**Module 6 – Managing resources**

**Module Overview**

Your users need access to resources such as files and printers. A typical way to facilitate this access is to share those resources. However, when you share file server resources, it’s important that those resources are secured properly.

In this module, you’ll learn how to secure file resources by using file permissions. You’ll also learn how to make those file resources available by creating shared folders, and using Work Folders to enable offsite access to your users’ files. Finally, you’ll learn about managing and securing shared printers.

**Objectives**

After completing this module, you will be able to:

* Configure and manage file access.
* Configure and manage shared folders.
* Implement Work Folders.
* Manage printers.

Lesson 1

**Configuring and managing file access**

Users need to share documents and other content with coworkers. In on-premises networks, you’ll likely be using file servers to facilitate this collaboration. In the last module, you learned about file systems and storage. In this lesson, you’ll learn how to secure files and folders that your users want to access.

**Lesson Objectives**

After completing this lesson, you will be able to:

* Describe the available tools for managing files and folders.
* List the available file and folder permissions.
* Describe the principle of inheritance.
* Use conditions to control file and folder access.
* Configure file and folder permissions.
* Review permissions using Effective Access.

**File and folder management tools**

There are a number of ways in which you can manage files and folders. For most situations, you’ll probably want to use File Explorer. But in some situations, it might be quicker to use Windows PowerShell, or the available Command Prompt tools.

**File Explorer**

You can use File Explorer to perform all common file management tasks, such as:

* Copying and moving files and folders.
* Renaming files and folders.
* Creating and deleted files and folders.
* Managing the file and folder properties, including:
* **General**. Includes name, and basic and advanced attributes.
* **Security**. Basic and advanced file or folder permissions.
* **Details**. Additional attributes, including Title, subject. Last printed, editing time and so on.
* **Previous Versions**. Useful for file recovery, if enabled on your computer.

File Explorer has changed in Windows 11, and users of Windows 10 might notice some small differences when working with files. The most notable difference is in the context menu; this now contains only the most common file or folder activities.

To access less frequently used file or folder tasks, you must select **Show more options**. This displays a context menu much like the one used in Windows 10.

**Command Prompt**

The Command Prompt has been part of Windows for decades. The file and folder management commands available in Command Prompt are, for the most part, the same as in the original Command Prompt from MS-DOS. The following list describes some of the more common commands:

* **cd**. Change directory.
* **md**. Make a new directory.
* **Copy**. Copies a file or folder.
* **Move**. Moves a file or folder.
* **Dir**. Lists the contents of the current folder.
* **Del**. Deletes the specified files of folders.

You can use the **icacls.exe** command to manage file or folder permissions. This is a powerful command-line tool, and you should exercise caution using it.

For example, to grant the user Oliver delete and write DAC permissions on a file called Document.doc, you’d use the following command:

icacls Document.doc /grant Oliver:(d,wdac)

**Windows PowerShell**

You can use Windows PowerShell to execute the commands supported by Command Prompt. But you can also use PowerShell cmdlets. These include:

* **Set-Location**. Changes the current directory.
* **Get-ChildItem**. Retrieves a list of the current folder’s contents. A bit like Dir.
* **New-Item**. Enables you to create a file or folder. Use the **-ItemType “directory”** parameter to create a folder.
* **Copy-Item**. Enables you to copy file system objects.
* **Rename-Item**. Enables you to change the name of a file or folder.
* **Remove-Item**. Deletes the specified file or folder.

To manage permissions, you’ll use the Get-ACL or Set-ACL cmdlets to manage file permissions using Windows PowerShell.

In the following example, the permissions of a file called Doc1 are retrieved and applied to a file called Doc2:

$DocACL = Get-Acl -Path "C:\Doc1.doc"

Set-Acl -Path "C:\Doc2.doc" -AclObject $DocACL

For the most part, you’ll probably use File Explorer to perform common file management tasks.

**What are file and folder permissions?**

In early operating systems, such as MS-DOS, the file system, FAT, didn’t have enough attribute space in the file allocation table to store much information. This meant that files and folder on a FAT volume couldn’t be assigned permissions to control user access.

However, when Microsoft introduced Windows NT in the early 90s, they also introduced a new file system, NTFS. The master file table (MFT) supports many more attributes, including the ability to define permissions on a file or folder. ReFS also supports additional attributes, and therefore supports file and folder permissions.

Windows Server and both Windows 10 and Windows 11 support the NTFS and ReFS file systems. So, it’s important that you know how to secure your file and folders.

On a typical out-of-box Windows 11 computer, you probably won’t need to configure file and folder permissions; you should be able to rely on the default security settings. However, as you begin to share content with colleagues, it becomes increasingly important to be able to define the level of access that your colleagues have on your shared content.

Both NTFS and ReFS offer the same file and folder permissions. These fall into two categories: basic and advanced. There are 13 individual advanced permissions. These combine into three basic level permissions; it’s these basic permissions you’ll typically use. Let’s examine both the basic and advanced permissions.

Advanced permissions:

* **Full control**. All available permissions are assigned.
* **Traverse folder / execute file**. Enables you navigate through a folder to a subfolder, or enables you to execute a file.
* **List folder / read data**. Enables you to view the contents of a folder or open a view the contents of a file.
* **Read attributes**. Read the basic attributes of a file or folder.
* **Read extended attributes**. Read the additional attributes for a file or folder.
* **Create files / write data**. Enables you to create a new file or to write data to a file.
* **Create folders / append data**. Enables you to create folders within the current folder or to make changes to the end of a file (but not to overwrite existing data).
* **Write attributes**. Modify the basic attributes of a file or folder
* **Write extended attributes**. Modify the additional attributes for a file or folder
* **Delete**. Enables you to delete the file or folder.
* **Read permissions**. Enables you to review the current file or folder permissions.
* **Change permissions**. Enables you to change permissions on a file or folder.
* **Take ownership**. Enables you to take ownership of the file or folder.

It’s important to note that these permissions, when assigned individually, rarely have much meaning. For example, it’s necessary to assign several permissions to allow users to read files in a folder; it’s usually not enough to just assign **List folder / read data** permissions.

It’s also important to know that the last two permissions (Change permissions and Take ownership) are very powerful. If a user has:

* Change permissions access, they can change their own (and their colleagues’ permissions) on an object.
* Take ownership access, they can take ownership of an object. The owner can always change permissions on an object.

Exercise caution when assigning these two permissions.

Generally, administrators don’t assign the Advanced permissions. Usually, they assign standard combinations of those 13 permissions; those standard combinations are known as *Basic permissions*. The following table describes these five Basic permissions.

|  |  |
| --- | --- |
| Basic permission | Explanation |
| Full control | All 13 permissions are assigned on the object. Generally, you should only assign Full control on users’ personal data areas, or when necessary to support a specific app’s requirements. |
| Modify | Modify permissions are as for Full control, with the exception of both Change permissions and Take ownership. This is good level of permissions for departmental data areas where Modify is assigned to a specific departmental group. |
| Read & execute | Read & execute includes five permissions: Traverse folder / execute file, List folder / read data, Read attributes, Read extended attributes, and Read permissions. These are the typical minimum permissions needed to work with files on a read-only basis, and allow users to view folder content, to read files, and to start apps. |
| Read | As for Read & execute, but lacking Traverse folder / execute file. Allows a user to read a file, but not make any changes. |
| Write | Four permissions are combined in Write. These are: Create files / write data, Create folders / append data, Write attributes, and Write extended attributes. Allows users to change file and folder content. |

In order to change file and folder permissions, you’ll need Full control permissions. However, if you are the file or folder owner, or have the Change permissions permission, then you can override this requirement.

When reviewing the Basic permissions list for an object, if the permissions display as Special permissions, that means the administrator has used a non-standard combination of permissions. In other words, Advanced permissions are being used.

**Using groups and permission inheritance**

If you think about the typical contents of your computer’s hard disk drive, there are probably hundreds of thousands of files in both system and user folders. For example, there’s over 200,000 files in the C:\Windows folder (and its subfolders). In a file server context, there are likely to be many hundreds or thousands of users that might need to be assigned permissions on files and folders throughout your organization’s file server infrastructure.

**Group your users**

If you had to individually assign a specific user account specific permissions on each and every file on the file system, that would likely be a very time-consuming and error-prone procedure. This is why network administrators use groups and rely on file permission inheritance.

Before you start assigning permissions to file and folders, you should:

1. Consider the collections of users that need access to those folders. Perhaps this is based on project teams, departments, or locations. Or a combination of all those factors.
2. Create groups that represent those collections of users in your organization.
3. Group your data files together in folders that mirror the group structure you created. For example, if users in the Sales department in Miami work on content together, then consider creating a folder called Miami-Sales-Data.
4. Assign permissions to the appropriate group on the appropriate folder.

By default, any permissions you assign to the Miami-Sales-Data folder are inherited in folders and subfolders beneath this folder. This means that you can quickly assign and review permissions. In Windows 11, you’ll usually use a *Local group* to group your users together.

In AD DS domain environments, you have more group options. In Windows Server, there are three group scopes: Universal, Global, and Domain Local. There are also two group types: Security, and Distribution.

In Windows Server environments, Global groups are often assigned permissions on resources. In multidomain AD DS environments, groups are sometimes nested across domains to help manage permissions.

**Inheritance**

When you start to assign permissions, you’ll need to be aware of the difference between and the impact of *explicit permissions* and *implicit permissions*.

Implicit permissions are usually referred to as inherited permissions.

By default, any file or folder you create in the file system inherits the permissions of the parent folder. This is also true for folders you create in the root of your volume. These are implicit permissions.

If you want to configure a different level of access on such a folder, you must disable inheritance on that folder and then assign the appropriate level of access. These are explicit permissions.

The advantage of using implicit permissions is that you can create files and subfolders in an existing, secured folder knowing that these files and subfolders automatically use the same permissions as the parent folder.

However, where you want change permissions and explicitly assign permissions to a subfolder, you must either:

* **Convert inherited permissions into explicit permissions on this object**. This option changes the permissions from implicit to explicit, but doesn’t change the permissions themselves.
* **Remove all inherited permissions from this object**. This option removes the current permissions and leaves the Access Control List (ACL) empty. Exercise this option with caution in case you inadvertently remove your own permissions.

It’s worth considering the effect of subfolders beneath the folder you’re reconfiguring. They’ll still be configured to use implicit permissions from their parent. However, their permissions will change because the parent folder has changed. Typically, that’s what you’ll want to do.

It’s also possible to add explicit permissions without removing existing implicit permissions. In this scenario, you might not want to update the existing implicit permissions, but you need to add a new user with specific permissions on the folder. If you do that, it’s possible that the implicit permissions you have on the subfolder conflict with the explicit permissions you assigned.

When this happens, the explicit permissions win. That’s to say, **explicit permissions override implicit permissions**.

**Allow and deny**

You should also be aware of the difference between *Allow* and *Deny* permissions. Let’s start by stating the obvious: if you haven’t assigned a user or a group permissions on a file or folder, that user or group doesn’t have permissions. There’s no requirement to specifically deny permissions; the absence of assigned permissions should be enough. However, there might be situations in which a group is assigned permissions to access a folder, but a single member of the group should not be able to access the folder.

One solution, of course, is to reconsider the groups you’re using. Maybe create a new group without the individual that shouldn’t have access. But where that’s not appropriate, then you can grant *Deny* permissions.

Up until now, our discussion has been about assigning permissions, and these have been assumed to be *Allow* permissions. But any permission you can assign can be assigned as either Allow or Deny.

For example, the **D:\Miami-Sales-Data** folder has assigned Modify (Allow) permissions for the Sales group. However, you don’t want Oliver, who belongs to the Sales group, to access content in that folder. You can now either:

* **Remove Oliver from the Sales group**. Oliver now has no permissions and cannot access the folder content. But not belonging to the group might introduce other management issues.
* **Assign Oliver Deny Modify permissions on the folder**. Oliver still belongs to the group, and perhaps can access other content in other folders, but the Deny permissions override the Allow permissions.

So, this means that **Deny permissions override Allow permissions**.

There is a single exception to this rule. If a user has explicit Allow permissions and also implicit Deny permissions (through group memberships), then the explicit permission overrides the implicit permission – even if it’s an allow permission.

**An explicit Allow permission overrides an implicit Deny permission.**

**Configuring conditions to control file access**

We’ve described how using groups can help simplify the process of assigning permissions to collections of users. However, it’s not the only way you can manage permissions to multiple users.

Windows Server includes a feature that enables you to require that your users to be able to meet a condition before they can access a resource. This condition might be membership of a group, but it can also be based on other properties of the user account. For example, you can require a user to live in a specific city, or belong to a particular department.

To make additional claims, your Active Directory administrator must define what claims the users can make. This AD DS definition modifies a user’s sign token to contain additional attributes, such as City, Department and so on. Thereafter, you can leverage those claims when assigning permissions.

Even if your Active Directory administrator has not extended the available claims, you can still use the following conditions. First, choose either User or Device. Then select the Group condition, and choose between:

* **Member of any**. Applies to the specified groups in the conditional statement.
* **Member of each**. Applies to the specified groups in the conditional statement
* **Not member of any**. Applies to the specified groups in the conditional statement
* **Not member of each**. Applies to the specified groups in the conditional statement

Use a User claim when you want to determine which groups a user must belong to, and use a device claim so that you can determine the level of access from specified computer or computers.

Your administrator can use the Active Directory Administrative Center to configure the Dynamic Access Control claims and related settings.

**Configuring file and folder permissions**

You can configure file and folder permissions by using **File Explorer**, the **icacls.exe** Command Prompt tool, or by using the **Set-ACL** PowerShell cmdlet.

**Configuring folder permissions**

To configure security setting on a folder, use the following procedure:

1. Open **File Explorer** and navigate to the appropriate folder.
2. Right-click the folder and select **Properties**.
3. In the ***Folder* Properties** dialog box, select the **Security** tab. You can review the existing permissions on this tab.
4. To change permissions for an existing security principal, click **Edit**.

You can now review and update permissions for the security principals listed. Note that the permissions you see are probably inherited, and so you’ll be able to make few changes here. You can, however, add a new security principal:

1. In the **Permissions for *Folder*** dialog box, click **Add**, and in the **Select Users, Computers, Service Accounts, or Groups** dialog box, in the **Enter the object names to select (examples)** text box, enter the security principal name.
2. Click **Check Names** and then click **OK**.
3. In the **Permissions for *Folder*** dialog box, in the **Group or user names** list, select the security principal you just added.
4. In the **Permissions for *Principal*** list, configure the required permissions and then click **OK** twice.

In this way, you have modified the ACL for the selected folder, and added an explicit permission on the folder object. The permissions are now a combination of implicit (inherited) permissions and the explicit permission you added.

**Managing inheritance**

To manage inheritance with File Explorer, use the following procedure:

1. Open **File Explorer** and navigate to the appropriate folder.
2. Right-click the folder and select **Properties**.
3. In the ***Folder* Properties** dialog box, select the **Security** tab.
4. Click **Advanced**.
5. In the **Advanced Security Settings for *Folder*** dialog box, you can review the exiting permission entries. Notice the entries in the **Inherited from** column. These entries indicate:

* That the permissions are inherited.
* The folder from which the permissions are inherited.

1. To remove inheritance, click **Disable inheritance**. Then choose one of the following options:

* **Convert inherited permissions into explicit permissions on this object**. This is recommended as you’ll then be able to finetune the permissions you want.
* **Remove all inherited permissions from this object**. Be cautious using this option. You’ll end up with an empty ACL, and you might inadvertently remove your own permissions.

1. Assuming you selected to convert, you’ll see the same permissions, only now, the **Inherited from** column displays **None**.
2. If you want to change all subfolders to inherit permissions from this folder, you can select the **Replace all child object permission entries with inheritable entries from this object** check box. Note that to perform this change, you’ll need at least **Change permissions** access on all subfolders.
3. Click **OK** twice to complete the configuration change.

**Verifying file permissions**

After you start configuring file and folder permission, especially if you’re doing so for many users and groups and folders, it can quickly become difficult to remember what level of access specific users should have. The Effective Access feature in Windows 11 File Explorer can help.

To check the user or group permissions on a folder, use the following procedure:

1. Open **File Explorer** and navigate to the appropriate folder.
2. Right-click the folder and select **Properties**.
3. In the ***Folder* Properties** dialog box, select the **Security** tab.
4. Click **Advanced**.
5. In the **Advanced Security Settings for *Folder*** dialog box, select the **Effective Access** tab.
6. On the **Effective Access** tab, click **Select a user**.
7. In the **Select User, Computer, Service Account, or Group** dialog box, in the **Enter the object name to select (examples)** text box, enter the security principal name.
8. Click **Check Names** and then click **OK**.
9. In the **Advanced Security Settings for *Folder*** dialog box, if you want to include claims, select either:

* Include a user claim
* Include a device claim

1. Enter the details of the claim. These will vary based on the allowable and configured claims in your Active Directory environment. You create the claim by using a combination of drop down lists and textboxes.
2. Click **View effective access**:

* A list of thirteen advanced permissions for the security principal is displayed in the **Permission** column.
* The **Effective access** column displays whether the principal has a specific permission:
* A green check indicates they do.
* A red cross indicates they don’t.
* The **Access limited by** column indicates whether the permission limitation is a result of:
* **File Permissions**. This means the local NTFS permissions are limiting access.
* **Share**. This means shared folder permissions are limiting access.

1. Click **OK** twice to complete your review.

We’ll examine the impact of shared folder permissions in the next lesson.

**Demonstration: Securing folders**

Lesson 2

**Configuring and managing shared folders**

After you’ve secured files and folders, you must make the folders available to your users. You’ll need to know how to create, manage, and secure shared folders.

**Lesson Objectives**

After completing this lesson, you will be able to:

* Create and manage shared folders.
* Understand shared folder permissions.
* Review the effective permissions of files accessed through a shared folder.

**Sharing folders**

To enable your colleagues to collaborate with you, you might need to give them access to your documents. This often means sharing the folders that contain your documents. There are several ways in which you can share folders in Windows 11.

**Public folder sharing**

Public folder sharing is enabled on your public document libraries, and is configured in Advanced sharing. The public document libraries exist in the C:\Users\Public folder. However, you configure the sharing settings using Control Panel. Use the following procedure:

1. Click **Start**, type **Control Panel** and then select **Control Panel**.
2. Click **Network and Internet**, and then click **Network and Sharing Center**.
3. In the navigation area, select **Change advanced sharing settings**.

* On the Advanced sharing settings page, you can see expandable lists for **Private**, **Guest or Public**, and **All Networks**. These equate to the network location profiles used by Windows to assess risks posed by connectivity to a specific network. The active profile for your current network is indicated with **(current profile)**. You can customize the settings for any or all profiles. For each profile, you can:
* **Turn on / off network discovery**. When On, this enables you to browse the Network object in File Explorer to locate shared resources. It also enables other users to locate your device and its shared contents.
* **Turn on / off file and printer sharing**. When On, users can access any of your shared resources, including files and printers.

Consider disabling these features on public or guest networks.

1. Under the **All Networks** node, you can configure:

* **Public folder sharing**. Enables users to access your public folder libraries.
* **Media streaming**. Enables users to access pictures, music, and media content on your computer.
* **File sharing connections**. Enables you to configure encryption settings to help protect file sharing.
* **Password protected sharing**. Allows you to specify that only users with a configured user account on your computer can access your shared content.

1. When you’ve configured the required settings, click **Save changes** and then close Control Panel.

You probably shouldn’t rely on public sharing as it’s not especially configurable. Instead, you should create specific folders for your content, and then use Advanced sharing.

**Shared Folders snap-in**

Computer Management provides access to a number of configuration and administration tools. One of these is the Shared Folders snap-in. Using this snap-in, you can:

* Review the existing shared folders.
* Reconfigure the existing shared folders.
* Create a new shared folder using the **Create A Shared Folder Wizard**.
* Review current sessions. These sessions display information about users that are connected to your shared folders, including User, Computer, Type (of computer), number of open files, connected time and idle time, and whether the connected user is a guest or not.
* Review open files. This displays a list of open files, and details including: the name of the files, the user accessing them, the type of computer being used, any file locks, and whether the file is open in read or write mode.

If you choose to use the Shared Folders snap-in, the wizard directs you to provide:

* Computer name
* Folder path
* Share name
* Description
* Offline setting
* Permissions

**Give access to**

A quick way to create a shared folder is to use **Give access to**. This is accessible in File Explorer, and enables you to create and configure a folder share, or remove access.

Locate the folder you want to share, right-click it, choose **Show more options**, select **Give access to**, and then click **Specific people**.

When you use this method to create a shared folder, you’ll need to provide the following information:

* List of users that can access the share. The owner of the folder is already listed.
* User permissions. The permissions are described with different terms than discussed earlier. Full control is Read/Write, while Read & execute is Read. There’s no Modify equivalent.

When you add the list of users and define their permissions, click **Share**. The folder is shared with a default name (you’re not prompted to define the name). Interestingly, when the folder is shared, the file system permissions are updated to match those you specified, but the shared folder permissions are also automatically configured to match.

This method of sharing is a very quick and effective way of establishing a shared folder, but it does lack fine control over settings.

**Advanced sharing**

This feature of File Explorer is what most administrators probably use. To share a folder this way:

1. Open **File Explorer** and locate the required folder.
2. Right-click the folder and then click **Properties**.
3. Click the **Sharing** tab.
4. Click the **Advanced Sharing** button, and then define the following properties:

* **Share this folder**. This enables the folder for sharing.
* **Share name**. The name users will use to connect to the folder across the network.
* **Limit the number of simultaneous users to**. Enter a maximum number of users that can concurrently connect to your folder. On Windows 11, the maximum is 20, which is the default value. Windows Servers support unlimited simultaneous users.
* **Permissions**. Enter the shared folder permissions. The default is Everyone Allow Read.

Shared folder permissions are described in the next topic.

* **Caching**. Enables users to access content when offline. Available options are:
* Only the files and programs that users specify are available offline (default).
* No files or programs from the shared folder are available offline.
* All files and programs that users open from the shared folder are automatically available offline. If you select this option, you can choose to Optimize for performance (on by default).

1. Click **OK** and then click **Close**.

**Command Prompt**

You can use the **Net Share** command to share folders from the Command Prompt. For example, use the following command to share the C:\Data folder:

Net share Data = C:\Data

You can use the /GRANT parameter to define shared folder permissions. For example:

Net share Data = C:\Data /GRANT:Everyone,Full

If you run Net Share without parameters, it lists the available shared folders on your computer. Also, if you run Net Share with the name of an existing shared folder, the command returns the details for that shared folder.

Using the Command Prompt can be a useful tool for scripting shared folder creation, but generally, it’s easier to use File Explorer or Windows PowerShell.

You must use an elevated Command Prompt window to manage shared folders.

**Windows PowerShell**

You can use the following PowerShell cmdlets to configure and manage shared folders.

|  |  |
| --- | --- |
| Command | Description |
| New-SmbShare | Create a new shared folder. |
| Get-SmbShare | Displays the computer’s existing shared folders. |
| Set-SmbShare | Modifies the properties of an existing shared folder. |
| Remove-SmbShare | Deletes an existing shared folder (but not the folder itself). |
| Get-SmbShareAccess | Displays a shared folder’s permissions. |
| Grant-SmbShareAccess | Configures shared folder permissions. |

For example, to create a shared folder, enter the following command at an elevated Windows PowerShell command prompt:

New-SmbShare -Name Data -Path C:\Data

In this instance, default shared folder permissions are assigned (Everyone Allow Read).

**What are shared folder permissions?**

When you create a shared folder, you assign permissions on the share. If you don’t specify permissions, default shared folder permissions are applied. It’s therefore important to understand shared folder permissions.

**Why use shared folders permissions?**

You might wonder why shared folder permissions are necessary, and that’s a good question. It’s historic, because early file systems, like FAT, didn’t support the notion of file system security. So there needed to be another way to control access to shared files.

If you weren’t sharing your files, then it wasn’t considered necessary to secure them. However, if you did share your files, then you might want to limit access to those files. That’s where shared folder permissions came in useful.

In Windows 11, and Windows Server, there are three available shared folder permission levels. These are:

* **Read**. Users can list files in the secured folder, open files and review the content. However, not changes can be made, and nor can users delete or create additional files in the share.
* **Change**. Users have the same access as with Read, but can also modify contents, create files, and delete files. However, they cannot take ownership or files or change permissions on files.
* **Full Control**. Users can perform all file actions.

When you share a folder on a FAT volume, you can only configure the shared folder permissions. However, when you share a folder on an NTFS volume, you must configure both the shared folder permissions and the local NTFS file system permissions. We’ll discuss the impact of two sets of permissions in the next topic.

If, however, you choose to share folders using **Give access to**, then automatic share permissions are used. When you select an access level for a security principal using **Give access to**, the file system permissions are configured according to your selection. You can choose between:

* **Read**. Equivalent to Read & execute.
* **Read/Write**. Equivalent to Full Control.

All inherited permissions are removed.

The shared folder permissions are assigned as follows:

* **Everyone**. Allow Full Control.
* **Administrators**. Allow Full Control.

**Reviewing effective access through shares**

When determining the effective permissions through a shared folder, it’s helpful to consider each set of permissions as being two filters. So, in other words, in order to have Allow Full Control permissions on a file on an NTFS volume through a shared folder, the security principal must have Allow Full Control permissions on the shared folder AND the NTFS folder.

The following table compares the two sets of available permissions.

|  |  |
| --- | --- |
| Shared folder permission | NTFS file system permission |
| Full Control | Full Control |
| Change | Modify |
| Read | Read & execute |

Essentially, the permissions that a security principal has on a shared folder must agree with the corresponding permission in this table in order for that principal to enjoy the configured shared permission. Or vice-versa.

For example, if Sales has Modify permissions on the Sales-Data folder, and Steve, a member of Sales, has Change permissions on the Sales-Data shared folder, Steve has Modify permissions on the files in the folder on the NTFS volume through the share.

But if Steve only has Read permissions on the shared folder, then Steve only has Read & execute permissions on the files in the folder on the NTFS volume.

As mentioned earlier, you can review effective permissions using File Explorer:

1. In **File Explorer**, navigate to the appropriate folder and open the Advanced Security Settings for the folder.
2. On the **Effective Access** tab, select a user or group you want to check and then click **View effective access**.
3. You can now review the permissions the user or group has by checking the **Effective access** column. The **Access limited by** column indicates whether any permission limitation is a result of:

* **File Permissions**. This means the local NTFS permissions are limiting access.
* **Share**. This means shared folder permissions are limiting access.

It’s worth noting a couple of things about shared folder permissions. These are:

* **The least permission applies**. This is an over-simplification, but is broadly correct. If the share permissions are Read, and the NTFS permissions are Full Control, the security principal has Read permissions. That is, the ‘least permission’.
* **Default shared folder permissions**. The default shared folder permissions are Everyone Allow Read. You’ll almost certainly need to change this as it prohibits write access through the share for all users.
* **Keep it simple**. You can modify the default shared folder permissions to Everyone Allow Full Control. This means that any permission assigned on the file system is the determining permission.

**Demonstration: Sharing folders**

Lesson 3

**Implementing Work Folders**

Many users need to be able to work away from the office, whether that’s from home, from a hotel, or somewhere else. Work Folders enables you to create a sync share on your file server and enable remote access to specified users to server-based content. In this lesson, you’ll learn how to configure Work Folders, and enable access from both domain-joined computers, and users’ own computers.

**Lesson Objectives**

After completing this lesson, you will be able to:

* Describe Work Folders and its components.
* Configure Work Folders.

**What is Work Folders?**

Work Folders enables your users to synchronize their work content to both their work devices and their personal devices. It’s important to understand that Work Folders is an on-premises technology based on Windows Server. Your server administrator must install the Work Folders role service and configuring a Sync share before your users can benefit from the service.

**Components**

Work Folders consists of several components. These are:

* **Work Folders server**. This is any Windows Server with the Work Folders role service enabled. The server must:
* Be a member of an AD DS domain. Group Policy is used to configure Work Folder settings.
* Have a computer certificate. The certificate is used to identify the server to users of Work Folders. Connections to Work Folders are over https using SSL.
* **Sync share**. The server must host one or more sync shares. These are special shared folders that host the synced content, and are secured for specific groups of users.
* **User devices**. Windows 11 has built-in support for Work Folders. Your users can also download and install a Work Folders app for iOS and Android to support their smartphones’ access to Work Folders.
* **Client certificate trust**. Your users’ devices must trust the certificate being used by the Work Folders server. For computers running Windows 11 in a domain-joined context, this is probably the case already. But for other devices, you might need to distribute a root certificate.

**Initial provisioning**

After your server administrator has installed the Work Folders role service, configured a Sync share, and configured the required Group Policy settings, the following occurs when users first connect to the Sync share:

1. A sync partnership between the file server and the user device is established.
2. On the user device, the following are created:

* Download-staging directory
* Data directory
* Version database
* This occurs on each of the user’s devices.

The Version database keeps the local copy of data in sync with the file server data.

1. On the server, after a user initiates their first sync, the server creates similar objects. This occurs only once for each user account.

**How does it work?**

When users make changes to Work Folders content, the following happens:

1. The Work Folders server detects the changes on the client.
2. The client initiates a sync session to upload changes.
3. The server applies the uploaded changes to the user’s content. If the file changes on multiple devices in the same sync cycle:
4. The latest version of the file is retained with the original file name.
5. Other copies of the file are retained but the filenames are appended with the originating device’s name.

**Considerations**

When using Work Folders, consider the following:

* Work Folders sync is limited to one partnership for each user on a specific device.
* Client devices:
* Initiate synchronization
* Synchronize only with the Work Folders server
* Conflicts are resolved automatically by renaming conflicting files.

**OneDrive versus Work Folders**

It’s worth comparing OneDrive with Work Folders.

OneDrive is also built-in to File Explorer, and supports automatic synchronization of users’ local library folders, such as Documents and Pictures. There are also apps available to support iOS and Android devices. But OneDrive is cloud-based storage, and designed to sync user content between their non-domain-joined devices. For users that are rarely connected to on-premises networks and servers, this is the ideal solution for data synchronization.

Work Folders is designed for primarily on-premises users that also want to access specific content that they’ve stored in a Sync share on their personal or non-domain-joined devices. Many administrators implement Folder Redirection as a way of storing and syncing user content from their local libraries to file server shared folders. Combined with Work Folders, for primarily on-premises users, this represents a good solution.

**Configuring Work Folders**

Your users can manually install Work Folders on their Windows 11 computer by using Control Panel (this is described in step 6). Usually, however, you’ll use domain-linked Group Policy settings to automatically configure Work Folders.

To complete setup for automatic configuration, you must complete the following high-level procedure:

1. Install the Work Folders role service
2. Verify presence of a certificate for SSL
3. Configure the Work Folders sync share
4. Configure the required Group Policy settings
5. Verify application of settings in domain-joined computer
6. Configure a standalone computer

Let’s examine these steps in more detail.

**Install the Work Folders role service**

You can add the Work Folders role service by using Server Manager or by using Windows PowerShell. You might also need to install the Web Server role if it’s not already installed.

1. Open **Server Manager**.
2. From the Dashboard, select **Add roles and features**.
3. Click through the wizard, and select the local server.
4. On the **Select server roles** page, expand **File and Storage Services**, expand **File and iSCSI Services**, and then select the **Work Folders** check box.
5. If necessary, select the **Web Server (IIS)** check box.
6. When prompted, click **Add Features**, then click **Next** twice.
7. Click **Install**, and when prompted, click **Close**.

You can also use the following PowerShell command to install the required role service:

Install-WindowsFeature FS-SyncShareService

**Verify presence of a certificate for SSL**

Certificates are used to identify the Work Folders server from the client device.

1. Open **Settings** and then search for and select **Manage computer certificates**.
2. In the Certificates console, expand **Personal** and then select **Certificates**.
3. Verify the presence of a certificate for Client Authentication purposes.

* If you don’t have an appropriate certificate, you must obtain one which the client devices will trust.
* The name to which the certificate is issued is the name that must be used to connect to the Work Folders server.

1. Open **Internet Information Services (IIS) Manager** from **Tools**.
2. Navigate to the **Default Web Site**.
3. In the Actions pane, select **Bindings**.
4. In the **Site Bindings** dialog box, click **Add**.
5. In the **Add Site Binding** dialog box, in the **Type** list, select **https**.
6. In the **SSL certificate** list, select the certificate you verified/installed earlier.
7. Click **OK** and then click **Close**.

**Configure the Work Folders sync share**

The Sync Share stores the users’ synchronized data. You need to create at least one sync share, and assign the necessary permissions for users that will use it.

1. In Server manager, expand **File and Storage Services** and then click **Work Folders**.
2. In the details pane, select **TASKS** and then select **New Sync Share**.
3. In the **New Sync Share Wizard**, click **Next**.
4. On the **Select the server and path** page, in the **Enter a local path** text box, enter the path to your sync share root folder and click **Next**.
5. When prompted, click **OK** to create the local path you defined.
6. Click **Next** twice, and then, on the **Grant sync access to groups** page, add the groups that should be able to access this sync share and then click **Next**.
7. Click **Next** and then click **Create**.
8. When prompted, click **Close**.

Alternatively, you can use the **New-SyncShare** cmdlet to create the sync share.

**Configure the required Group Policy settings**

Domain-joined computers are easily configured using a single GPO setting.

1. Open **Group Policy Management**.
2. Locate the appropriate container. For example, select the domain object.
3. Right-click the container, and then choose **Create a GPO in this domain, and Link it here**.
4. Enter a name for the GPO. For example, enter **Work Folders** and click **OK**.
5. Right-click **Work Folders**, and then select **Edit**.
6. Expand **User Configuration**, **Policies**, **Administrative Templates**, **Windows Components**, and then select **Work Folders**.
7. Double-click **Specify Work Folders settings**, and then select **Enabled**.
8. In the **Work Folders URL** text box, enter the full URL for your Work Folders server. For example, enter **https://Adatum-SVR1.Adatum.com**.
9. Select the **Force automatic setup** check box.
10. Click **OK** and close Group Policy Management Editor and Group Policy Management.

**Verify application of settings in domain-joined computer**

You can verify the application of the Group Policy setting from a Command Prompt.

1. Switch to a client computer and sign in using an account which has permissions on the Work Folders sync share.
2. Open **File Explorer**. You should see a Work Folders node in the navigation pane.

* If you don’t, then refresh Group Policy by running **gpupdate /force** at an elevated Command Prompt.

1. Test Work Folders by adding files and verifying that they sync.

**Configure a standalone computer**

A standalone computer, or a smartphone, is not domain-joined. Therefore, you must configure the settings on the device without Group Policy setting. Use this procedure:

1. On a standalone computer, download and install the root CA certificate from your on-premises certification authority. Install the certificate into the Computer Trusted Root Certification Authorities node.
2. Open **Control Panel** and search for and select **Work Folders**.
3. Click **Set up Work Folders**.
4. Click **Enter a Work Folders URL instead**.
5. Enter the URL for your Work Folders server and click **Next**.
6. You’re prompted to sign in. Use an account which has been granted permissions to use the Sync Share.
7. Complete the setup wizard. You should now be able to see a Work Folders node in File Explorer.

**Demonstration: Implementing Work Folders**

Lesson 4

**Managing printers**

It’s important that users are able to print documents and other content. Some users have locally connected printers to which they have exclusive use. Others connect to printers that are directly attached to the network. But many connect to printers that are shared on a Windows Server computer.

In this lesson, you’ll learn how to manage local printers, how to connect to network printers, and how to create, secure, and manage shared printers.

**Lesson Objectives**

After completing this lesson, you will be able to:

* Describe the printer architecture.
* Create and manage a printer.
* Use Print Management.

**Overview of printing in Windows 11**

We still live in a world where printing matters. That’s changing all the time, and much that was previously printed is now distributed and consumed electronically.

But for the foreseeable future, a big part of managing any network will entail managing the printers attached to that network. In this topic, you’ll learn about Windows printing components, and how they interact.

The printing architecture in Windows consists of the following elements:

* **Print device**. The actual physical printer.
* **Printer**. An operating system object that contains configuration settings, preferences, and drivers that apps use to format print output.
* **Driver**. Acts as the interface between the operating system and the physical device. You’ll need a specific driver for each operating system architecture: x86 and x64.
* **Port**. Connects the printer to the print device. Ports can be local, such as USB connections. But they can also be networked ports, such as TCP ports. Printers can be configured to use multiple print ports enabling output to be distributed across physical print devices.
* **Print server**. This is any device that’s sharing its connected printers.

Computers that want to print to a print device require a driver. That driver might well be present in the driver store that ships as part of the operating system. However, if it’s not, you’ll need to install the driver.

If you install the driver on a print server, then users connecting their device to that print server’s printers can obtain the driver from the print server. Alternatively, you can install the print drivers you expect to need into the driver store, either after Windows installation, or as part of a desktop image that you use to deploy Windows.

**Creating and managing a printer**

**Create a printer**

To create a printer on a Windows 11 computer, use the following procedure:

1. Open the **Settings** app.
2. Select **Bluetooth & devices**.
3. Expand **Printers & scanners**. Any existing printers are listed here.
4. Click **Add device**. Windows attempts to detect any attached print devices.
5. If Windows can’t locate the device, then click **Add manually**.
6. The **Add Printer** wizard displays the **Find a printer by other options** page. You can now choose between:

* My printer is a little older. Help me find it.
* Select a shared printer by name. You’ll need to enter the printer UNC or URL.
* Add a printer using an IP address or hostname.
* Add a Bluetooth, wireless or network discoverable printer.
* Add a local printer or network printer with manual settings.
* The option you choose determines what the wizard displays next.

1. For example, let’s assume you choose **Add a local printer or network printer with manual settings**. Click **Next**.
2. On the **Choose a printer port** page, select the appropriate printer port. Choose between:

* Use an existing port
* Create a new port
* This might be a local port, such as a USB connection, or a networked port using a generic protocol such as TCP, or using a vendor specific print port.

1. Let’s assume you choose an existing local port. Click **Next**.
2. On the **Install the printer driver** page, navigate through the list of available **Manufacturers** and **Printers**.

* If the printer you want is not listed, you can choose either **Windows Update** or **Have Disk** to install the driver.

1. Once you’ve selected the printer, click **Next**.
2. On the **Type a printer name** page, enter a name for your printer. A default is provided. Click **Next**.
3. On the **Printer Sharing** page, if you want to share your printer, and thereby designate your computer a print server, click **Next**. Otherwise, select **Do not share this printer**, and then click **Next**. Let’s assume you share your printer.

You can also enter a Location and Comment string for your printer.

1. Finally, click **Print a test page** to verify your printer and the port connecting it to the print device is correctly configured. Then click **Finish**.

**Manage a printer**

To manage a local printer on a Windows 11 computer, you can use the Settings app. You can also use Print Management, and a number of other related tools, including PowerShell cmdlets. You can access most tools by using the Settings app to launch them:

1. Open **Settings**.
2. Select **Bluetooth & devices**, expand **Printers & scanners**, and select the printer you want to manage.
3. The following options are displayed:

* **Open print queue**. Displays the print queue, from which you can manage submitted print jobs.
* **Print test page**. Enables you to test your print device.
* **Run the troubleshooter**. Detects common problems and suggests typical solutions.
* **Printer properties**. Displays the detailed printer properties, including: sharing, ports, advanced settings, color management, and security settings.
* **Printing preferences**. Enables you to configure your printing preferences, such as layout and paper choices. Options vary depending on printer type.
* **Hardware properties**. Enables you to review the print device driver details.

Most of these options open in a separate window.

Typical management tasks might include:

* Modifying printer properties, such as sharing, security, and advanced properties.
* Choosing a default printer.
* Managing the print queue.
* Taking your printer offline.

Let’s review these tasks in more detail.

**Modify printer properties**

In **Settings**, select **Bluetooth & devices**, expand **Printers & scanners**, and select the printer you want to manage. To modify printer properties, click **Printer properties**. Six tabs are displayed.

* **General**. Provides access to:
* **Location**. This is an important aid in enabling users to discover the location of a printer. In Active Directory environments, you can add Location strings to objects such as subnets and physical sites, such as a Head Office. These settings enable a user to automatically default to adjacent printers when they move around your organizational locations.
* **Preferences**. Enables you to define default printing characteristics.
* **Sharing**. Enables you to configure:
* **Share this printer**. Enable sharing and define a share name. Users connect using a UNC such as \\Adatum-CL22\LaserJet.
* **Render print jobs on client computers**. When selected, the client device creating the print job processes that print job before routing a (partially) formatted output file to the print server for physical printing. This reduces workload on the print server.
* **Ports**. Enables you to change ports, or enable printer pooling. With printer pooling, multiple ports are specified, each of which has an identical print device attached. Jobs are distributed across all ports.
* **Advanced**. Provides access to:
* **Availability**. Most printers are always available. However, you can define specific hours of use.
* **Priority**. You can define a priority for a printer. This assumes you have created multiple printer objects all pointing to the same physical print device. Each printer can be assigned a different priority value, 1 being the highest priority. Different users can then use different printers, with higher or lower priorities – but the print jobs always route to the same print device (or pool of print devices).
* **Spool options**. There are a number of spooling options with which you can control jobs. These enable you to hold print jobs until they’re fully spooled, or start printing immediately after the first page is spooled. Spooling accelerates the printing process from the client device’s perspective.
* **Document management options**. You can control document submission behavior. For example, you can Hold mismatched documents, Print spooled documents first, and Keep printed documents.
* **Color Management**. Enables you to manage default color settings for your color printers.
* **Security**. There are three basic security settings. These are:
* **Print**. Enables a user with this permission to submit print jobs. By default, the Everyone group is assigned this permission.
* **Manage this printer**. Enables a user to manage the printer properties.
* **Manage documents**. Enables a user to manage the print queue. Normally, the CREATOR OWNER group is assigned this permission effectively enabling users to manage their own print jobs.
* The printer owner and the local Administrators group are both assigned all three permissions on the printer. There is an Advanced button with which you can review advanced security settings and also effective access.

**Choose a default printer**

By default, Windows 11 is configured to **Let Windows manage my default printer**. This is generally a good setting as it enables Windows to choose the most appropriate printer based on your location.

You can change this behavior in **Printers & scanners** under the **Printer preferences** heading.

If you want to manually select a default printer, you must use **Control Panel**:

1. In Control Panel, select **Hardware and Sound**.
2. Select **Devices and Printers**.
3. Right-click the printer you want to set as default, and then select **Set as default printer**.
4. You are warned that Windows will stop managing your default printer setting. If you want to proceed, click **OK**.

**Manage the print queue**

You use the Settings app to manage the queue. After you’ve selected the appropriate printer in **Printers & scanners**, click **Open print queue**. A new window opens.

You can now review all print jobs, and perform the following functions on print jobs in the queue:

* Pause
* Restart
* Cancel
* View properties

Consider using the **Get-PrintJob** Windows PowerShell cmdlet to retrieve queue information. For example:

Get-PrintJob –PrinterName LaserJet

**Take the printer offline**

If you’re experiencing problems with your printer, you might need to take it offline. In the print queue window, select the **Printer** option in the menu, and then choose **Pause Printing**. This stops the printer from submitting to the print device. This can be useful to sort out physical printer problems, like paper jams or toner issues.

It’s a good idea, if possible, to change the port for a shared printer during this time. Point the printer to another print device by selecting a different port. Then deselect Pause Printing, and jobs are routed to another print device.

**Using Print Management**

As discussed, you can share your printers for other users to connect to. By doing so, your computer becomes a print server. The tool used to manage print servers is Print Management.

Print Management provides a consolidated view on your printing architecture, and enables you to perform the following management tasks:

* Add or remove print servers.
* Add and delete printers.
* Install and manage drivers.
* Manage print queues.
* Review and modify printer status.
* Create custom filters. Default filters are:
* All Printers
* All Drivers
* Printer Not Ready
* Printers With Jobs

Under the Print Servers node, you can add or remove print servers. For a particular print server, you can review the following:

* **Drivers**. Review, install, and manage drivers.
* **Forms**. Manage and configure printer paper size and settings.
* **Ports**. List and configure the available ports on the target server.
* **Printers**. Access Printer Properties, access print queues, and modify other configuration settings.

To access Print Management, click **Start**, type **Print Management** and then click **Print Management**.

**Demonstration: Managing printers**

**Lab: Managing resources**

**Question:**In the lab, you configured Work Folders. What is the certificate used for?

**Module Review and Takeaways**

Review Questions

**Question:**You want to quickly and easily make local content available to your colleagues. Should you use **Give access to**, or **Advanced Sharing**?

**Question:**When configuring Work Folders, which method is used to configure domain-joined computers?

**Question:**What’s the default permission for the Everyone group on a printer?

Tools

The following table lists the tools that this module references.

| **Tool** | **How used** | **Where found** |
| --- | --- | --- |
| icacls.exe | * Manage permissions | Command Prompt |