Access Control List Simulation

Group: Executives

CEO – Gru

Gru is the Chief Executive Officer (CEO) for Companies Incorporated and is the highest-ranking executive in the company. Since he is the CEO of the company, his main duties as well as other duties include making major corporate decisions, managing or overseeing the overall operations of the company, and lastly acting as the main line of communication between the board of directors and corporate operations. Overall, the CEO is a very vital and busy individual that makes sure that the company is performing at its absolute best.

Gru should have access to ALL FOLDERS and FILES with the only permission to READ. Being that he is the CEO and is very busy, he should only be able to gain access to all folders and read the files within them to ensure that the company is running well and smoothly. It is best if he did not have access to write and execute permissions, because if he ever makes a mistake by dragging a folder into the wrong place, then efficiency would drop and folders and files would end up disorganized. Overall, if things need to be changed or altered then the department head will be able to do with the approval of the executives.

CSO – El Macho

El Macho is the Chief Security Officer (CSO) for Companies Incorporated and is part of the highest-ranking executives in the company that deals with the company's security. His duties include having the company run and operate normally but within safe parameters to promote a safe and secure environment for all departments within. Besides protecting the company from potential threats and attacks, El Macho should also be able to identify and provide possible solutions toward the company. Such as having strategic plans that protect the company's goals, assets, work environment, as well as objectives. Overall, El Macho is the head executive of security for Companies Incorporated.

El Macho should have access to ALL FOLDERS and FILES with the permission to READ. He is as busy all the other executives and should be able to access all folders and read files within them so he may review them to see if there is any security risk that needs to be looked over. It would be advisable if he did not have access to write and execute within the folders, because he might make a mistake when accidentally dragging a new file within folders, for example. Overall, if things need to be changed or altered then the department head will be able to do with the approval of the executives.

CIO – Herb

Herb is the Chief Information Officer and has similar job duties as El Macho who is the CSO. His duty as a CIO is to oversight day to day IT operations as well as manage and collaborate with other executives and managers to formulate plans to move the company to a secure step forward. Overall, as a CIO, Herb is expected to manage and ensure that Companies Incorporated is operating at its best.

Herb is part of the executive group and is a very busy individual for the company. Therefore, since he is in the executive group he will only have READ access to the folders. Reason being to Herb having the READ permission like the other executives in his group is due to the chance of him wrongfully dragging a file in the wrong folder or dragging a folder inside another folder. Overall, if things need to be changed or altered then the department head will be able to do with the approval of the executives.

CRO – Lucy

Lucy is part of the executive group like Gru, El Macho, and Herb. They are all busy people and do not have time to create changes and execute programs. Lucy is the Chief Risk Officer, which means that she is in charge of overlooking business risks within Companies Incorporated. That means she needs to be aware of risks such as employees that violated company policies, hackers, and even data breaches. In all she needs to be wary of things that can negatively affect the company.

As stated earlier, Lucy is a very busy individual like the other Chiefs at Companies Incorporated. Therefore, she will only need READ permissions to specific folders. The only folders that Lucy is able to READ are: Executive Meeting, Company Policies, Compliance, Security Breaches, Employees, and Security. The reason why she has the READ permission is due to the fact that she just oversees and analyzes the company's risk values. If any changes need to be made then Lucy can contact and reach out to the executives. If changes are then approved by the executives, then the Department Head should be able to make changes to any of the desired files.

Group: Department Head

Department Head – Scarlet

Scarlet is a vital part of the team at Companies Incorporated. Let's give Scarlet the responsibility of being a secretary alongside her duty as a Department Head. As a Department Head Secretary, her duty consists of taking notes for the Executives during their professional meetings or conferences. Her other duty is to ensure that the Mid-Level Manager is providing a proficient service to the lower staff.

This group will be able to READ, WRITE, and EXECUTE the folder Executive Meetings as well as its internal files. As Secretary, her main goal is to list all of the decisions and notes from the Executives and save them for future use. Other files that she is able to READ is the Company Policies folder and its internal files.

Group: Manager

Mid-Level Manager – Walter

Walter is the Mid-Level Manager for Companies Incorporated. He is a very hard worker that oversees the staff such as Ms. Haddy, Flux, and Madge. He ensures that everyone is doing the very best they can at their jobs. However, if a particular employee or staff is caught committing mischievous acts the manager can file a complaint with higher management or the department head, Scarlet.

Since Walter is part of management we need to give him special permissions with folder access. Walter should be able to READ only on specific folders which is listed below. He would need READ permissions for both the Employee and Company Policies folder so he can read files within such as policies and programs and share them with the lower staff.

Group: Employees

Staff – Ms. Haddy, Flux, Madge

Ms. Haddy, Flux, and Madge are the three staff members of Companies Incorporated. Their jobs vary from being the front desk receptionist, analyst, to sales associate for Companies Incorporated. They are very respectable, bright, and diligent works for the company. They show up to work ready to tackle a full day ahead of themselves.

Since they are just normal staff for the company, they are placed with very strict permissions. Which means Ms. Haddy, Flux, and Madge have special permissions to specific folder(s). With that being said, they have the ability READ only for the Employee folder. They are able to READ in order to access their training modules, policies, and programs and see the files that they need to work on. They are not offered WRITE or EXECUTE permissions because it is possible that they may make mistakes or worse, upload suspicious malware or viruses within the folder.

Folders that they may access includes Company Policies and Employees as well as its internal files. They are only restricted to the READ permission for their restricted files.

Group: CSIR Team

Members: Flux

Members of the Computer Security Incident Response Team will be responsible for all security measures around the company as well as testing technology and security equipment for accessibility and safety. This position will be taken by Flux.

This group will be able to READ, WRITE, and EXECUTE the following folders: Compliance, Security, and Security Breaches. Permissions remains the same for their internal files except for the file Independent Audit from the Security Breaches folder. In this file, the group is only restricted to a READ only permission as this file was created from a third party company.

Group: SETA Team

Members: Miss Haddy

Also known as Security Education Training and Awareness Team, this group is responsible to create training documents and procedures that benefits the whole staff's awareness and knowledge of the security technology around our company. This position will be taken by Miss Haddy.

This group will be able to READ, WRITE, and EXECUTE the Employees folder as well as its internal files. Since they are responsible to create education guidelines in our company, it would make sense to let this group WRITE up in this folder. This group are also allowed to READ the folder Company Policies.

Group: HR Team

Members: Madge

This group will be in charge of Human Resources. For our company, we have Madge take up this position. In this position, members are to help create policies for the company.

With that, this group should be able to access the folder Company Policies as well as its internal files. This group should be able to READ, WRITE, and EXECUTE the Company Policies folder. This group also has access to READ the folder Employees as well as its internal files. They are also allowed to READ the folder Employees as well as its internal files.

Group: IT Admin

Members: Brandon

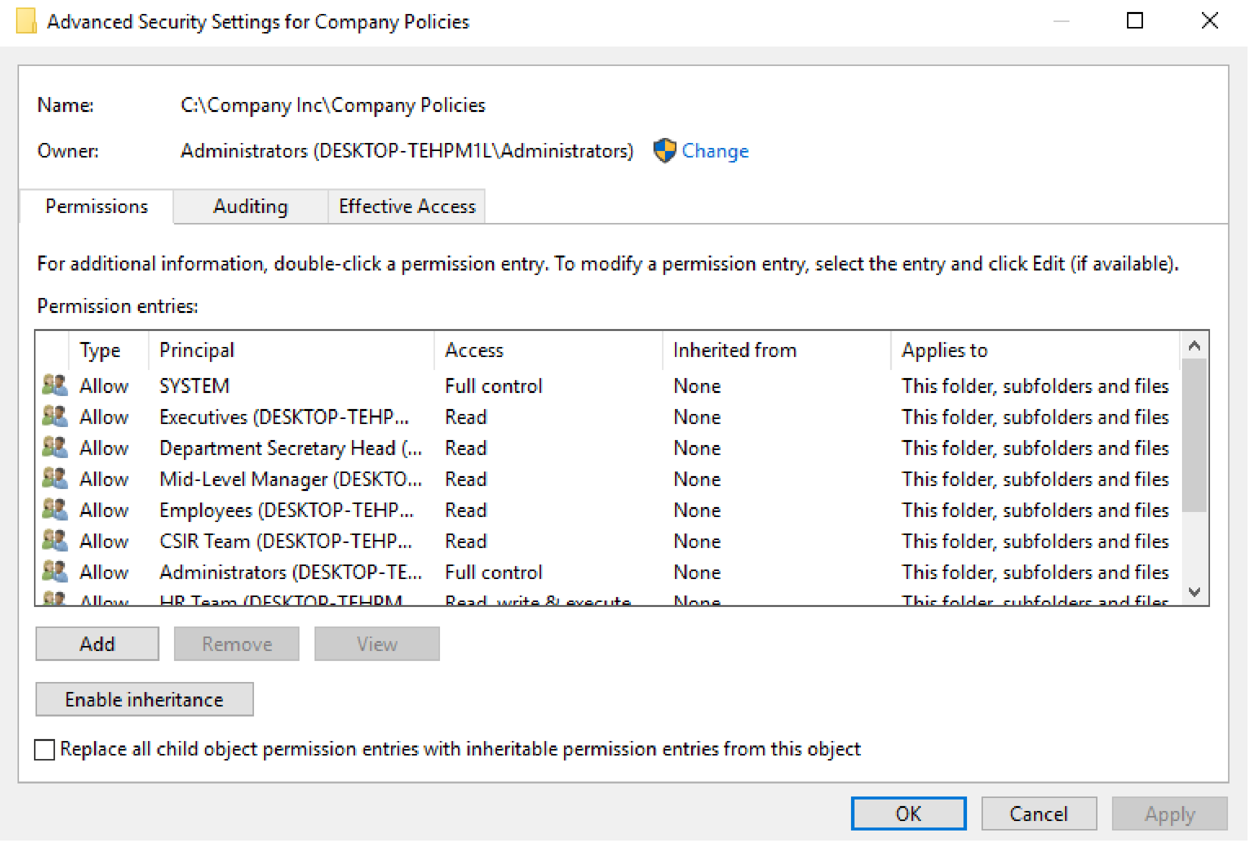
The Companies Inc. want to keep all of our files safe. It has been a rollercoaster of events for deciding who should be admin for our company. First it was decided that the Department Head or Manager should be admin. However, some files are restricted for them and we would like to keep every position's privacy in check. With that being said, the best thing to do is to hire a new member that can fill in our new IT Administrator Manager position. Our new member, Brandon, was chosen to fill in this role.

Here, he is responsible to make any possible changes or privileges among company folders. Being IT Admin, he gains full access of all company folders and can decide which groups of members can access or cannot access such folders and files. To ensure admin rights, Brandon must gain a level of trust among company members. We believe he is suited to do the job done.

Permissions for Folders and Files

Folder: Company Policies

- HR Team = Read, Write, and Execute
- Executives = Read
- Department Secretary Head = Read
- Mid-Level Manager = Read
- Employees = Read
- CSIR Team = Read
- SETA Team = Read
- IT Admin = Full Control



Advanced Security Settings for Company Policies

Name: C:\Company Inc\Company Policies

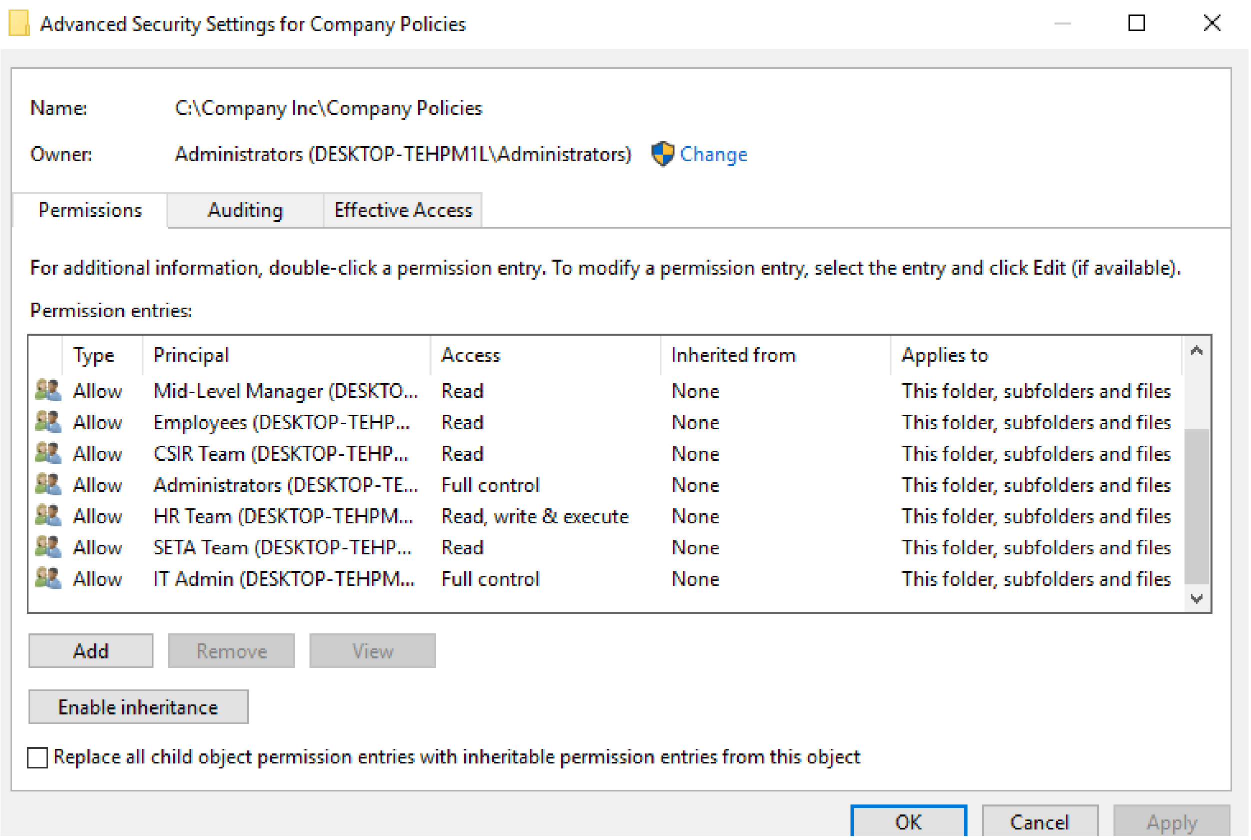
Owner: Administrators (DESKTOP-TEHPM1L\Administrators) Change

For additional information, double-click a permission entry. To modify a permission entry, select the entry and click Edit (if available).

Permission entries:

Type	Principal	Access	Inherited from	Applies to
Allow	SYSTEM	Full control	None	This folder, subfolders and files
Allow	Executives (DESKTOP-TEHP...	Read	None	This folder, subfolders and files
Allow	Department Secretary Head (...	Read	None	This folder, subfolders and files
Allow	Mid-Level Manager (DESKTO...	Read	None	This folder, subfolders and files
Allow	Employees (DESKTOP-TEHP...	Read	None	This folder, subfolders and files
Allow	CSIR Team (DESKTOP-TEHP...	Read	None	This folder, subfolders and files
Allow	Administrators (DESKTOP-TE...	Full control	None	This folder, subfolders and files
Allow	HR Team (DESKTOP-TEHPM	Read, write & execute	None	This folder, subfolders and files

□ Replace all child object permission entries with inheritable permission entries from this object



Advanced Security Settings for Company Policies

Name: C:\Company Inc\Company Policies

Owner: Administrators (DESKTOP-TEHPM1L\Administrators)

For additional information, double-click a permission entry. To modify a permission entry, select the entry and click Edit (if available).

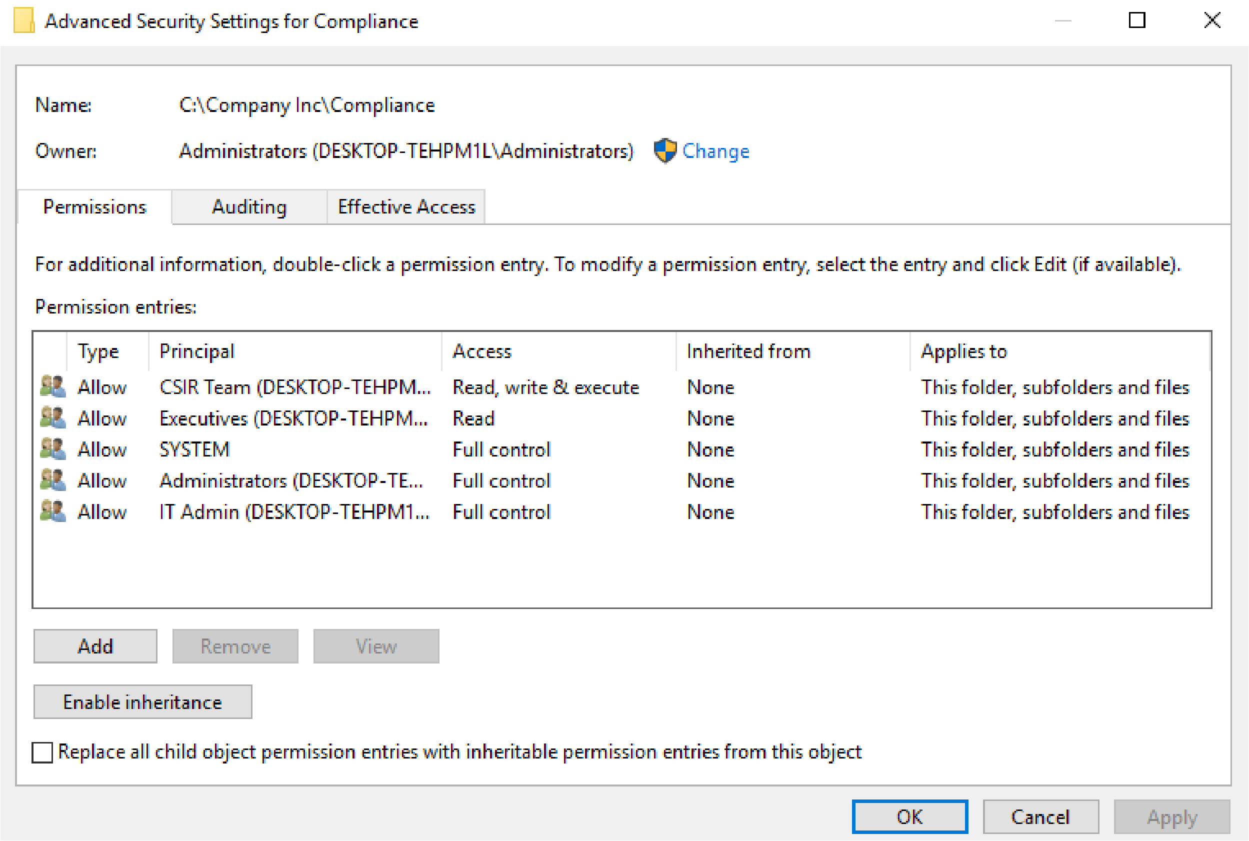
Permission entries:

Type	Principal	Access	Inherited from	Applies to
Allow	Mid-Level Manager (DESKTO...	Read	None	This folder, subfolders and files
Allow	Employees (DESKTOP-TEHP...	Read	None	This folder, subfolders and files
Allow	CSIR Team (DESKTOP-TEHP...	Read	None	This folder, subfolders and files
Allow	Administrators (DESKTOP-TE...	Full control	None	This folder, subfolders and files
Allow	HR Team (DESKTOP-TEHPM...	Read, write & execute	None	This folder, subfolders and files
Allow	SETA Team (DESKTOP-TEHP...	Read	None	This folder, subfolders and files
Allow	IT Admin (DESKTOP-TEHPM...	Full control	None	This folder, subfolders and files

☐ Replace all child object permission entries with inheritable permission entries from this object

Folder: Compliance

- CSIR Team = Read, Write, and Execute
- Executives = Read
- IT Admin = Full Control



Advanced Security Settings for Compliance

Name: C:\Company Inc\Compliance

Owner: Administrators (DESKTOP-TEHPM1L\Administrators)

For additional information, double-click a permission entry. To modify a permission entry, select the entry and click Edit (if available).

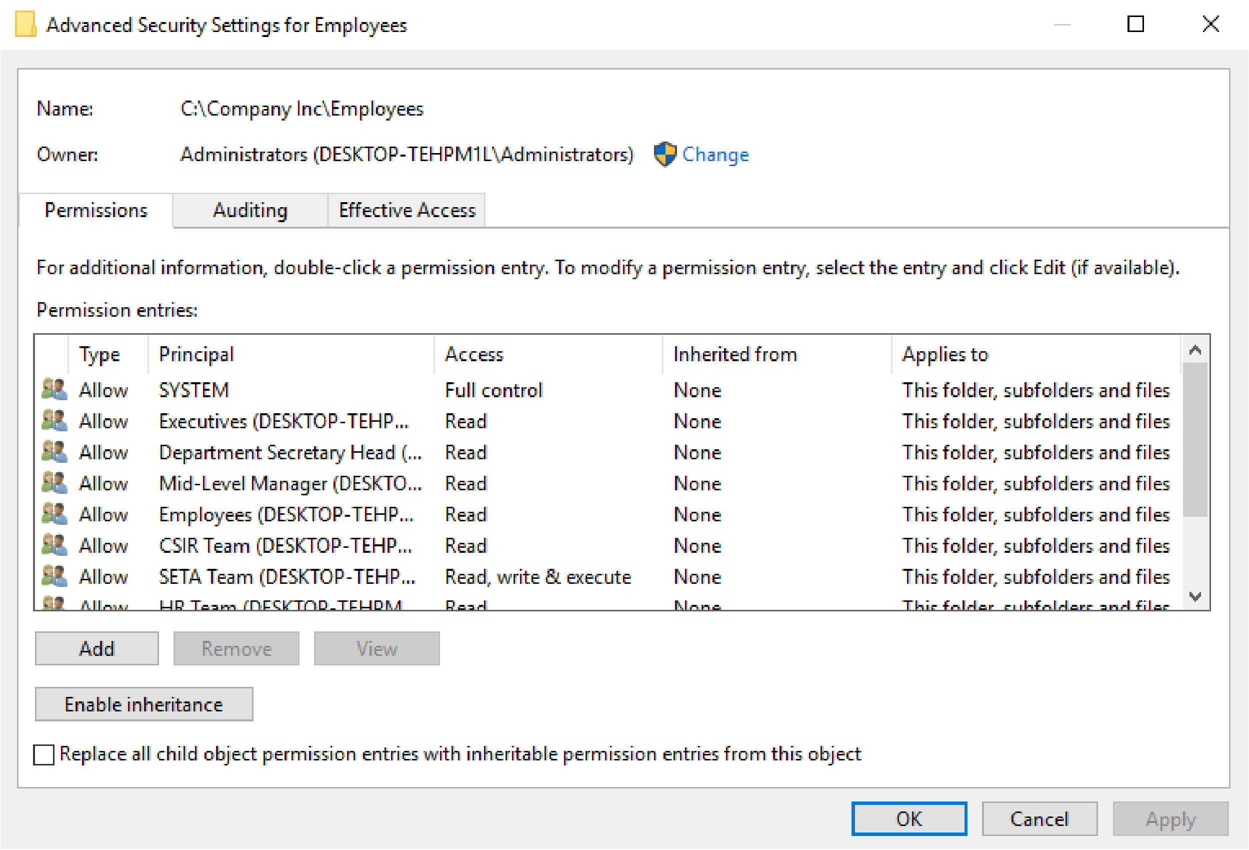
Permission entries:

Type	Principal	Access	Inherited from	Applies to
Allow	CSIR Team (DESKTOP-TEHPM...	Read, write & execute	None	This folder, subfolders and files
Allow	Executives (DESKTOP-TEHPM...	Read	None	This folder, subfolders and files
Allow	SYSTEM	Full control	None	This folder, subfolders and files
Allow	Administrators (DESKTOP-TE...	Full control	None	This folder, subfolders and files
Allow	IT Admin (DESKTOP-TEHPM1...	Full control	None	This folder, subfolders and files

□ Replace all child object permission entries with inheritable permission entries from this object

Folder: Employees

- SETA Team = Read, Write, and Execute
- Executives = Read
- Department Secretary Head = Read
- Mid-Level Manager = Read
- Employees = Read
- CSIR Team = Read
- HR Team = Read
- IT Admin = Full Control



Advanced Security Settings for Employees

Name: C:\Company Inc\Employees

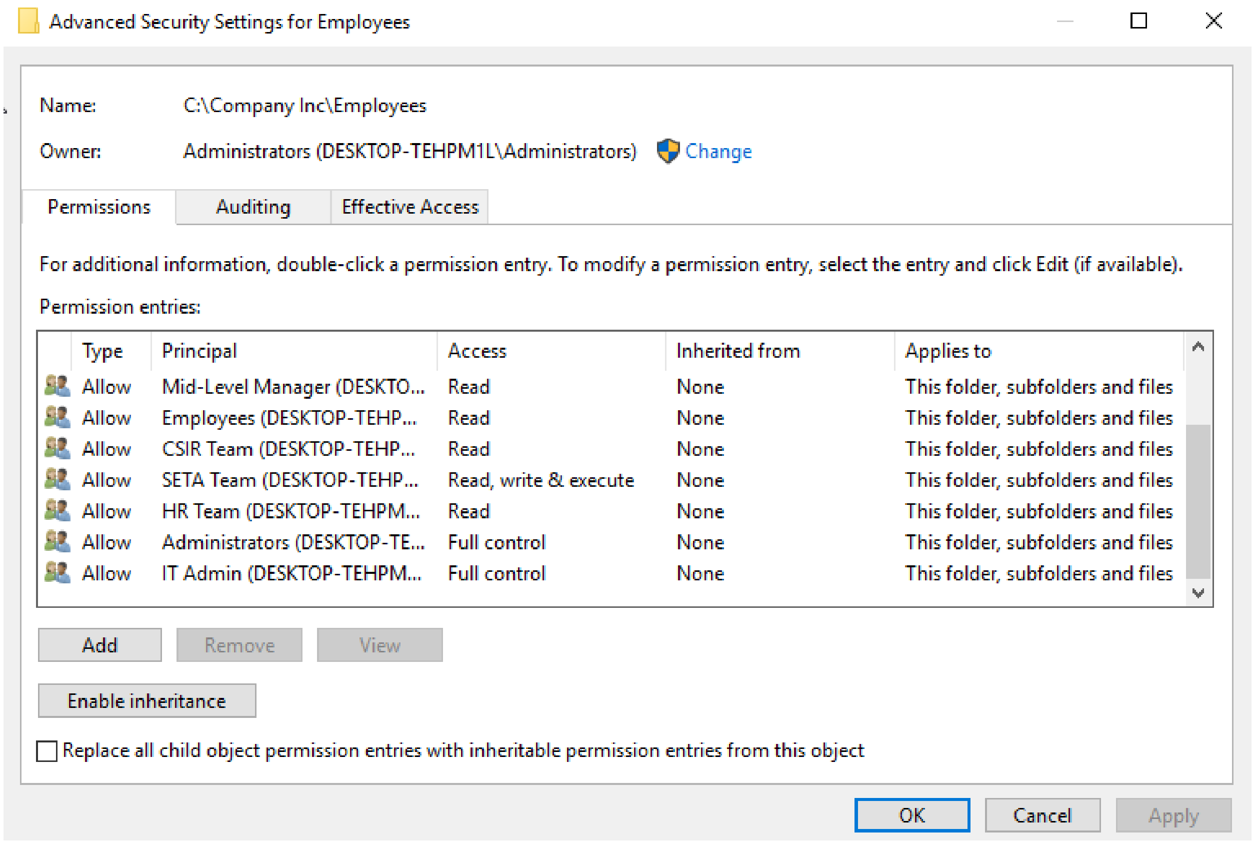
Owner: Administrators (DESKTOP-TEHPM1L\Administrators)

For additional information, double-click a permission entry. To modify a permission entry, select the entry and click Edit (if available).

Permission entries:

Type	Principal	Access	Inherited from	Applies to
Allow	SYSTEM	Full control	None	This folder, subfolders and files
Allow	Executives (DESKTOP-TEHP...	Read	None	This folder, subfolders and files
Allow	Department Secretary Head (...	Read	None	This folder, subfolders and files
Allow	Mid-Level Manager (DESKTO...	Read	None	This folder, subfolders and files
Allow	Employees (DESKTOP-TEHP...	Read	None	This folder, subfolders and files
Allow	CSIR Team (DESKTOP-TEHP...	Read	None	This folder, subfolders and files
Allow	SETA Team (DESKTOP-TEHP...	Read, write & execute	None	This folder, subfolders and files
Allow	HR Team (DESKTOP-TEHPM...	Read	None	This folder, subfolders and files

☐ Replace all child object permission entries with inheritable permission entries from this object



Name: C:\Company Inc\Employees

Owner: Administrators (DESKTOP-TEHPM1L\Administrators) Change

For additional information, double-click a permission entry. To modify a permission entry, select the entry and click Edit (if available).

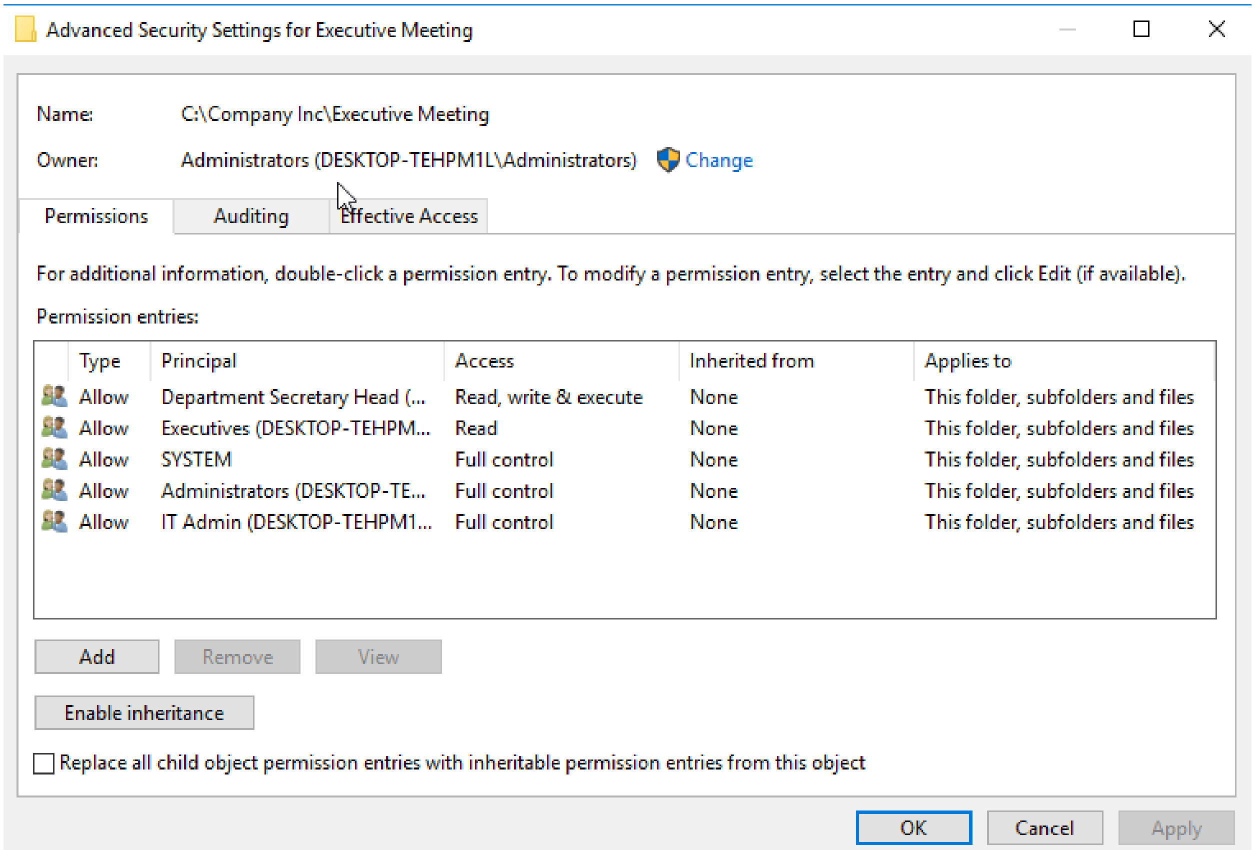
Permission entries:

Type	Principal	Access	Inherited from	Applies to
Allow	Mid-Level Manager (DESKTO...	Read	None	This folder, subfolders and files
Allow	Employees (DESKTOP-TEHP...	Read	None	This folder, subfolders and files
Allow	CSIR Team (DESKTOP-TEHP...	Read	None	This folder, subfolders and files
Allow	SETA Team (DESKTOP-TEHP...	Read, write & execute	None	This folder, subfolders and files
Allow	HR Team (DESKTOP-TEHPM...	Read	None	This folder, subfolders and files
Allow	Administrators (DESKTOP-TE...	Full control	None	This folder, subfolders and files
Allow	IT Admin (DESKTOP-TEHPM...	Full control	None	This folder, subfolders and files

☐ Replace all child object permission entries with inheritable permission entries from this object

Folder: Executive Meetings

- Department Secretary Head = Read, Write, and Execute
- Executives = Read
- IT Admin = Full Control



Advanced Security Settings for Executive Meeting

Name: C:\Company Inc\Executive Meeting

Owner: Administrators (DESKTOP-TEHPM1L\Administrators) Change

For additional information, double-click a permission entry. To modify a permission entry, select the entry and click Edit (if available).

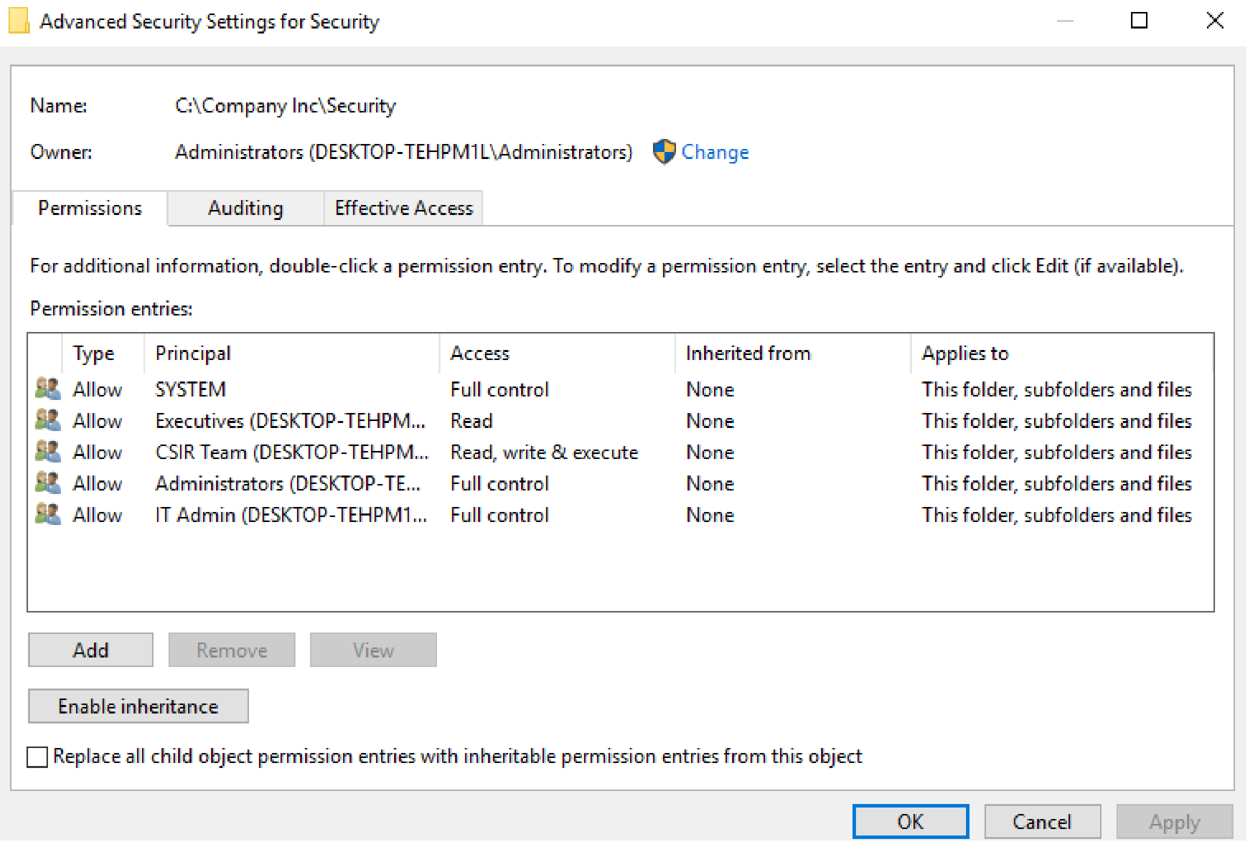
Permission entries:

Type	Principal	Access	Inherited from	Applies to
Allow	Department Secretary Head (...	Read, write & execute	None	This folder, subfolders and files
Allow	Executives (DESKTOP-TEHPM...	Read	None	This folder, subfolders and files
Allow	SYSTEM	Full control	None	This folder, subfolders and files
Allow	Administrators (DESKTOP-TE...	Full control	None	This folder, subfolders and files
Allow	IT Admin (DESKTOP-TEHPM1...	Full control	None	This folder, subfolders and files

□ Replace all child object permission entries with inheritable permission entries from this object

Folder: Security

- CSIR Team = Read, Write, and Execute
- Executives = Read
- IT Admin = Full Control



Advanced Security Settings for Security

Name: C:\Company Inc\Security

Owner: Administrators (DESKTOP-TEHPM1L\Administrators) Change

For additional information, double-click a permission entry. To modify a permission entry, select the entry and click Edit (if available).

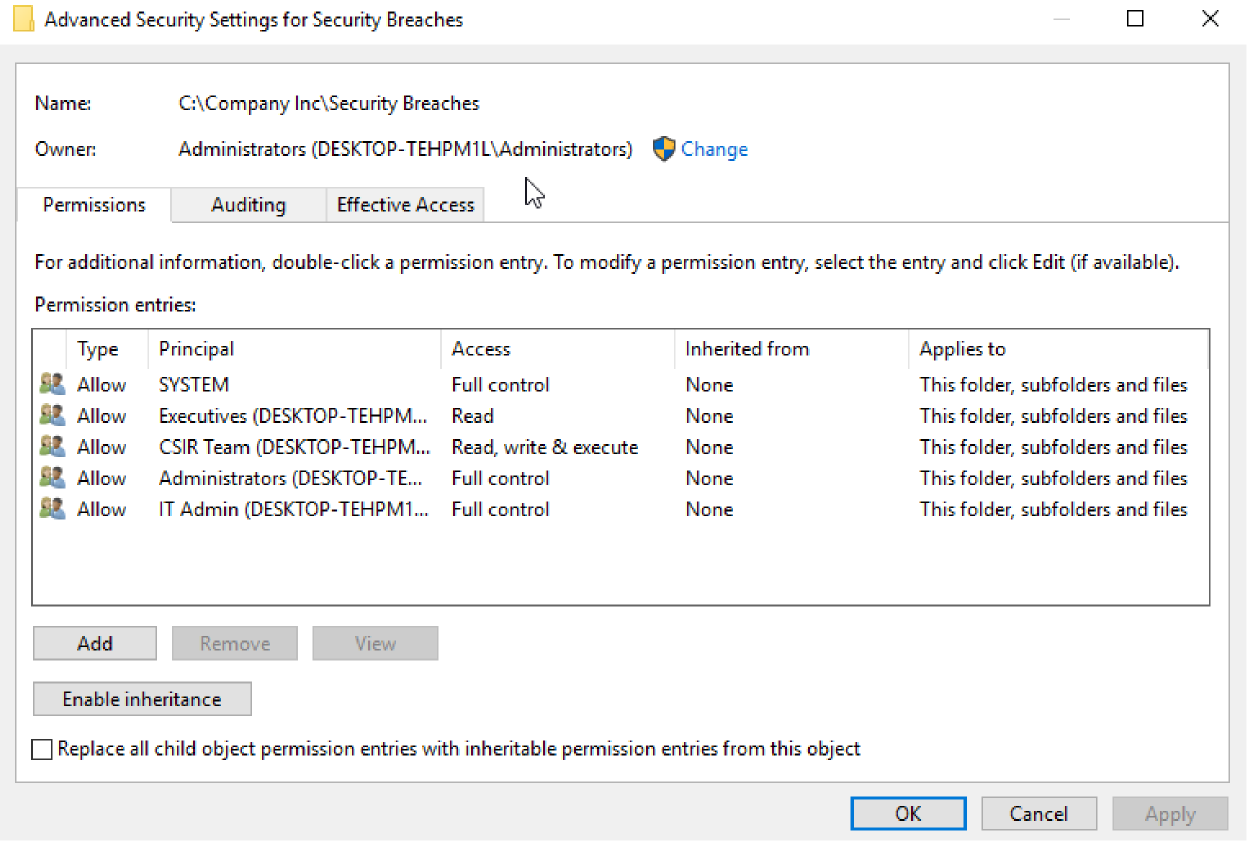
Permission entries:

Type	Principal	Access	Inherited from	Applies to
Allow	SYSTEM	Full control	None	This folder, subfolders and files
Allow	Executives (DESKTOP-TEHPM...	Read	None	This folder, subfolders and files
Allow	CSIR Team (DESKTOP-TEHPM...	Read, write & execute	None	This folder, subfolders and files
Allow	Administrators (DESKTOP-TE...	Full control	None	This folder, subfolders and files
Allow	IT Admin (DESKTOP-TEHPM1...	Full control	None	This folder, subfolders and files

□ Replace all child object permission entries with inheritable permission entries from this object

Folder: Security Breaches

- CSIR Team = Read, Write, and Execute
- Executives = Read
- IT Admin = Full Control



Advanced Security Settings for Security Breaches

Name: C:\Company Inc\Security Breaches

Owner: Administrators (DESKTOP-TEHPM1L\Administrators) Change

For additional information, double-click a permission entry. To modify a permission entry, select the entry and click Edit (if available).

Permission entries:

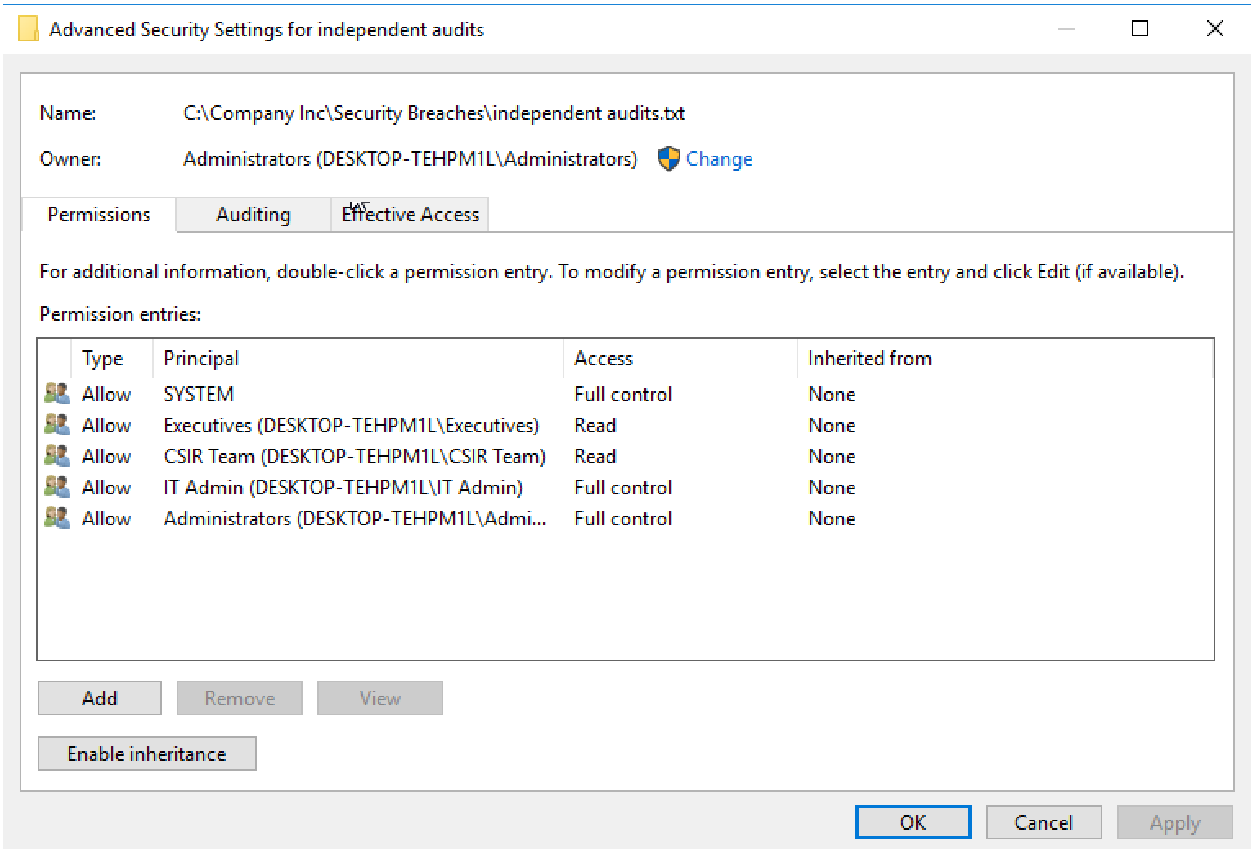
Type	Principal	Access	Inherited from	Applies to
Allow	SYSTEM	Full control	None	This folder, subfolders and files
Allow	Executives (DESKTOP-TEHPM...	Read	None	This folder, subfolders and files
Allow	CSIR Team (DESKTOP-TEHPM...	Read, write & execute	None	This folder, subfolders and files
Allow	Administrators (DESKTOP-TE...	Full control	None	This folder, subfolders and files
Allow	IT Admin (DESKTOP-TEHPM1...	Full control	None	This folder, subfolders and files

□ Replace all child object permission entries with inheritable permission entries from this object

File: Independent Audits

This file is a special since this was delivered and created from a third party company. Unlike our internal audit, this independent audit should not be able to have access to WRITE for the specified groups.

- CSIR Team = Read
- Executives = Read
- IT Admin = Full Control



Advanced Security Settings for independent audits

Name: C:\Company Inc\Security Breaches\independent audits.txt

Owner: Administrators (DESKTOP-TEHPM1L\Administrators) Change

For additional information, double-click a permission entry. To modify a permission entry, select the entry and click Edit (if available).

Permission entries:

Type	Principal	Access	Inherited from
Allow	SYSTEM	Full control	None
Allow	Executives (DESKTOP-TEHPM1L\Executives)	Read	None
Allow	CSIR Team (DESKTOP-TEHPM1L\CSIR Team)	Read	None
Allow	IT Admin (DESKTOP-TEHPM1L\IT Admin)	Full control	None
Allow	Administrators (DESKTOP-TEHPM1L\Admi...	Full control	None

Created Passwords for Login

Gru = password4ceo

El Macho = password4cso

Herb = password4cio

Lucy = password4cro

Scarlet = password4depthead

Walter = password4manager

Miss Haddy = password4staff1

Flux = password4staff2

Madge = password4staff3

Brandon = password4admin