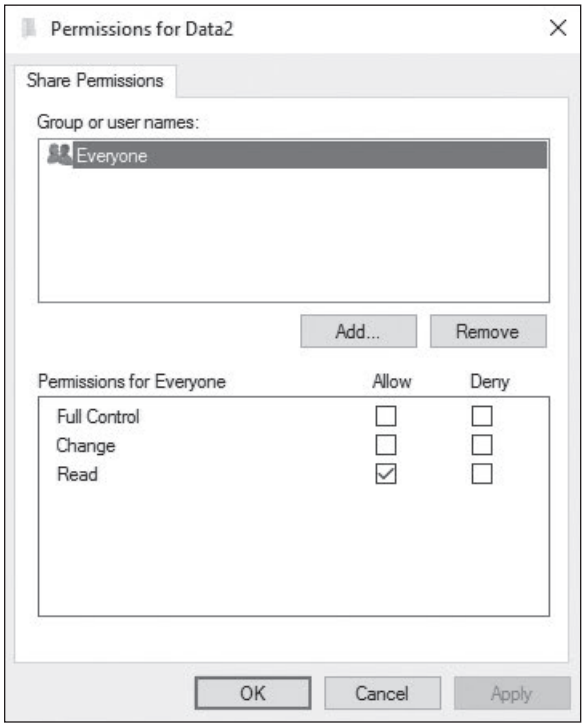
**Figure 2-10**
Sharing a folder




4. If necessary, specify the maximum number of people that can access the shared folder at the same time.
5. Click the **Permissions** button.

6. By default, Everyone is given Allow Read permission. If you don't want everyone to access the folder, remove **Everyone** and assign additional permissions or add additional people. See Figure 2-11.

**Figure 2-11**
Specifying share permissions




7. After the users and groups have been added with the proper permissions, click **OK** to close the Permissions dialog box.
8. To close the Advanced Sharing dialog box, click **OK**.
9. Click **Close** to close the Properties dialog box.

The share permissions that are available are:

- **Full Control:** Users allowed this permission have Read and Change permissions, as well as the additional capabilities to change file and folder permissions and take ownership of files and folders.
- **Change:** Users allowed this permission have Read permissions and the additional capability to create files and subfolders, modify files, change attributes on files and subfolders, and delete files and subfolders.
- **Read:** Users with this permission can view file and subfolder names, access the subfolders of the share, read file data and attributes, and run program files.

It should be noted that share permissions always apply when accessed remotely using a UNC, even if it is on the FAT, FAT32, or NTFS volume.

Much like NTFS, you can allow or deny each share permission. To simplify managing share and NTFS permissions, Microsoft recommends giving Everyone Full Control, and then controlling access using NTFS permissions. In addition, because a user can be a member of several groups, it is possible for the user to have several sets of permissions to a shared drive or folder. The effective share permissions are the combination of the user and all group permissions for which the user is a member.

When a person logs on directly to the server console and accesses the files and folders without using the UNC, only the NTFS permissions apply and not the share permissions. When a person accesses a shared folder using the UNC, combine the NTFS and share permissions to see what a user can do. To figure the overall access, first calculate the effective NTFS permissions. Then, determine the effective share permissions. Lastly, apply the more restrictive permissions between the NTFS and share permissions.

### Understanding Special Shares and Administrative Shares

There are several special shared folders that are automatically created by Windows for administrative and system use. Different from regular shares, these shares do not show when a user browses the computer resources using Network Neighborhood, My Network Place, or similar destinations. In most cases, special shared folders should not be deleted or modified. For Windows Servers, only members of the Administrators, Backup Operators, and Server Operators groups can connect to these shares.

An ***administrative share*** is a shared folder typically used for administrative purposes. To make a shared folder or drive into a hidden share, the share name must have a $ at the end of it. Because the share folder or drive cannot be seen during browsing, use a UNC name which will include the share name and the trailing '$'. By default, all volumes with drive letters automatically have administrative shares (C$, D$, E$, and so on). Other administrative shares can be created as needed for individual folders.

In addition to the administrative shares for each drive, the following special shares are also available:

- **ADMIN$:** A resource used by the system during remote administration of a computer. The path of this resource is always the path to the Windows 10 system root (the directory in which Windows 10 is installed—for example, C:\Windows).
- **IPC$:** A resource sharing the named pipes that are essential for communication between programs. It is used during remote administration of a computer and when viewing a computer's shared resources.
- **PRINT$:** A resource used during remote administration of printers.

## ■ Introducing the Registry

THE BOTTOM LINE

The ***registry*** is a central, secure database in which Windows stores all hardware configuration information, software configuration information, and system security policies. Components that use the registry include the Windows kernel, device drivers, setup programs, hardware profiles, and user profiles.

**CERTIFICATION READY**
What is used to specify who can access specific registry settings?
Objective 2.1

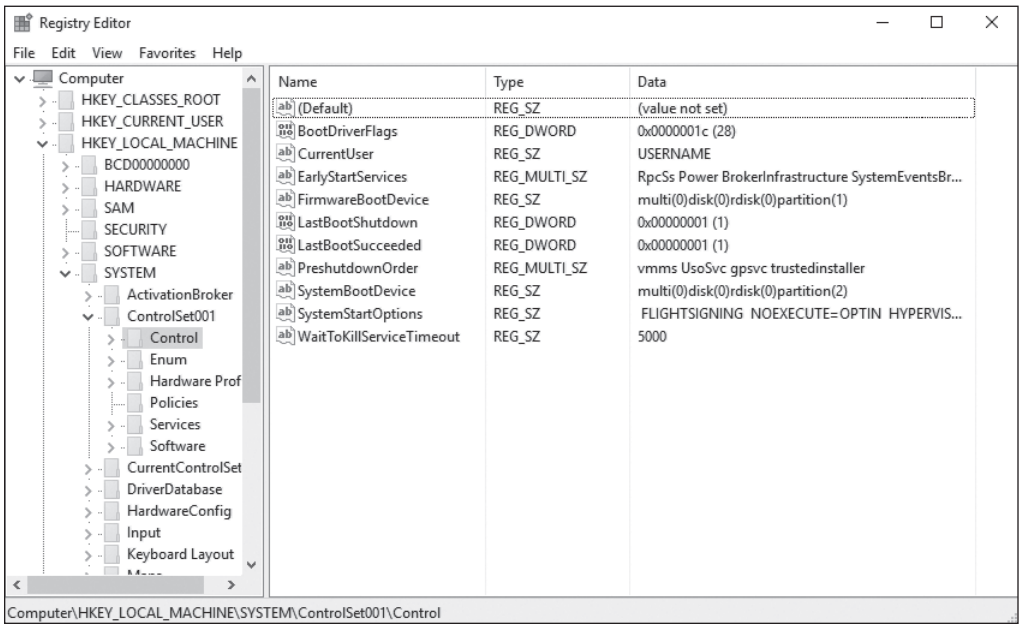
Most of the time, it is not necessary to access the Windows registry because programs and applications typically make all the necessary changes to the registry automatically. For example, when changing the desktop background or changing the default color for Windows, access the Display settings within Control Panel and Windows will save the changes to the registry.

There may be a time when it is necessary to make a change in the registry because there is no interface or program to make the change. To view and manually change the registry, use the

Registry Editor (Regedit.exe), which can be executed from the command prompt, Start search box, or Run box. See Figure 2-12.

**Figure 2-12**

The Registry Editor




**TAKE NOTE***

If it is necessary to access and make changes to the registry, closely follow the instructions from a reputable source, because an incorrect change to your computer's registry could render your computer inoperable.

The registry is split into several logical sections, often referred to as hives, which are generally named by their Windows API definitions. The hives begin with HKEY are often abbreviated to a three- or four-letter short name starting with "HK". For example, HKCU refers to HKEY_CURRENT_USER and HKLM refers to HKEY_LOCAL_MACHINE. Windows 10 has five root keys/HKEYs:

- **HKEY_CLASSES_ROOT:** Stores information about registered applications, such as file association that tells which default program opens a file with a certain extension.
- **HKEY_CURRENT_USER:** Stores settings that are specific to the currently logged-on user. When a user logs off, the HKEY_CURRENT_USER is saved to HKEY_USERS.
- **HKEY_LOCAL_MACHINE:** Stores settings that are specific to the local computer.
- **HKEY_USERS:** Contains subkeys corresponding to the HKEY_CURRENT_USER keys for each user profile actively loaded on the machine.
- **HKEY_CURRENT_CONFIG:** Contains information gathered at runtime. Information stored in this key is not permanently stored on disk, but rather regenerated at the boot time.

Registry keys are similar to folders, which can contain values or subkeys. Navigating the keys within the registry follows a syntax similar to Windows folders or a file path, using backslashes to separate each level. For example:

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows

refers to the subkey "Windows" of the subkey "Microsoft" of the subkey "Software" of the HKEY_LOCAL_MACHINE key.

Registry values include a name and a value. There are multiple types of values. Some of the common registry key types are shown in Table 2-2.

**Table 2-2**
Common Registry Key Types

| Name | Data Type | Description |
|---|---|---|
| Binary Value | REG_BINARY | Raw binary data. Most hardware component information is stored as binary data and is displayed in Registry Editor in hexadecimal format. |
| DWORD Value | REG_DWORD | Data represented by a number that is 4 bytes long (a 32-bit integer). Many parameters for device drivers and services are this type and are displayed in Registry Editor in binary, hexadecimal, or decimal format. |
| Expandable String Value | REG_EXPAND_SZ | A variable-length data string. This data type includes variables that are resolved when a program or service uses the data. |
| Multi-String Value | REG_MULTI_SZ | A multiple string. Values that contain lists or multiple values in a form that people can read are generally this type. Entries are separated by spaces, commas, or other marks. |
| String Value | REG_SZ | A fixed-length text string. |
| QWORD Value | REG_QWORD | Data represented by a number that is a 64-bit integer. This data is displayed in Registry Editor as a Binary Value and was introduced in Windows 2000. |

Reg files (also known as Registration entries) are text files for storing portions of the registry. They have a .reg file name extension. Double-click a reg file to add the registry entries into the registry. To export any registry subkey, right-click the subkey and choose Export. To back up the entire registry to a reg file, right-click Computer at the top of Regedit and choose export; or, back up the system state with Windows Backup.

### ACCESS REGISTRY PERMISSIONS

**GET READY.** Similar to NTFS permissions, the registry uses registry permissions that are stored in ACLs. To access the registry permissions, perform the following steps.

1. Open **Registry Editor**.
2. Click the key to which you want to assign permissions.
3. Click **Edit > Permissions**.

Then, add the affected user or group and assign either allow or deny Full Control or Read permission.

## ■ Using Encryption to Protect Data


***Encryption*** is the process of converting data into a format that cannot be read by another user. Once a user has encrypted a file, it automatically remains encrypted when the file is stored on disk. ***Decryption*** is the process of converting data from encrypted format back to its original format.

**CERTIFICATION READY**
Can you describe and contrast the three primary methods of encryption?
Objective 2.5

With commonly used encryption methods, the encryption algorithm needs to provide a high level of security, while being available to the public. Because the algorithm is made available to the public, the security resides in the key, and not in the algorithm itself.One of the simplest cipher algorithms is the substitution cipher, which changes one character or symbol into another. For example, if you have:

```
clear text
```

And you substitute each 'e' with the 'y' and each 'c' with the letter 'j' and the letter 't' with 'y', you would get the following ciphertext:

```
jlyar yyxy
```

Another simple technique is based on the transposition cipher, which involves transposing or scrambling the letters in a certain manner. For example, if you have:

```
clear text
```

and you switch each two letters, you get:

```
lcae rettx
```

A ***key***, which can be thought of as a password, is applied mathematically to plain text to provide cipher or encrypted text. A different key produces a different encrypted output. With computers, encryption is often based on bits, not characters. For example, if you have the Unicode letters 'cl', it would be expressed in the following binary format:

01100011 01101100

and if you mathematically add the binary form of 'z' (01111010), which is the key, you get:

| | |
|---|---|
| 01100011 | 01101100 |
| +01111010 | +01111010 |
| 11011101 | 11100110 |

which would show as strange Unicode characters: Ýæ.

Similar to a password, the longer the key (usually expressed in bits), the more secure it is. For a hacker to figure out a key, they would also have to use a brute force attack, which means the hacker would have to try every combination of bits until they figure out the correct key. While a key could be broken given enough time and processing power, long keys are chosen so that it would take months, maybe even years, to calculate. Of course, similar to passwords, some encryption algorithms change the key frequently. Therefore, a key length of 80 bits is generally considered the minimum for strong security with symmetric encryption algorithms. Today, 128-bit keys are commonly used and considered very strong.

## Types of Encryption

Encryption algorithms can be divided into three classes: Symmetric, Asymmetric, and Hash function. Symmetric and Asymmetric encryption can encrypt and decrypt data. A Hash function can only encrypt data; that data cannot be decrypted.

### SYMMETRIC ENCRYPTION

***Symmetric encryption*** uses a single key to encrypt and decrypt data. Therefore, it is also referred to as secret-key, single-key, shared-key, and private-key encryption. To use symmetric key algorithms, you need to initially exchange the secret key with both the sender and receiver.

Symmetric-key ciphers can be divided into block ciphers and stream ciphers. A block cipher takes a block of plain text and a key, and outputs a block of ciphertext of the same size. Two popular block ciphers include the Data Encryption Standard (DES) and the Advanced Encryption Standard (AES), which have been designated cryptography standards by the U.S. government.

The Data Encryption Standard was selected by the National Bureau of Standards as an official Federal Information Processing Standard (FIPS) for the United States in 1976. It is based on a symmetric-key algorithm that uses a 56-bit key.

Because DES is based on a relatively small 56-bit key size, DES was subject to brute force attacks. Therefore, without designing a completely new block cipher algorithm, Triple DES (3DES) was developed, which uses three independent keys. DES and the more secure 3DES are still popular and used across a wide range of applications, including ATM encryption, email privacy, and secure remote access.

While DES and 3DES are still popular, a more secure encryption called Advanced Encryption Standard (AES) was announced in 2001 and is growing in popularity. The standard comprises three block ciphers, AES-128, AES-192, and AES-256 used on 128-bit blocks, with key sizes of 128, 192, and 256 bits, respectively. The AES ciphers have been analyzed extensively and are now used worldwide, including being used with Wi-Fi Protected Access 2 (WPA2) wireless encryption.

Stream ciphers create an arbitrarily long stream of key material, which is combined with plain text bit-by-bit or character-by-character. RC4 is a widely used stream cipher, used in Secure Sockets Layer (SSL) and Wired Equivalent Privacy (WEP). While RC4 is simple and is known for its speed, it can be vulnerable if the key stream is not discarded, nonrandom or related keys are used, or a single key stream is used twice.

## ASYMMETRIC ENCRYPTION

***Asymmetric encryption*** uses two keys for encryption. Asymmetric key, also known as public key cryptography, uses two mathematically-related keys. One key is used to encrypt the data, while the second key is used to decrypt the data. Unlike symmetric key algorithms, it does not require a secure initial exchange of one or more secret keys to both sender and receiver. Instead, you can make the public key known to anyone and use the other key to encrypt or decrypt the data. The public key could be sent to someone or could be published within a digital certificate via a Certificate Authority (CA). Secure Sockets Layer (SSL)/Transport Layer Security (TLS) and Pretty Good Privacy (PGP) use asymmetric keys. Two popular asymmetric encryption protocols are Diffie-Hellman and RSA.

For example, say you want a partner to send you data. Therefore, you send the partner the public key. The partner will then encrypt the data with the key and send you the encrypted message. Then, you use the private key to decrypt the message. If the public key falls into someone else's hands, they still could not decrypt the message.

## HASH FUNCTION ENCRYPTION

The last type of encryption is the hash function. Different from the symmetric and asymmetric algorithms, a ***hash function*** is meant as a one-way encryption. This means that after data has been encrypted, it cannot be decrypted. It can be used to encrypt a password that is stored on disk and for digital signatures. Anytime a password is entered, the same hash calculation is performed on the entered password and it is compared to the hash value of the password stored on disk. If the two passwords match, the user must have typed the correct password. This avoids having to store the passwords in a readable format, where a hacker might try to access them.

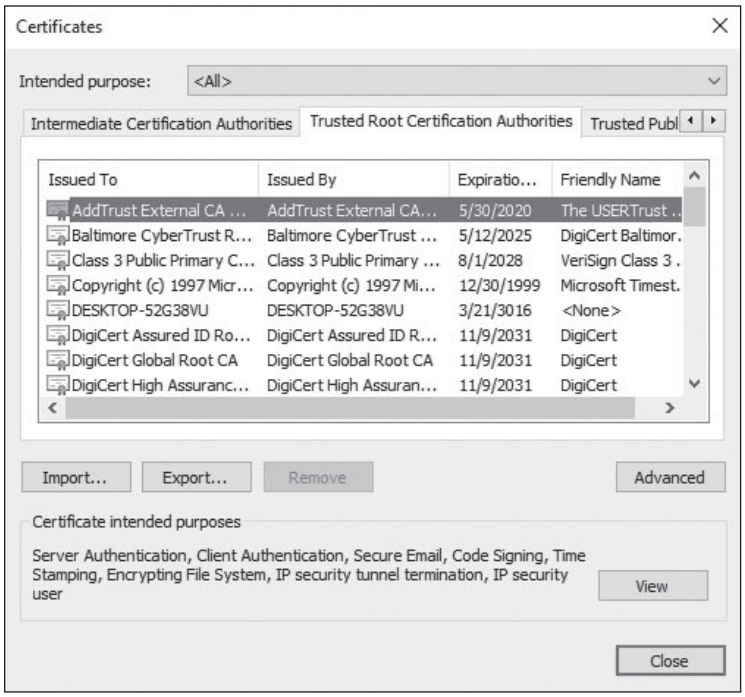
## Introducing Public Key Infrastructure (PKI)

When surfing the internet, there are times when it is necessary to transmit private data over the internet, such as credit card numbers, social security numbers, and so on. During these times, use http over SSL (https) to encrypt the data sent over the internet. By convention, URLs that require an SSL connection start with https: instead of http:.

A ***public key infrastructure (PKI)*** is a system consisting of hardware, software, policies, and procedures that create, manage, distribute, use, store, and revoke digital certificates. Within the PKI, the certificate authority (CA) binds a public key with respective user identities and issues digital certificates containing the public key. For this system to work, the CA must be trusted. Typically, within an organization, you may install a CA on a Windows server, specifically on a domain controller, and it would be trusted within the organization. If it is necessary to have a CA trusted outside of your organization, use a trusted third-party CA, such as VeriSign or Entrust. Established commercial CAs charge to issue certificates that will automatically be trusted by most web browsers. See Figure 2-13.

**Figure 2-13**

Trusted CAs within Internet Explorer




The registration authority (RA), which may or may not be the same server as the CA, is used to distribute keys, accept registrations for the CA, and validate identities. The RA does not distribute digital certificates; instead digital certificates are distributed by the CA.

Besides having an expiration date, a digital certificate can also be revoked if it was compromised or the situation has changed for the system to which the digital certificate was assigned. A ***certificate revocation list (CRL)*** is a list of certificates (or more specifically, a list of serial numbers for certificates) that have been revoked or are no longer valid, and therefore should not be relied upon.

Windows servers can host a certificate authority. The Enterprise Root CA is at the top level of the certificate authority hierarchy. Once an Enterprise Root CA is configured, it registers

automatically within Active Directory and all computers within the domain will trust it. It will support auto-enrollment and auto-renewal of digital certificates.

To support outside clients and customers, you would most likely build a standalone CA. Different from an Enterprise Root CA, the standalone CA does not use Active Directory. Because standalone CA does not support auto-enrollment, all requests for certificates are pending until an administrator approves them.

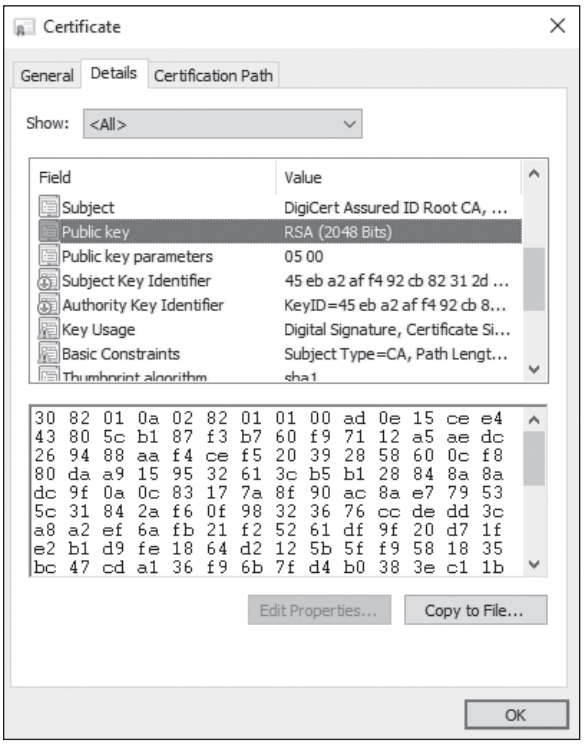
## DIGITAL CERTIFICATE

A digital certificate is an electronic document that contains a person's or organization's name, a serial number, expiration date, a copy of the certificate holder's public key (used for encrypting messages and to create digital signatures), and the digital signature of the CA that assigned the digital certificate so that a recipient can verify that the certificate is real.

The most common digital certificate is the X.509 version 3. The X.509 version 3 standard specifies the format for the public key certificate, certificate revocation lists, attribute certificates, and a certificate path validation algorithm. See Figure 2-14.

**Figure 2-14**

X.509 digital certificate




Digital certificates can be imported and exported via an electronic file. Four common formats are:

- **Personal Information Exchange (PKCS #12):** The Personal Information Exchange format (PFX, also called PKCS #12) supports secure storage of certificates, private keys, and all certificates in a certification path. The PKCS #12 format is the only file format that can be used to export a certificate and its private key. It will usually have a .p12 file name extension.
- **Cryptographic Message Syntax Standard (PKCS #7):** The PKCS #7 format supports storage of certificates and all certificates in the certification path. It will usually have a .p7b or .p7c file name extension.

- **DER-encoded binary X.509:** The Distinguished Encoding Rules (DER) format supports storage of a single certificate. This format does not support storage of the private key or certification path. It will usually have a .cer, .crt, or .der file name extension.
- **Base64-encoded X.509:** The Base64 format supports storage of a single certificate. This format does not support storage of the private key or certification path.

## ACQUIRE A DIGITAL CERTIFICATE

**GET READY.** To acquire a digital certificate using IIS 7/7.5, perform the following steps.

1. Request an internet server certificate from the IIS server. To request an internet server certificate, click the server from within **IIS Manager** and double-click **Server Certificates** in Features View. Then click **Create Certificate Request** from the Actions pane.
2. Send the generated certificate request to the CA, usually using the vendor's website.
3. Receive a digital certificate from the CA and install it on the IIS server. Again, open **IIS Manager**, double-click the server from within IIS Manager, and then double-click **Server Certificates** in Features View. Then, select the **Complete Certificate Request**.

If you have a farm that consists of multiple web servers, it is necessary to install the digital certificate from the first server and then export the digital certificate to a .pfx format needed to copy the public and private key to the other servers. Therefore, export the key from the first server and import to the other servers.

## EXPORT A DIGITAL CERTIFICATE

**GET READY.** To export a digital certificate, perform the following steps.

1. Open **IIS Manager** and navigate to the level you want to manage.
2. In the Features View, double-click **Server Certificates**.
3. In the **Actions** pane, click **Export**.
4. In the Export dialog box, type a file name in the **Export to** box or click the **Browse** button to navigate to the name of a file in which to store the certificate for exporting.
5. Type a password in the **Password** box if you want to associate a password with the exported certificate. Retype the password in the **Confirm password** box.
6. Click **OK**.

## IMPORT A DIGITAL CERTIFICATE

**GET READY.** To import a digital certificate, perform the following steps.

1. Open **IIS Manager** and navigate to the level you want to manage.
2. In the Features View, double-click **Server Certificates**.
3. In the **Actions** pane, click **Import**.
4. In the Import Certificate dialog box, type a file name in the **Certificate File** box or click the **Browse** button to navigate to the name of a file where the exported

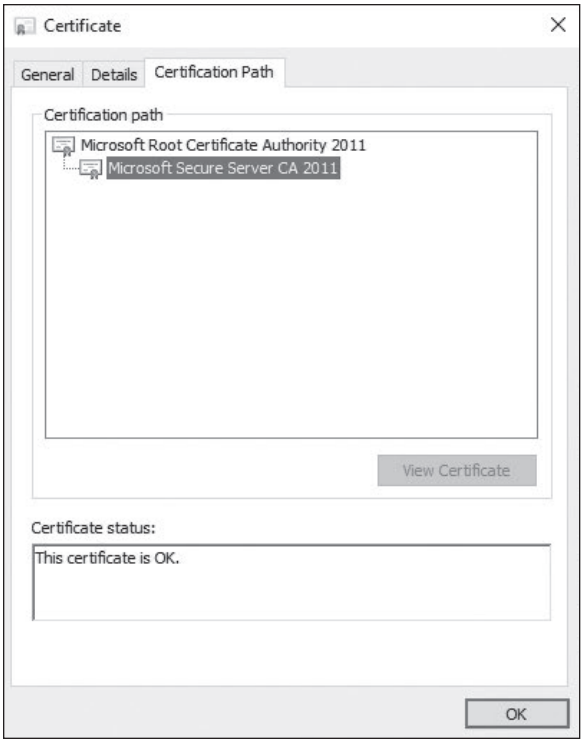
certificate is stored. Type a password in the **Password** box if the certificate was exported with a password.

5. Select **Allow this certificate to be exported** if you want to be able to export the certificate, or clear **Allow this certificate to be exported** if you want to prevent additional exports of this certificate.
6. Click **OK**.

## CERTIFICATE CHAIN

There are only so many root CA certificates that are assigned to commercial third-party organizations. Therefore, when acquiring a digital certificate from a third-party organization, it might be necessary to use a certificate chain to obtain the root CA certificate. In addition, it might be necessary to install an intermittent digital certificate that will link the assigned digital certificate to a trusted root CA certificate. The ***certificate chain***, also known as the certification path, is a list of certificates used to authenticate an entity. It begins with the certificate of the entity and ends with the root CA certificate. See Figure 2-15.

**Figure 2-15**
A certificate chain




## DIGITAL SIGNATURE

A ***digital signature*** is a mathematical scheme that is used to demonstrate the authenticity of a digital message or document. It is also used to confirm that the message or document has not been modified. The sender uses the receiver's public key to create a hash of the message, which is stored in the message digest. The message is then sent to the receiver. The receiver will then use her private key to decrypt the hash value, perform the same hash function on the message, and compare the two hash values. If the message has not been changed, the hash values will match.

To prove that a message comes from a particular person, perform the hashing function with your private key and attach the hash value to the document to be sent. When the document is sent and received by the receiving party, the same hash function is completed. Then, use the sender's public key to decrypt the hash value included in the document. If the two hash values match, the user who sent the document must have known the sender's private key, proving who sent the document. It will also prove that the document has not been changed.

### SECURE SOCKETS LAYER (SSL) AND TRANSPORT LAYER SECURITY (TLS)

When surfing the internet, there are times when it is necessary to transmit private data over the internet such as credit card numbers, social security numbers, and so on. During these times, use SSL over http (https) to encrypt the data sent over the internet. By convention, URLs that require an SSL connection start with https: instead of http:.

**SSL** is short for ***Secure Sockets Layer***. It uses a cryptographic system with two keys to encrypt data—a public key known to everyone and a private or secret key known only to the recipient of the message. The public key is published in a digital certificate, which also confirms the identity of the web server.

When connecting to a site that is secured using SSL, a gold lock appears in the address bar, along with the name of the organization to which the CA issued the certificate. Clicking the lock icon displays more information about the site, including the identity of the CA that issued the certificate. For even more information, click the View Certificate link to open the Certificate dialog box.

When visiting certain websites, Internet Explorer may find problems with the digital certificate. For example, the certificate has expired, it is corrupted, it has been revoked, or it does not match the name of the website. When this happens, IE will block access to the site and display a warning stating that there is a problem with the certificate. Either close the browser window or ignore the warning and continue to the site. Of course, ignore the warning only if you trust the website and believe that you are communicating with the correct server.

Transport Layer Security (TLS) is an extension of SSL, which is supported by the Internet Engineering Task Force (IETF) so that it could be an open, community supported standard, which could then be expanded with other internet standards. While TLS is often referred to as SSL 3.0, it does not interoperate with SSL. While TLS is usually the default for most browsers, it has a downgrade feature that allows SSL 3.0 to run as needed.

## Encrypting Email

Because email is sent over the internet, one may be concerned with the data packets being captured and read. Therefore, there is a need to encrypt emails that contain confidential information.

There are multiple protocols that can be used to encrypt emails. They include:

- Secure/Multipurpose Internet Mail Extensions (S/MIME)
- Pretty Good Privacy (PGP)

Secure/Multipurpose Internet Mail Extensions (S/MIME) is the secure version of MIME, used to embed objects within email messages. It is the most widely supported standard used to secure email communications, which uses the PKCS #7 standard. S/MIME is included with popular web browsers and has also been endorsed by other vendors that make messaging products.

Pretty Good Privacy (PGP) is a freeware email encryption system that uses symmetrical and asymmetrical encryption. When an email is sent, the document is encrypted with the public key and a session key. The session key is a one-use random number used to create the ciphertext. The session key is encrypted into the public key and sent with the ciphertext. When the message is received, the private key is used to extract the session key. The session key and the private key are used to decrypt the ciphertext.

## Encrypting Files with EFS

If someone steals a hard drive that is protected by NTFS permissions, they could take the hard drive, place it in a system in which they are an administrator, and access all files and folders on the hard drive. Therefore, to truly protect a drive that could be stolen or accessed illegally, encrypt the files and folders on the drive.

Windows 10 offers two file encrypting technologies—Encrypting File System (EFS) and BitLocker Drive Encryption. EFS protects individual files or folders, while BitLocker protects entire drives.

Encrypting File System (EFS) can encrypt files on an NTFS volume that cannot be used unless the user has access to the keys required to decrypt the information. After a file has been encrypted, it is not necessary to manually decrypt an encrypted file before using it. After encrypting a file or folder, work with the encrypted file or folder as with any other file or folder.

EFS is keyed to a specific user account, using the public and private keys that are the basis of the Windows public key infrastructure (PKI). The user who creates a file is the only person who can read it. As the user works, EFS encrypts the files he creates using a key generated from the user's public key. Data encrypted with this key can be decrypted only by the user's personal encryption certificate, which is generated using his private key.

### ENCRYPT A FOLDER OR FILE USING EFS

**GET READY.** To encrypt a folder or file using EFS, perform the following steps.

1. Right-click the folder or file you want to encrypt and choose **Properties**.
2. Click the **General** tab and click **Advanced**. See Figure 2-16.
3. Select the **Encrypt contents to secure data** check box, click **OK**, and then click **OK** again.

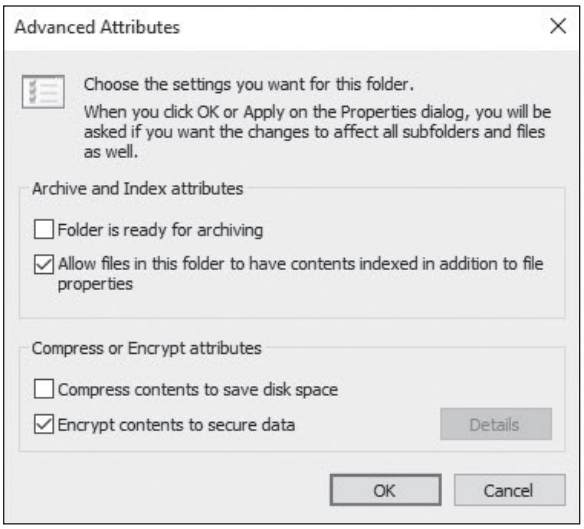



**Figure 2-16**
Encrypting data with EFS

## DECRYPT A FOLDER OR FILE

**GET READY.** To decrypt a folder or file, perform the following steps.

1. Right-click the folder or file you want to decrypt and choose **Properties**.
2. Click the **General** tab and click **Advanced**.
3. Clear the **Encrypt contents to secure data** check box, click **OK**, and then click **OK** again.

**TAKE NOTE***

You cannot encrypt a file with EFS while also compressing a file with NTFS.

The first time a folder or file is encrypted, an encryption certificate is automatically created. If the certificate and key are lost or damaged and there isn't a backup, you won't be able to use the encrypted files. Therefore, always back up your encryption certificate.

## BACK UP AN EFS CERTIFICATE

**GET READY.** To back up an EFS certificate, perform the following steps.

1. Execute the **certmgr.msc** program. If prompted for an administrator password or confirmation, type the password or provide confirmation.
2. In the left pane, double-click **Personal**.
3. Click **Certificates**.
4. In the main pane, click the certificate that lists **Encrypting File System** under the Intended Purposes column. If there is more than one EFS certificate, you should back up all of them.
5. Click **Action > All Tasks > Export**.
6. In the Certificate Export Wizard, click **Next**, click **Yes, export the private key**, and then click **Next**.
7. Click **Personal Information Exchange** and click **Next**.
8. Type the password, confirm the password, and then click **Next**. The export process will create a file to store the certificate.
9. Type a name for the file and the location (include the whole path); or, click **Browse**, navigate to a location, type a file name, and then click **Save**.
10. Click **Next**, click **Finish**, and then click **OK**.

Place the certificate in a safe place. If for some reason, a person leaves the company and you cannot read encrypted files, set up a recovery agent who can recover encrypted files for a domain.

## ADD USERS AS RECOVERY AGENTS

**GET READY.** To add new users as recovery agents, they must first have recovery certificates issued by the enterprise CA structure. Perform the following steps.

1. Using Server Manager, on a domain controller, click **Tools > Group Policy Management**.
2. In the Group Policy Management window, navigate to **Forest: Adatum.com > Domains > Adatum.com**. Then, right-click the **Default Domain Policy** and choose **Edit**.
3. In the Group Policy Management Editor, expand **Computer Configuration\Policies\Windows Settings\Security Settings\Public Key Policies**.
4. Right-click **Encrypting File System** and choose **Add Data Recovery Agent**.
5. In the Add Recovery Agent Wizard, click **Next**.

6. Click **Browse Directory**. Locate the user and click **OK**.
7. Click **Next**.
8. Click **Finish**.
9. Close the Group Policy Editor.

If copying a file or folder, the new folder and file will automatically acquire the encryption attribute of the original drive or folder. If the folder or file is moved within the same volume, the folder or file will retain the original assigned encryption attribute. Thus, if it is encrypted, it will remain encrypted at the new location. When the file or folder is moved from one volume to another, it copies the folder or file to the new location and then deletes the old location. Therefore, the moved folder and files are new to the volume and acquire the new encryption attribute.

## Encrypting Disks in Windows

Different from EFS, BitLocker allows encryption of entire disks. Therefore, if a drive or laptop is stolen, the data is still encrypted even if they install the drive or laptop into another system in which they are an administrator.

BitLocker Drive Encryption is the feature in Windows 10 that makes use of a computer's TPM. A Trusted Platform Module (TPM) is a microchip that is built into a computer. It is used to store cryptographic information, such as encryption keys. Information stored on the TPM can be more secure from external software attacks and physical theft. BitLocker Drive Encryption can use a TPM to validate the integrity of a computer's boot manager and boot files at startup, and to guarantee that a computer's hard disk has not been tampered with while the operating system was offline. BitLocker Drive Encryption also stores measurements of core operating system files in the TPM.

**TAKE NOTE***

BitLocker is a feature of Windows 10 Pro, Enterprise, and Education editions. It is not supported on Windows 10 Home edition.

The system requirements of BitLocker include the following:

- Because BitLocker stores its own encryption and decryption key in a hardware device that is separate from the hard disk, one of the following is required:
  - **A computer with Trusted Platform Module (TPM):** If the computer was manufactured with TPM version 1.2 or higher, BitLocker will store its key in the TPM.
  - **A removable USB memory device, such as a USB flash drive:** If the computer doesn't have TPM version 1.2 or higher, BitLocker will store its key on the flash drive.
- Have at least two partitions—a system partition (which contains the files needed to start the computer, and must be at least 200 MB) and an operating system partition (which contains Windows). The operating system partition will be encrypted and the system partition will remain unencrypted so the computer can start. If the computer doesn't have two partitions, BitLocker will create them. Both partitions must be formatted with the NTFS file system.
- The computer must have a BIOS that is compatible with TPM and supports USB devices during computer startup. If this is not the case, it will be necessary to update the BIOS before using BitLocker.

BitLocker has five operational modes, which define the steps involved in the system boot process. These modes, in descending order from most to least secure, are as follows:

- **TPM + startup PIN + startup key:** The system stores the BitLocker volume encryption key on the TPM chip, but an administrator must supply a personal identification number (PIN) and insert a USB flash drive containing a startup key before the system can unlock the BitLocker volume and complete the system boot sequence.

- **TPM + startup key:** The system stores the BitLocker volume encryption key on the TPM chip, but an administrator must insert a USB flash drive containing a startup key before the system can unlock the BitLocker volume and complete the system boot sequence.
- **TPM + startup PIN:** The system stores the BitLocker volume encryption key on the TPM chip, but an administrator must supply a PIN before the system can unlock the BitLocker volume and complete the system boot sequence.
- **Startup key only:** The BitLocker configuration process stores a startup key on a USB flash drive, which the administrator must insert each time the system boots. This mode does not require the server to have a TPM chip, but it must have a system BIOS that supports access to the USB flash drive before the operating system loads.
- **TPM only:** The system stores the BitLocker volume encryption key on the TPM chip, and accesses it automatically when the chip has determined that the boot environment is unmodified. This unlocks the protected volume and the computer continues to boot. No administrative interaction is required during the system boot sequence.

When enabling BitLocker using the BitLocker Drive Encryption control panel, select the TPM + startup key, TPM + startup PIN, or TPM only option. To use the TPM + startup PIN + startup key option, it is necessary to first configure the Require additional authentication at startup Group Policy setting, found in the Computer Configuration\Policies\Administrative Templates\Windows Components\BitLocker Drive Encryption\Operating System Drives container.

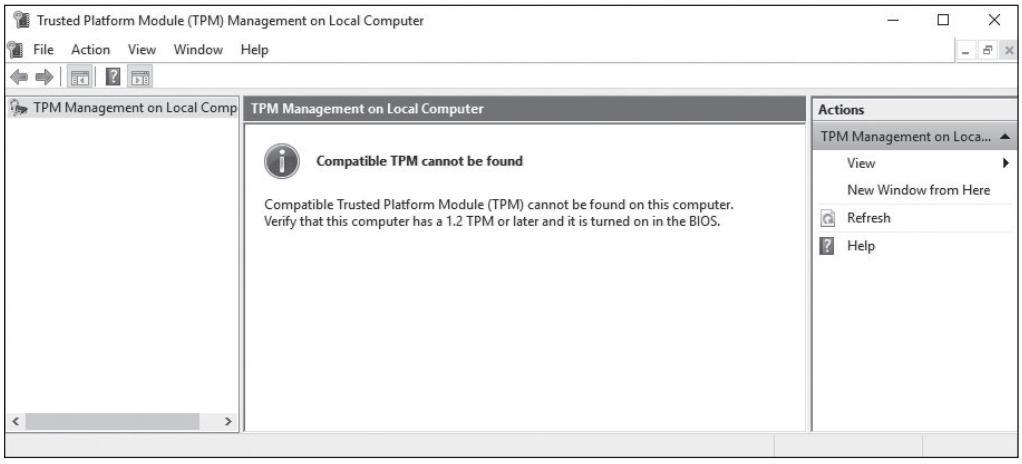
## DETERMINE WHETHER A COMPUTER HAS TPM

**GET READY.** To find out if a computer has Trusted Platform Module (TPM) security hardware, perform the following steps.

1. Right-click **Start** and choose **Control Panel**.
2. Click **System and Security > BitLocker Drive Encryption**.
3. In the left pane, click **TPM Administration**. If prompted for an administrator password or confirmation, type the password or provide confirmation.

The TPM Management on Local Computer snap-in indicates whether the computer has the TPM security hardware. See Figure 2-17. If the computer doesn't have it, a removable USB memory device is necessary to turn on BitLocker and store the BitLocker startup key that will be needed whenever you start the computer.

**Figure 2-17**
The TPM Management console

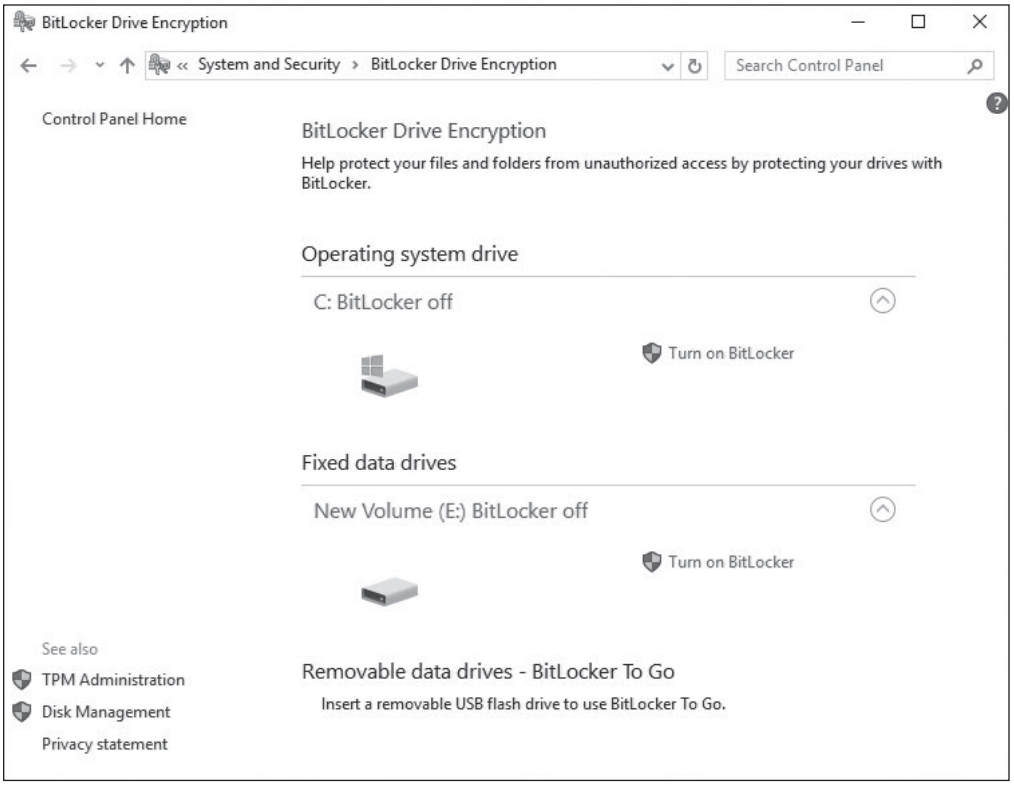


### TURN ON BITLOCKER

**GET READY.** Log on to Windows 10 using an account with administrative privileges. To turn on BitLocker, perform the following steps.

1. Right-click **Start** and choose **Control Panel**.
2. Click **System and Security** > **BitLocker Drive Encryption**. The BitLocker Drive Encryption window appears, as shown in Figure 2-18.

**Figure 2-18**
Turning on BitLocker




**TAKE NOTE*** If a computer has a TPM chip, Windows 10 provides a Trusted Platform Module (TPM) Management console that can be used to change the chip's password and modify its properties.

3. For the E: drive, click **Turn on BitLocker** for your hard disk drives. The Set BitLocker startup preferences page appears.
4. On the Choose how you want to unlock this drive page, click the **Use a password to unlock the drive** option. Then, in the Enter your password text box and the Reenter your password text box, type **Pa$$w0rd**. Click **Next**.
5. On the How do you want to back up your recovery key page, click the **Save to a file** option and click **Next**. The Save your Startup key page appears.
6. In the Save BitLocker recovery key as dialog box, specify the path for the text file, such as **\\LON-DC1\Software**. Then, click **Save**. Click **Next**.
7. On the Choose which encryption mode to use page, the **New encryption mode (best for fixed drives on this device)** option should already be selected. Click **Next**.
8. On the Are you ready to encrypt this drive page, click **Start Encrypting**.
9. When the disk is encrypted, click **Close**.

Once the encryption process is completed, open the BitLocker Drive Encryption window to ensure that the volume is encrypted, or to turn off BitLocker, such as when performing a BIOS upgrade or other system maintenance.

The BitLocker applet allows recovery of the encryption key and recovery password at will. Consider carefully how to store this information, because it will allow access to encrypted data. It is also possible to escrow or store this information into Active Directory.

### DATA RECOVERY AGENTS AND BITLOCKER

If the user loses the startup key and/or startup PIN needed to boot a system with BitLocker, the user can supply the recovery key created during the BitLocker configuration process and gain access to the system. If the user loses the recovery key, use a data recovery agent designated with Active Directory to recover the data on the drive.

A data recovery agent (DRA) is a user account that an administrator has authorized to recover BitLocker drives for an entire organization with a digital certificate on a smart card. In most cases, administrators of Active Directory Domain Services (AD DS) networks use DRAs to ensure access to their BitLocker-protected systems, to avoid having to maintain large numbers of individual keys and PINs.

To create a DRA, first add the user account you want to designate to the Computer Configuration\Policies\Windows Settings\Security Settings\Public Key Policies\BitLocker Drive Encryption container in a GPO or to the system's Local Security Policy. Then, configure the Provide the Unique Identifiers For Your Organization policy setting in the Computer Configuration\Policies\Administrative Templates\Windows Components\BitLocker Drive Encryption container with unique identification fields for your BitLocker drives.

Finally, enable DRA recovery for each type of BitLocker resource to be recovered by configuring the following policies:

- Choose How BitLocker-Protected Operating System Drives Can Be Recovered
- Choose How BitLocker-Protected Fixed Drives Can Be Recovered
- Choose How BitLocker-Protected Removable Drives Can Be Recovered

These policies enable you to specify how BitLocker systems should store their recovery information, and enable you to store it in the AD DS database.

### USING BITLOCKER TO GO

***BitLocker To Go*** is a feature introduced with Windows 7 that enables users to encrypt removable USB devices, such as flash drives and external hard disks. While BitLocker has always supported the encryption of removable drives, BitLocker To Go allows use of the encrypted device on other computers without having to perform an involved recovery process. Because the system is not using the removable drive as a boot device, a TPM chip is not required.

To use BitLocker To Go, insert the removable drive and open the BitLocker Drive Encryption window. The device appears in the interface, with a Turn on BitLocker link just like that of the computer's hard disk drive.

## ■ Understanding IPsec

THE BOTTOM LINE

***IP Security***, more commonly known as ***IPsec***, is a suite of protocols that provide a mechanism for data integrity, authentication, and privacy for the Internet Protocol. It is used to protect data that is sent between hosts on a network by creating secure electronic tunnels between two machines or devices and it can be used for remote access, VPN, server connections, LAN connections, or WAN connections.

**CERTIFICATION READY**
Which security features are included with IPsec?
Objective 3.3

**CERTIFICATION READY**
Which technology protects data transmitted on the wire or over the air?
Objective 3.3

IPsec was designed to provide interoperable, high quality, cryptographically-based security for IPv4 and IPv6, and it provides a comprehensive set of security services, including the following:

- Access control
- Connectionless data integrity checking
- Data origin authentication
- Replay detection and rejection
- Confidentiality using encryption
- Traffic flow confidentiality

IPsec ensures that data cannot be viewed or modified by unauthorized users while being sent to its destination. Before data is sent between two hosts, the source computer encrypts the information by encapsulating each data packet in a new packet that contains the information vnecessary to set up, maintain, and tear down the tunnel when it is no longer needed. The data is then decrypted at the destination computer.

There are a couple of modes and a couple of protocols available in IPsec, depending on whether they are implemented by the end hosts, such as the server, or implemented on the routers and the desired level of security. IPsec can be used in one of two modes:

- **Transport mode (host-to-host):** In transport mode, only the data packet payload is encapsulated. Because the packet header is left intact, the original routing information is used to transmit the data from sender to recipient. When used in conjunction with AH, this mode cannot be used in a NAT environment, as the encryption of the header is not compatible with the translated addressing.
- **Tunnel mode (gateway-to-gateway or gateway-to-host):** In the tunnel mode, the IP packet is entirely encapsulated and given a new header. The host/gateway specified in the new IP header decapsulates the packet. This is the mode used to secure traffic for a remote access VPN connection from the remote host to the VPN concentrator on the internal network. This is also the mode used to secure site-to-site IPsec connections.

The IPsec protocols are:

- **Encapsulating Security Payload (ESP):** Provides confidentiality, authentication, integrity, and anti-replay for the IP payload only, not the entire packet. ESP operates directly on top of IP.
- **Authentication Header (AH):** Provides authentication, integrity, and anti-replay for the entire packet (both the IP header and the data payload carried in the packet). It does not provide confidentiality, which means that it does not encrypt the payload. The data is readable, but protected from modification. Some fields that are allowed to change in transit are excluded because they need to be modified as they are relayed from router to router. AH operates directly on top of IP.
- **Internet Key Exchange (IKE):** IKE is used to negotiate, create, and manage security associations (SA), which means that it is the protocol that establishes the secure communication channel between two network hosts.

ESP and AH can be combined to provide authentication, integrity, and anti-replay for the entire packet (both the IP header and the data payload carried in the packet) and confidentiality for the payload.

While AH and ESP provide the means to protect data from tampering, preventing eavesdropping, and verifying the origin of the data, it is the Internet Key Exchange (IKE) that defines the method for the secure exchange of the initial encryption keys between the two endpoints. IKE allows nodes to agree on authentication methods, encryption methods, the keys to use, and the lifespan of the keys.

The information negotiated by IKE is stored in a Security Association (SA). An SA is like a contract laying out the rules of the VPN connection for the duration of the SA. An SA is

assigned a 32-bit number that, when used in conjunction with the destination IP address, uniquely identifies the SA. This number is called Security Parameters Index (SPI).

In order for IPsec to work in conjunction with NAT, the following protocols need to be allowed across the firewall:

- **Internet Key Exchange (IKE):** User Datagram Protocol (UDP) port 500
- **Encapsulating Security Payload (ESP):** IP protocol number 50
- **Authentication Header (AH):** IP protocol number 51

IPsec can be used with Windows in various ways. To enable IPsec communications for a Windows Server 2008 or higher computer, create group policies and assign them to individual computers or groups of computers. You can also use the Windows Firewall with Advanced Security.

## Encrypting with VPN Technology

Today, it is very common for an organization to use remote access server (RAS), which enables users to connect remotely using various protocols and connection types. By connecting to RAS over the internet, users can connect to their organization's network so that they can access data files, read email, and access other applications just as if they were sitting at work. Because the internet is considered an insecure medium, encryption must be used to secure the data.

A ***virtual private network (VPN)*** links two computers through a wide-area network, such as the internet. To keep the connection secure, the data sent between the two computers is encapsulated and encrypted. In one scenario, a client connects to the RAS server to access internal resources from offsite. Another scenario is to connect one RAS server on one site or organization to another RAS server on another site or organization so that the site or organizations can communicate with each other.

The three types of tunneling protocols used with a VPN server/RAS server running on Windows Server 2008 R2 include:

- **Point-to-Point Tunneling Protocol (PPTP):** A VPN protocol based on the legacy Point-to-Point protocol used with modems. Although PPTP is easy to set up, it is considered weak encryption technology.
- **Layer 2 Tunneling Protocol (L2TP):** Used with IPsec to provide security. It is the industry standard when setting up secure tunnels.
- **Secure Socket Tunneling Protocol (SSTP):** Introduced with Windows Server 2008, which uses the HTTPS protocol over TCP port 443 to pass traffic through firewalls and web proxies that might block PPTP and L2TP/IPsec.
- **IKEv2 (short for Internet Key Exchange version 2):** This protocol uses IPsec for encryption while supporting VPN Reconnect (also called Mobility), which enables VPN connections to be maintained when a VPN client moves between wireless cells or switches, and to automatically reestablish broken VPN connectivity. Different from L2TP with IPsec, IKEv2 client computers do not need to provide authentication through a machine certificate or a pre-shared key.

When using VPNs, Windows 10 and Windows Server 2016 support the following forms of authentication:

- **Password Authentication Protocol (PAP):** Uses plain text (unencrypted passwords). PAP is the least secure authentication and is not recommended.

- **Challenge Handshake Authentication Protocol (CHAP):** A challenge-response authentication that uses the industry standard md5 hashing scheme to encrypt the response. CHAP was an industry standard for years and is still quite popular.
- **Microsoft CHAP version 2 (MS-CHAP v2):** Provides two-way authentication (mutual authentication). MS-CHAP v2 provides stronger security than CHAP.
- **Extensible Authentication Protocol (EAP):** EAP is a universal authentication framework that allows third-party vendors to develop custom authentication schemes, including retinal scans, voice recognition, fingerprint identification, smart cards, Kerberos, and digital certificates. It also provides a mutual authentication method that supports password-based user or computer authentication.

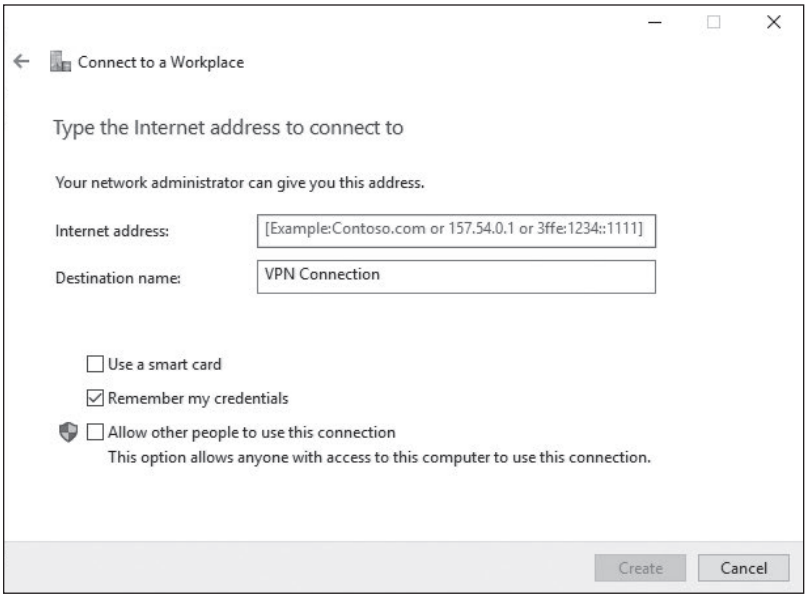
## CREATE A VPN TUNNEL

**GET READY.** To create a VPN tunnel on a computer running Windows 10 so that you can connect to a Remote Access Server, perform the following steps.

1. In Control Panel, click **Network and Internet > Network and Sharing Center**.
2. Click **Set up a new connection or network**.
3. In the Set Up a Connection or Network window, click **Connect to a workplace** and click **Next**.
4. In the Connect to a Workplace window, click **Use my Internet connection (VPN)**.
5. On the next screen (see Figure 2-19), select your VPN connection or specify the internet address for the VPN server and a Destination name. Optionally, select the **Use a Smart card**, **Remember my credentials**, and **Allow other people to use this connection** check boxes.

**Figure 2-19**

Setting up a VPN connection

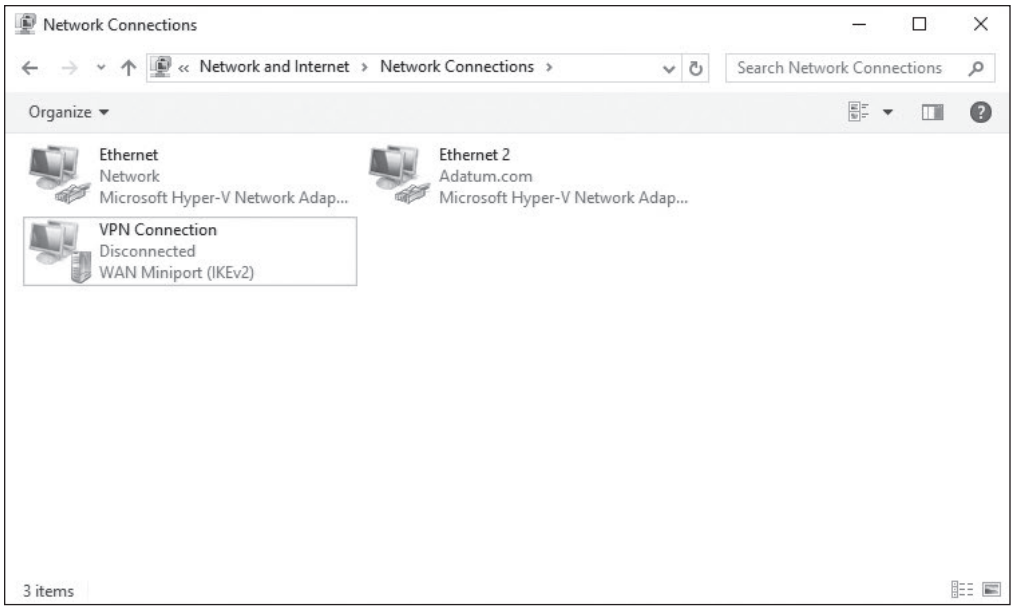



Often, additional configuration of your VPN connection may be needed, such as specifying the type of protocol, which authentication protocol to use, and the type of encryption.

When the VPN connection is created and configured to connect using the VPN, open the Network and Sharing Center and click Change adapter settings. Then, right-click the VPN

connection and choose Connect to open the Connect to a Workplace dialog box, as shown in Figure 2-20.

**Figure 2-20**
Connecting to a VPN




Another method for Windows 10 is to right-click the network status icon on the taskbar and choose the VPN connection. In the Settings window, click the VPN connection and click Connect.

By default, when connecting to a VPN using the previous configuration, all web browsing and network traffic goes through the default gateway on the Remote Network unless you are communicating with local home computers. Having this option enabled helps protect the corporate network, because all traffic will also go through firewalls and proxy servers and help prevent a network from being infected or compromised.

To route your browsing through a home internet connection rather than going through the corporate network, disable the "Use default gateway on remote network" option. When disabling this option, it is called using split tunnel.

### ENABLE SPLIT TUNNELING

**GET READY.** To enable split tunneling, perform the following steps.

1. Right-click a VPN connection and choose **Properties**.
2. Click the **Networking** tab.
3. Double-click **Internet Protocol Version 4 (TCP/IPv4)**.
4. Click the **Advanced** button.
5. Deselect the **Use default gateway on remote network** check box.

It can be a lot of work to configure multiple clients to connect to a remote access server and may be too complicated for a computer novice.

Configuring multiple clients to connect to a remote server can be a daunting task that is prone to errors. To help simplify the administration of the VPN client into an easy to install executable, use Connection Manager Administration Kit (CMAK). To install CMAK on Windows Server 2016, install it as a feature.

## ■ Introducing Smart Cards

**THE BOTTOM LINE**

Used with a smart card reader attached to a computer, smart cards contain an embedded processor that is used to communicate with the host computer and the card reader. They can be used to authenticate users, ensure data integrity when signing documents, and provide confidentiality when encryption is needed. In order to authenticate, users insert their cards into readers connected to their computers and then type their PINs. The smart card holds the user's logon information, private key, digital certificate, and other private information.

**CERTIFICATION READY**
How does virtual smart card resemble a physical smart card?
Objective 2.1

To deploy smart cards, it is necessary to use a public key infrastructure (PKI), which includes digital certificates, CAs, and other components that are used to create, distribute, validate, and revoke certificates. Smart cards can be credit card-sized devices or a token style (USB) device. Information stored on the cards cannot be extracted from the device—all communication with the card is encrypted to protect against malicious software intercepting it, and brute force attempts to hack the PIN will result in the card being blocked until an administrator can unlock it. Because both the smart card and a PIN are required, it is much less likely that someone will be able to steal both.

Windows 8 introduced ***virtual smart cards (VSCs)***, which make additional hardware (smart card readers and smart cards) unnecessary. These cards emulate the functionality of regular smart cards, but require a ***Trusted Platform Module (TPM) chip***–an international standard for a secure cryptoprocessor—to protect the private keys. The TPM is used to encrypt the information, which is then stored on the computer's hard drive. If the user needs to access multiple computers using the VSC, the user will need a new VSC for each system.

It is also possible to use multiple VSCs (one for each user) on multi-use computers. If a computer is lost or stolen, the user can contact an administrator, who can revoke the certificate associated with the VSC on the user's computer.

### SET UP A VIRTUAL TPM SMART CARD ENVIRONMENT

**GET READY.** To set up a virtual TPM smart card environment, you must have a computer running Windows 10 (TPM supported), you must be connected to a domain, and you must have access to a domain server with a functional CA in place. Perform the following steps.

1. Create a certificate template (on the domain controller). This is the certificate that will be requested in Step 3 on the client.
2. Create the VSC on the Windows 10 client machine using the TPM VSC Manager and then type a PIN.
3. Use the Certificate console on the Windows 10 client machine to request a new certificate and then select the certificate that was created in Step 1.

After these steps are completed, use the VSC the next time you boot your system.

For authentication, virtual smart cards use two-factor authentication. The user must have the computer with the virtual smart card and the user must know the PIN associated with the smart card.

Besides the TPM chip, the computer must be running Windows 8 or higher, must be part of the domain, and must have access to the certificate authority (CA). Then, follow these steps:

1. Create the certificate template, which is based on the Smartcard Logon.
2. Create the TPM virtual smart card.
3. Enroll the certificate on the TPM virtual smart card.

## CREATE A CERTIFICATE TEMPLATE

**GET READY.** To create a certificate template on the Certificate Authority, perform the following steps.

1. On LON-DC1, click **Start** and type **mmc** to open the Microsoft Management Console (MMC).
2. Click **File > Add/Remove Snap-in**.
3. In the available snap-ins list, double-click **Certificate Templates** and click **OK**.
4. Double-click **Certificate Templates** to view all available certificate templates.
5. Right-click the **Smartcard Logon** template and choose **Duplicate Template**.
6. On the Compatibility tab, under Certification Authority, click **Windows Server 2003**.
7. On the General tab, specify the following:
   - For the name, type **TPM Virtual Smart Card Logon**.
   - Set the validity period to the desired value.
8. On the Request Handling tab, set the Purpose to **Signature and smartcard logon**. Click **Prompt the user during enrollment**.
9. On the Cryptography tab, set the minimum key size to **2048**. Click **Requests must use one of the following providers** and select the **Microsoft Base Smart Card Crypto Provider** check box.
10. On the Security tab, add the security group to which you want to provide enroll access. If you want to give access to all users, select the **Authenticated** users group and give them **Enroll** permissions.
11. Click **OK** to close the Properties of New Template dialog box.
12. Using Server Manager, click **Tools > Certificate Authority**.
13. In the left pane of the MMC, expand **Certification Authority (Local)**, and then expand your CA within the Certification Authority list.
14. Right-click **Certificate Templates** and choose **New > Certificate Template to Issue**.
15. From the list, select **TPM Virtual Smart Card Logon** and click **OK**.

## CREATE A TPM VIRTUAL SMART CARD

**GET READY.** To create a TPM virtual smart card on a domain-joined computer running Windows 10, perform the following steps.

1. On LON-DC1, open a command shell with administrative privileges.
2. At the command prompt, execute the following command:

   ```
   tpmvscmgr.exe create /name tpmvsc /pin default /adminkey random /generate
   ```

3. When prompted for a PIN, type a PIN that is at least eight characters in length and then confirm it.
4. Wait several seconds for the process to finish.

Upon completion, tpmvscmgr.exe will provide the device instance ID for the TPM VSC. Store this ID for later reference; it will be needed to manage or remove the VSC.

### ENROLL FOR THE CERTIFICATE ON THE TPM VIRTUAL SMART CARD

**GET READY.** To enroll for the certificate on the TPM virtual smart card on the domain-joined computer running Windows 10, perform the following steps.

1. On LON-DC1, click **Start** and type **certmgr.msc** to open the Certificates console.
2. Right-click **Personal** and choose **All Tasks > Request New Certificate**.
3. On the Before You Begin page, click **Next.**
4. On the Select Certificate Enrollment Policy page, click **Next.**
5. On the Request Certificates page, select **TPM Virtual Smart Card Logon** and click **Enroll.**
6. If prompted for a device, select **Microsoft virtual smart card.**
7. Type the PIN for the TPM smart card that you entered when creating the VSC and click **OK.**
8. Wait for the enrollment to finish and then click **Finish.**

## ■ Configuring Biometrics, Windows Hello, and Microsoft Passport

**THE BOTTOM LINE**

In the past, administrators had to struggle with managing third-party software and hardware to support biometrics. With each vendor providing different drivers, software, and management tools, it became very labor-intensive to support. Fortunately, Microsoft introduced native support for biometric technologies through its ***Windows Biometric Framework (WBF)***. WBF enables users to manage device settings for biometric devices through Control Panel, provides support for managing device drivers, and manages Group Policy settings that can be used to enable, disable, or limit use of biometric data for a local computer or domain.

**CERTIFICATION READY**
Can you describe what is meant by the term biometrics?
Objective 2.1

A fingerprint reader is the most commonly used biometric device in corporate networks. These devices can be purchased separately or can be built in to new laptops. The reader captures an image of your fingerprint and then saves it to the computer. This process is called enrolling. When you log on, the reader scans your fingerprint and compares it to the fingerprint on file.

***Windows Hello*** is a Windows 10 biometric authentication system that uses a user's face, iris, or fingerprint to unlock devices. To use Windows Hello, specialized hardware is needed, including a fingerprint reader, illuminated infrared (IR) sensor, or other biometric sensors. Windows Hello will not work with an ordinary webcam, but it will work with an existing fingerprint sensor.

### SET UP WINDOWS HELLO FACIAL RECOGNITION

**GET READY.** To set up Windows Hello facial recognition on a computer running Windows 10, perform the following steps.

1. On LON-CL1, click **Start > Settings**.
2. Click **Accounts**.
3. Click **Sign-in options**.
4. Under Windows Hello, select the **infrared IR camera** option. If a Windows Hello section is not shown, you do not have compatible hardware.
5. On the Welcome to Windows Hello page, click the **Get Started** button.

6. Set up a PIN code if prompted to do so.
7. To scan your face, for best results, hold your face six to eight inches away from the front of the camera.
8. Click **Finish** to complete scanning or click **Improve Recognition** to continue scanning.

## SET UP WINDOWS HELLO FINGERPRINT READER

**GET READY.** To set up a Windows Hello fingerprint reader on a computer running Windows 10, perform the following steps.

1. On LON-CL1, click **Start** > **Settings**.
2. Click **Accounts**.
3. Click **Sign-in options**.
4. Under Windows Hello, select the **Fingerprint** option and click **Set up**. If a Windows Hello section is not shown, you do not have compatible hardware.
5. On the Welcome to Windows Hello page, click the **Get Started** button.
6. Repeatedly place your preferred finger on the fingerprint ID sensor on your type cover. The system will tell you when setup is complete. You can set up multiple fingers to be read by the scanner.
7. Click **Finish** to complete scanning.

***Microsoft Passport*** is a two-factor authentication that consists of an enrolled device (such as a smartphone) and a Windows Hello (biometric) or PIN. The two factors are an encrypted key stored on the device combined with Windows Hello or a PIN. Microsoft Passport lets users authenticate to a Microsoft account, an Active Directory account, a Microsoft Azure Active Directory (AD) account, or a non-Microsoft service that supports Fast ID Online (FIDO) authentication.

TAKE NOTE*

Don't confuse Microsoft Passport used with Windows 10 with the Microsoft Account, which was previously known as Microsoft Passport. Microsoft Account is a single sign-on web server developed and provided by Microsoft that allows users to log on to websites, devices, and applications using one account. It is also known as .NET Passport, Microsoft Passport Network, or Windows Live ID.

To implement Microsoft Passport, one of the following is needed:

- Microsoft account
- Azure Active Directory
- Windows Server 2016 Active Directory

To implement Microsoft Passport using a Microsoft account, perform the following steps:

1. Log on with a Microsoft account on a computer running Windows 10.
2. Configure a PIN or Windows Hello.

After performing the initial two-step verification during Microsoft Passport enrollment, a Microsoft Passport is set up on the user's device and the user gets a gesture, which can be Windows Hello or a PIN.

To implement Microsoft Password in your organization, create a Group Policy that will implement Microsoft Passport on devices running Windows 10. The GPO settings are located at:

Computer Configuration > Policies > Administrative Templates > Windows Components > Microsoft Passport for Work

## ■ Using Auditing to Complete the Security Picture

**THE BOTTOM LINE**

As mentioned before, security can be divided into three areas. Authentication is used to prove the identity of a user while authorization gives access to the user that was authenticated. To complete the security picture, enable auditing, so that you can have a record of the users who have logged on and what the users accessed or tried to access.

**CERTIFICATION READY**
Why is auditing so important to security?
Objective 2.4

It is important to protect your information and service resources from people who should not have access to them, and at the same time make those resources available to authorized users. Along with authentication and authorization, enable auditing so that you can have a record of the following:

- Who has successfully logged on
- Who has attempted to log on, but failed
- Who has changed accounts in Active Directory
- Who has accessed or changed certain files
- Who has used a certain printer
- Who restarted a system
- Who has made some system changes

In Windows, auditing is not enabled by default. To enable auditing, specify what types of system events to audit using group policies or the local security policy (Security Settings\Local Policies\Audit Policy). See Figure 2-21.

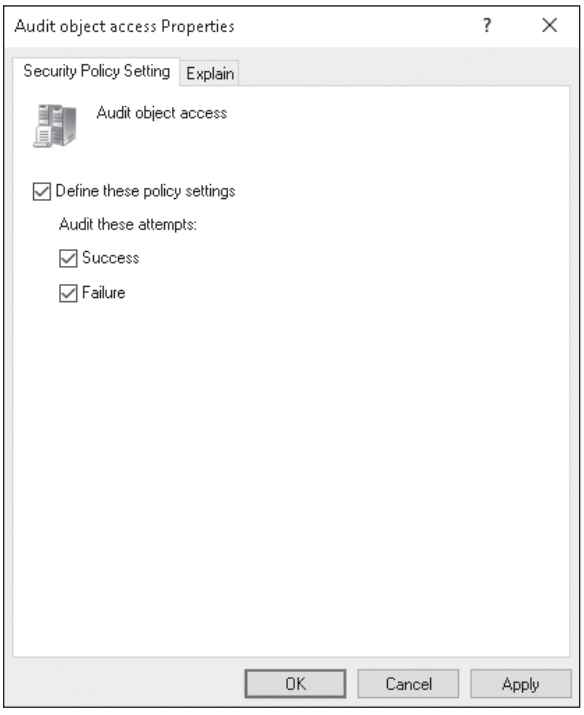



**Figure 2-21**
Enabling auditing using group policies

**Table 2-3**
Audit Events

| Event | Explanation |
|---|---|
| Account Logon | Determines whether the OS audits each time the computer validates an account's credentials, such as account logon. |
| Account Management | Determines whether to audit each event of account management on a computer, including changing passwords, and creating or deleting user accounts. |
| Directory Service Access | Determines whether the OS audits user attempts to access Active Directory objects. |
| Logon | Determines where the OS audits each instance of a user attempting to log on, or log off, her computer. |
| Object Access | Determines whether the OS audits user attempts to access non-Active Directory objects, including NTFS files and folders and printers. |
| Policy Change | Determines whether the OS audits each instance of attempts to change user rights assignments, auditing policy, account policy, or trust policy. |
| Privilege Use | Determines whether to audit each instance of a user exercising a user right. |
| Process Tracking | Determines whether the OS audits process-related events, such as process creation, process termination, handle duplication, and indirect object access. This is usually used for troubleshooting. |
| System | Determines whether the OS audits if the system time is changed, system startup or shutdown, attempts to load extensible authentication components, loss of auditing events due to auditing system failure, and security logs exceeding a configurable warning threshold level. |

Table 2-3 shows the basic events to audit that are available in Windows Server 2016. Windows Server 2008 and higher have additional options for more granular control. After you enable logging, open the Event Viewer security logs to view the security events. By default, the security logs can only be seen and managed by the Administrators group.

To audit NTFS files, NTFS folders, and printers is a two-step process. First, enable Object Access using group policies. Then, specify which files or folders you want to audit or which printer you want to audit. After you enable logging, open the Event Viewer security logs to view the security events.

Because Windows is only part of what makes up a network, also look at other areas to audit. For Microsoft's web server, IIS, enable logging of who visits each site. For Microsoft's Internet Security and Acceleration (ISA) and Microsoft's Threat Management Gateway (TMG) servers, enable logging to record who accesses your network through a VPN or what is accessed through the firewall. If your company has Cisco routers and firewalls, enable auditing so that if someone reconfigures the router and firewall, there is a record of it.

To audit non-Microsoft products, it might be necessary to use Syslog. ***Syslog*** is a standard for logging program messages that can be accessed by devices that would not otherwise have a method for communications. For example, Cisco firewalls and routers, computers running Linux and UNIX, and many printers can use Syslog. Syslog can be used for computer system management and security auditing as well as generalized informational, analysis, and debugging messages.

Lastly, make sure there is a change management system and a ticket system. A change management system will record what changes are made. It gives the IT department a method to review the changes before they are implemented, so that if the change could cause problems with a system, it can be raised as a concern. In addition, if a problem does occur, all the changes made to your environment will be listed in a single place.

The ticket system will provide a record of all problems and requests by users. A ticket system helps to determine the most common problems and identify trends.

## AUDIT FILES AND FOLDERS

**GET READY.** Assuming object auditing has been enabled, to audit files and folders, perform the following steps.

1. Open **File Explorer**.
2. Right-click the file or folder that you want to audit, choose **Properties**, and then click the **Security** tab.
3. Click **Advanced**.
4. In the Advanced Security Settings for <object> dialog box, click the **Auditing** tab.
5. Do one of the following:
   - To set up auditing for a new user or group, click **Add**. In the Enter the object name to select box, type the name of the user or group and click **OK**.
   - To remove auditing for an existing group or user, click the group or user name, click **Remove**, click **OK**, and then skip the rest of this procedure.
   - To view or change auditing for an existing group or user, click its name and click **Edit**.
6. In the **Apply onto** box, click the location where auditing should take place.
7. In the **Access** box, indicate what actions should be audited by selecting the appropriate check boxes:
   - To audit successful events, select the **Successful** check box.
   - To stop auditing successful events, clear the **Successful** check box.
   - To audit unsuccessful events, select the **Failed** check box.
   - To stop auditing unsuccessful events, clear the **Failed** check box.
   - To stop auditing all events, click **Clear All**.
8. If you want to prevent subsequent files and subfolders of the original object from inheriting these audit entries, select the **Apply these auditing entries to objects and/or containers within this container only** check box.
9. Click **OK** to close the Advanced Security Settings dialog box.
10. Click **OK** to close the Properties dialog box.

## SKILL SUMMARY

**In this lesson, you learned:**

- In security, AAA (Authentication, Authorization, and Accounting) is a model for access control.
- Authentication is the process of identifying an individual.
- After a user is authenticated, users can access network resources based on the user's authorization. Authorization is the process of giving individuals access to system objects based on their identity.
- Accounting, also known as Auditing, is the process of keeping track of a user's activity while accessing the network resources, including the amount of time spent on the network, the services accessed while there, and the amount of data transferred during the session.
- Nonrepudiation prevents one party from denying actions they carried out.
- A user can authenticate using what they know, what they own or possess, and who they are.
- When two or more authentication methods are used to authenticate someone, a multi-factor authentication system is being implemented.
- The most common method of authentication with computers and networks is the password.
- A password is a secret series of characters that enables a user to access a file, computer, or program.
- To hack a password, users will try obvious passwords, brute force attacks, and dictionary attacks.
- To make a password more secure, be sure to choose a password that nobody can guess. Therefore, it should be lengthy and should be considered a strong or complex password.
- A personal identification number (PIN) is a secret numeric password shared between a user and a system that can be used to authenticate the user to the system.
- The digital certificate is an electronic document that contains an identity such as a user or organization and a corresponding public key.
- A smart card is a pocket-sized card with embedded integrated circuits consisting of non-volatile memory storage components, and perhaps dedicated security logic.
- A smart card can contain digital certificates to prove the identity of someone carrying the card and may also contain permissions and access information.
- Biometrics is an authentication method that identifies and recognizes people based on voice recognition or physical traits such as a fingerprint, face recognition, iris recognition, and retina scan.
- Because administrators have full access to a computer or the network, it is recommended that a standard non-administrator user should perform most tasks.
- Active Directory is a technology created by Microsoft that provides a variety of network services, including LDAP, Kerberos-based and single sign-on authentication, DNS-based naming and other network information, and central location for network administration and delegation of authority.
- Kerberos is the default computer network authentication protocol, which allows hosts to prove their identity over a non-secure network in a secure manner.
- Single sign-on (SSO) allows a user to log on once and access multiple, related, but independent software systems without having to log on again.
- A user account enables a user to log on to a computer and domain.
- The local user account is stored in the Security Account Manager (SAM) database on the local computer.

- A group is much like it sounds; it is used to group users and computers together so that when rights and permissions are assigned, they are assigned to the group rather than to each user individually.
- A right authorizes a user to perform certain actions on a computer, such as logging on to a system interactively or backing up files and directories on a system.
- A permission defines the type of access that is granted to an object (an object can be identified with a security identifier) or object attribute.
- Explicit permissions are permissions granted directly to the file or folder.
- Inherited permissions are permissions that are granted to a folder (parent object or container) that flow into child objects (subfolders or files inside the parent folder).
- The owner of the object controls how permissions are set on the object and to whom permissions are granted.
- Encryption is the process of converting data into a format that cannot be read by another user. Once a user has encrypted a file, it automatically remains encrypted when the file is stored on disk.
- Decryption is the process of converting data from encrypted format back to its original format.
- Encryption algorithms can be divided into three classes: Symmetric, Asymmetric, and Hash function.
- Symmetric encryption uses a single key to encrypt and decrypt data. Therefore, it is also referred to as secret-key, single-key, shared-key, and private-key encryption.
- Asymmetric encryption, also known as public key cryptography, uses two mathematically related keys. One key is used to encrypt the data, while the second key is used to decrypt the data.
- Different from the symmetric and asymmetric algorithms, a hash function is meant as a one-way encryption. This means that after it has been encrypted, it cannot be decrypted.
- A public key infrastructure (PKI) is a system consisting of hardware, software, policies, and procedures that create, manage, distribute, use, store, and revoke digital certificates.
- The most common digital certificate is the X.509 version 3.
- The certificate chain, also known as the certification path, is a list of certificates used to authenticate an entity. It begins with the certificate of the entity and ends with the root CA certificate.
- A digital signature is a mathematical scheme that is used to demonstrate the authenticity of a digital message or document. It is also used to confirm that the message or document has not been modified.
- When surfing the internet and needing to transmit private data over the internet, use SSL over HTTPS (https) to encrypt the data sent over the internet. By convention, URLs that require an SSL connection start with https: instead of http:.
- IP Security, more commonly known as IPsec, is a suite of protocols that provide a mechanism for data integrity, authentication, and privacy for the Internet Protocol.
- Virtual private network (VPN) links two computers through a wide-area network, such as the internet.
- Windows Hello is a Windows 10 biometric authentication system that uses a user's face, iris, or fingerprint to unlock devices.
- Syslog is a standard for logging program messages that can be accessed by devices that would not otherwise have a method for communications.

# Knowledge Assessment

## Multiple Choice

*Select the correct answer(s) for each of the following questions.*

1. Which of the following is *not* a method for authentication?
   - **a.** Something the user knows
   - **b.** Something the user owns or possesses
   - **c.** Encryption
   - **d.** Something a user is
2. Which of the following would *not* be a biometric device?
   - **a.** Password reader
   - **b.** Retina scanner
   - **c.** Fingerprint scanner
   - **d.** Face scanning
3. Which service is used for centralized authentication, authorization, and accounting?
   - **a.** VPN
   - **b.** PGP
   - **c.** RADIUS
   - **d.** PKI
4. Which of the following is the primary authentication used on Microsoft Active Directory?
   - **a.** LDAP
   - **b.** Kerberos
   - **c.** NTLAN
   - **d.** SSO
5. Which of the following is the master time keeper and master for password changes in an Active Directory domain?
   - **a.** PDC Emulator
   - **b.** RID
   - **c.** Infrastructure master
   - **d.** Schema master
6. Local user accounts are found in which of the following?
   - **a.** Active Directory
   - **b.** Registry
   - **c.** SAM
   - **d.** LDAP
7. Which of the following authorizes a user to perform certain actions on a computer?
   - **a.** Permissions
   - **b.** An encryption algorithm
   - **c.** Authentication protocol
   - **d.** A right
8. Which file system offers the best security?
   - **a.** FAT
   - **b.** FAT32
   - **c.** NTFS
   - **d.** EFS

9. Which NTFS permission is needed to change attributes and permissions?
   a. Full Control
   b. Modify
   c. Read & Execute
   d. Write

10. Which permission is granted directly to the file or folder?
   a. Explicit
   b. Inherited
   c. Effective
   d. Share

11. When copying a file or folder to a new volume, which permissions are acquired?
   a. The same permissions that it had before.
   b. The same permissions as the target folder.
   c. The same permissions as the source folder.
   d. No permissions

12. Which of the following uses an ACL? (Choose all that apply.)
   a. NTFS folder
   b. Active Directory user
   c. Registry key
   d. Logon rights

13. Which type of key has one key for encryption and a different key for decryption?
   a. Symmetric
   b. Asymmetric
   c. Hash function
   d. PKI

14. Which infrastructure is used to assign and validate digital certificates?
   a. Asymmetric algorithm
   b. Active Directory
   c. PKI
   d. VPN

15. Which technology is used to encrypt an individual file on an NTFS volume?
   a. BitLocker
   b. BitLocker To Go
   c. PPTP
   d. EFS

16. Which physical device is used to authenticate users based on what a user has?
   a. Smart card
   b. Windows Hello
   c. Universal Windows Platform
   d. Device Guard

17. Which of the following is a two-factor authentication that uses an enrolled device and Windows Hello?
   a. Device Guard
   b. Credential Guard
   c. Virtual secure mode
   d. Microsoft Passport

### Fill in the Blank

*Complete the following sentences by writing the correct word or words in the blanks provided.*

1. A(n) _____ is a secret numeric password shared between a user and a system that can be used to authenticate the user to the system.
2. A pocket-sized card with embedded integrated circuits used for authentication is known as a(n) _____.
3. A device that may provide a second password to log on to a system is a(n) _____.
4. The _____ holds a copy of the centralized database used in Active Directory.
5. By default, a computer clock should not be off more than _____ minutes or there might be problems with Kerberos authentication.
6. A(n) _____ defines the type of access over an object or the properties of an object such as an NTFS file or printer.
7. The _____ permissions flow from the parent object to the child object.
8. When a folder cannot be accessed because someone removed the permissions so that no one can access it, it is necessary to take _____ of the folder.
9. The centralized database that holds most of the Windows configurations is known as the _____.
10. To track a user's activities in Windows, it is necessary to enable _____.

## ■ Business Case Scenarios

### Scenario 2-1: Understanding Biometrics

As an IT administrator for the Contoso Corporation, your CIO wants you to investigate the corporation using biometrics. The CIO understands what biometrics is and how it can be used. But he does not understand the disadvantages of using biometrics. Describe your recommended solution.

### Scenario 2-2: Limiting Auditing

As an IT administrator for the Contoso Corporation, your CIO needs to know when a particular user accessed a folder. However, the information was not available because auditing was not enabled. To ensure that this does not happen in the future, the CIO asks you to enable auditing for everything. Describe your recommended solution.

### Scenario 2-3: Assigning NTFS Permissions

As an IT administrator for the Contoso Corporation, you are tasked with assigning NTFS permissions. You will need to log on as an administrator on a computer running Windows 10. Create a group called Managers on your computer. Create a user account called JSmith and assign it to the Managers group. Create another user account called JHamid. Create a folder called SharedTest. Create a text file called test.txt in the SharedTest folder. Share the folder. Assign Allow Full Control to Everyone, and assign Read & Execute to the Managers group. Log on as JHamid and try to access the \\localhost\SharedTest folder. Log on as JSmith and try to access the \\localhost\SharedTest folder. Describe the step-by-step procedure for assigning NTFS permissions.

### Scenario 2-4: Using EFS

In this exercise, you will describe how to use EFS. Add JHamid to the Managers group. Log on as JSmith. Encrypt the test.txt file with EFS. Log on as JHamid and try to access the test .txt file.

## Workplace Ready

### Planning and Maintaining Security

When planning security, you need to consider the big picture. Security must be planned from the beginning. Therefore, define what the goals of the security need to be, determine what effect it will have on current access and network applications, and look at how it will affect the users. After security is implemented, maintain it by constantly monitoring the security of the system, making changes as needed, patching security holes, and constantly reviewing the security logs.