Assign NTFS permissions using Group Policy

You can use group policies to set access rights to directories or files for multiple computers. They not only save you the interactive configuration but also ensure that permissions do not deviate from the default in the future.

Contents of this article

For most directories installed by the operating system, there is usually no need to change the permissions. Exceptions are vulnerabilities such as CVE-2021-36934 ("HiveNightmare"), where critical components such as the SAM database are not sufficiently protected due to misconfiguration of access rights.

Other use cases

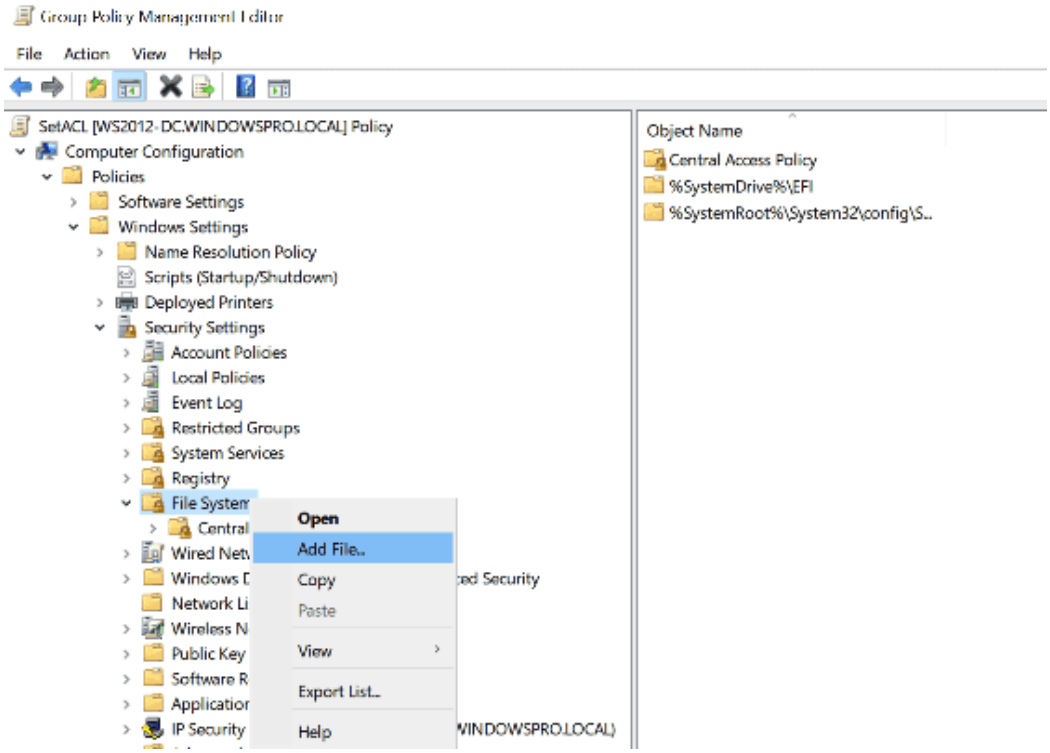
In this case, as a workaround, you could change the permissions to a secure state using a GPO on all affected PCs. Another use case could be when you create a folder via group policy preferences and want to configure its access rights immediately.

Another example would be that an application runs under a service account, and the account needs access to certain data directories.

Since the client-side extensions reapply the settings of a GPO on every refresh, this ensures that the desired permissions are always maintained, e.g., on file shares with a deep folder structure. Manual changes would be corrected automatically.

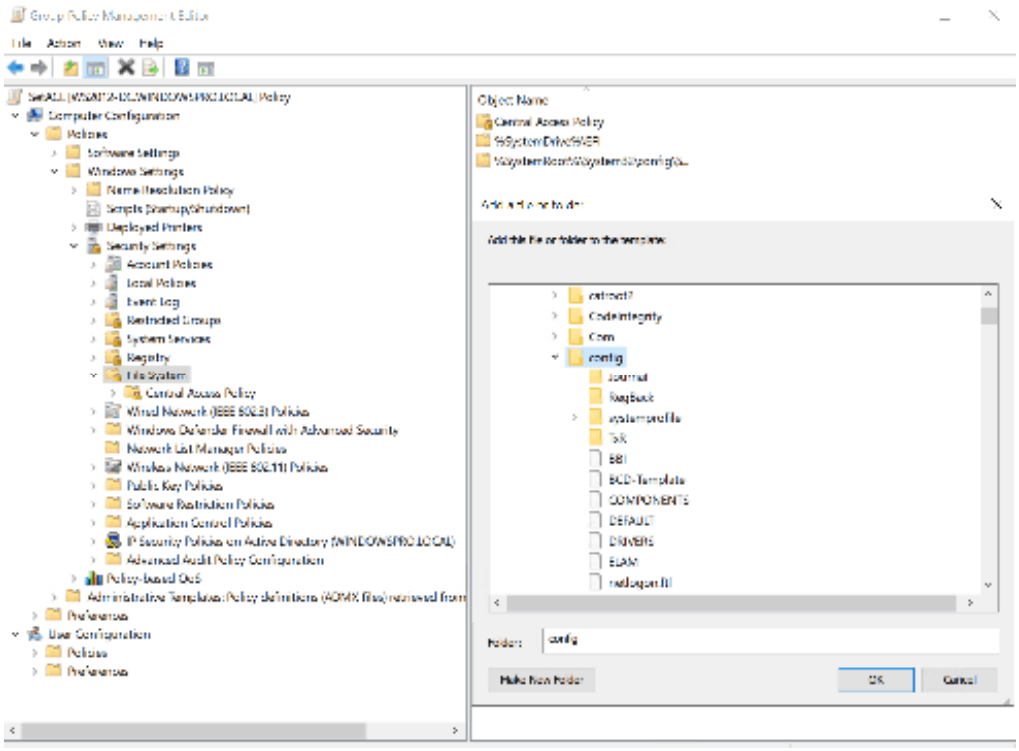
Creating a GPO

After you have created a GPO and linked it to the desired OU or domain, open it in the GPO editor. There, you switch to **Computer configuration > Policies > Windows Settings > Security Settings > File System**. From the context menu of **File System** select **Add File**.



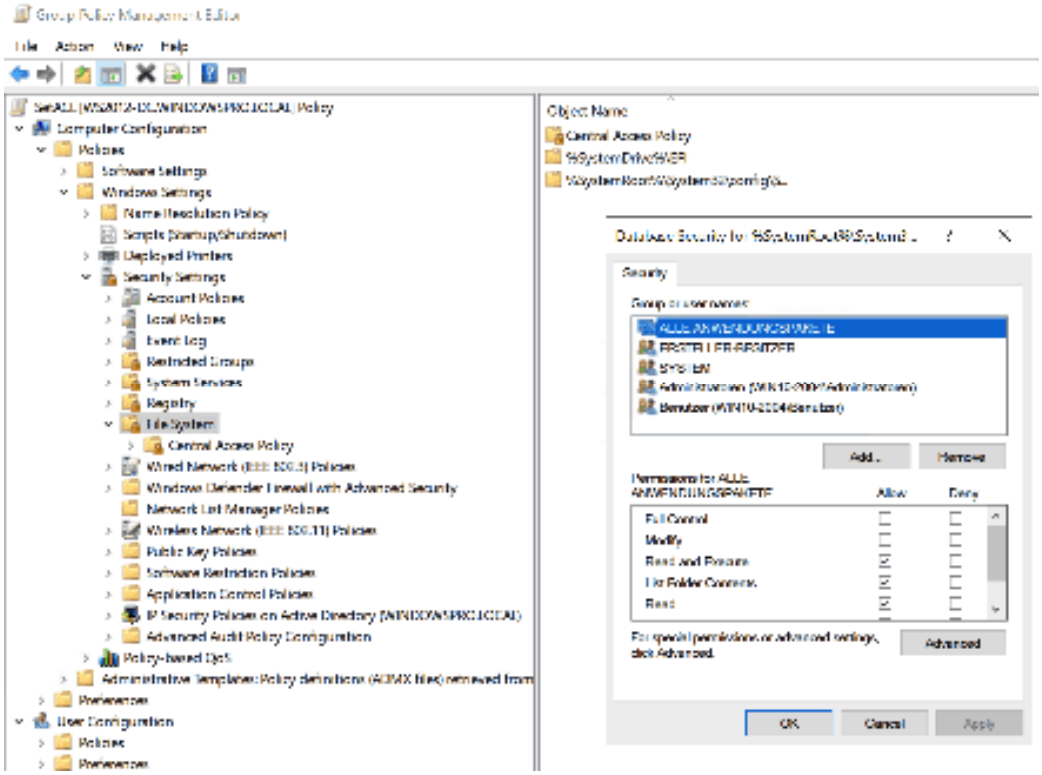
Add the file or directory to the GPO for which you want to set the permissions

This opens a dialog box that can be used to navigate the file system of the admin workstation. This is convenient if the target computers have the same folders. Otherwise, you can enter any path in the **Folder** input field.



Select the directory or file for which the access rights are to be configured

After selecting a directory or a file, the Security dialog box (as you know it from the properties of a file system object in Explorer) appears. Here, enter the required principals and assign them the desired permissions. Removing accounts or groups has the same effect on the target systems.

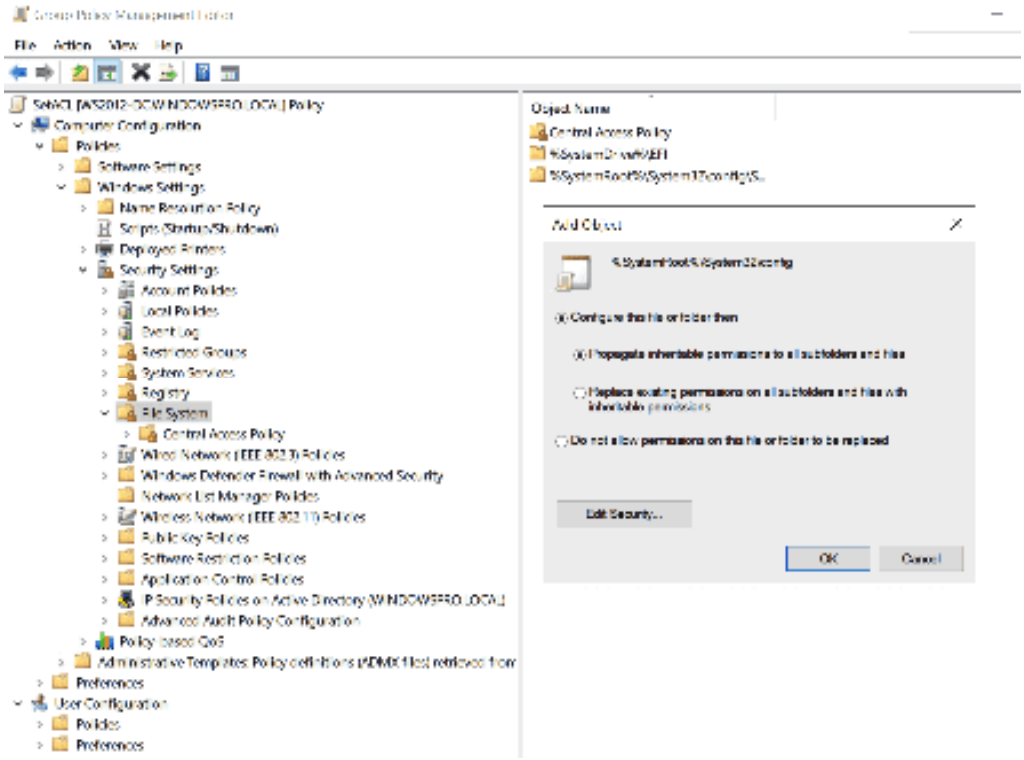


Configuring permissions for the selected directory

Controlling inheritance

If you open the advanced security settings by clicking **Advanced**, you can configure inheritance there. After confirming the new permissions, you also have the option to replace existing permissions in all

subfolders with inheritable permissions or, if permissions were assigned there directly, to leave them as they are.



Specify how and whether the changed permissions are passed to the subfolders and files

Another option, called **Do not allow permissions on this file or folder to be replaced**, disables the transfer of permissions to subdirectories. In this case, you will probably configure a separate GPO setting for the permissions of the subdirectory tree.