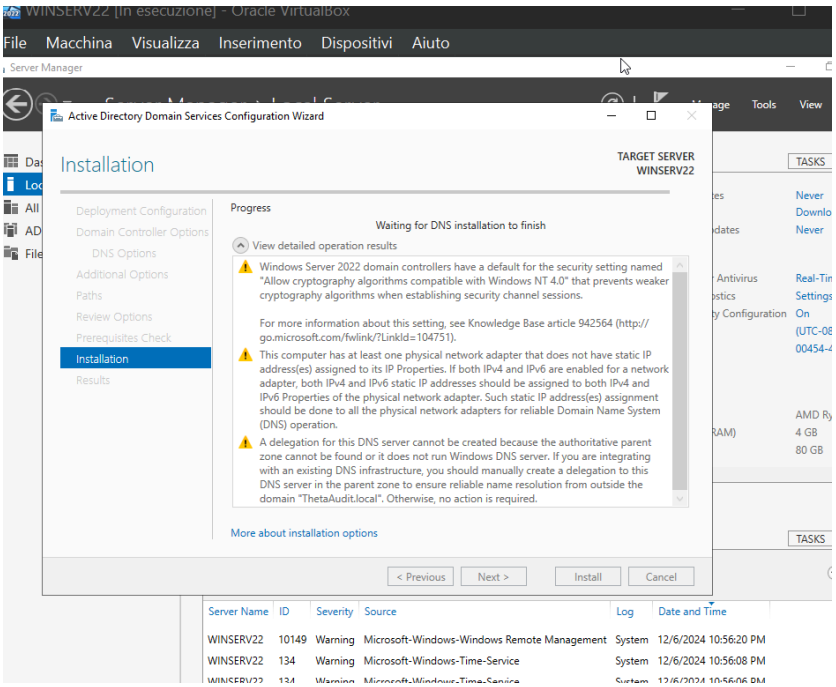
Introduction

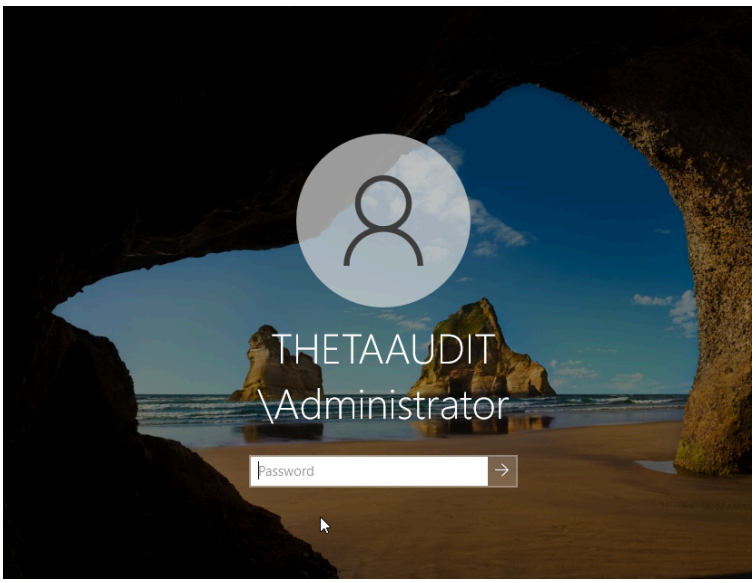
This document details a critical project undertaken for the company Theta to optimize user group management within Windows Server 2022. The initiative aimed to support the company's fiscal year-end review (FYE2024) by creating distinct user groups with specific permissions to streamline workflows and enhance data security.The project involved configuring an efficient system that allowed secure access to sensitive financial information, fostering collaboration, and ensuring the integrity of data through well-defined access controls. This document outlines the process, key configurations, and outcomes, offering a comprehensive look at the strategies employed to achieve these goals.

Initial Setup and Preparation

The first step was to set up the environment on Windows Server 2022. To ensure smooth execution:

- Administrative access was secured to create and manage groups.
- An Active Directory forest was established to serve as the foundational framework for group management.
- Organizational Units (OUs) were created within the Active Directory to segregate users based on roles and responsibilities.





Three OUs were configured:

FinanceAdmin: Designed for high-level financial administrators.

FinanceUsers: Tailored for general finance team members.

ExternalAuditors: Created to provide restricted access to external auditors for reviewing final fiscal data.

Each Organizational Unit contained users assigned based on their roles:

FinanceAdmin OU: Included a user named Fantozzi.

FinanceUsers OU: Included a user named Fantozzina.

ExternalAuditors OU: Included a user named Filini.

Group Creation

The project proceeded with the creation of distinct user groups, reflecting the specific roles and responsibilities required for the fiscal review process. These groups were:

FinanceAdmin

This group was granted ownership of financial documents and had full permissions to manage them. It included only administrative-level users, such as Fantozzi, who required unrestricted access to ensure the integrity and accuracy of the financial data.

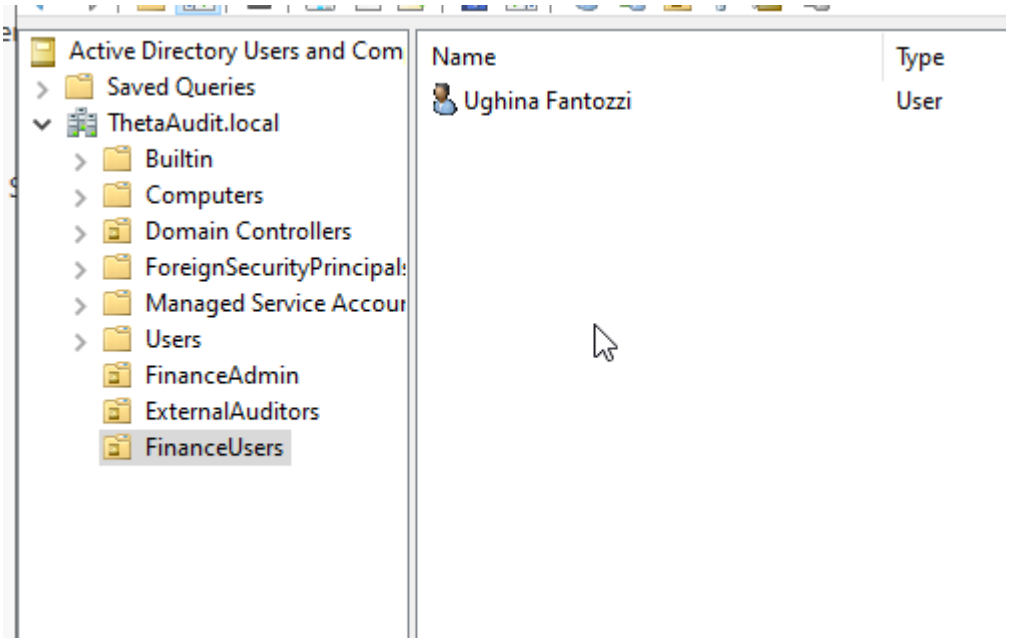
FinanceUsers

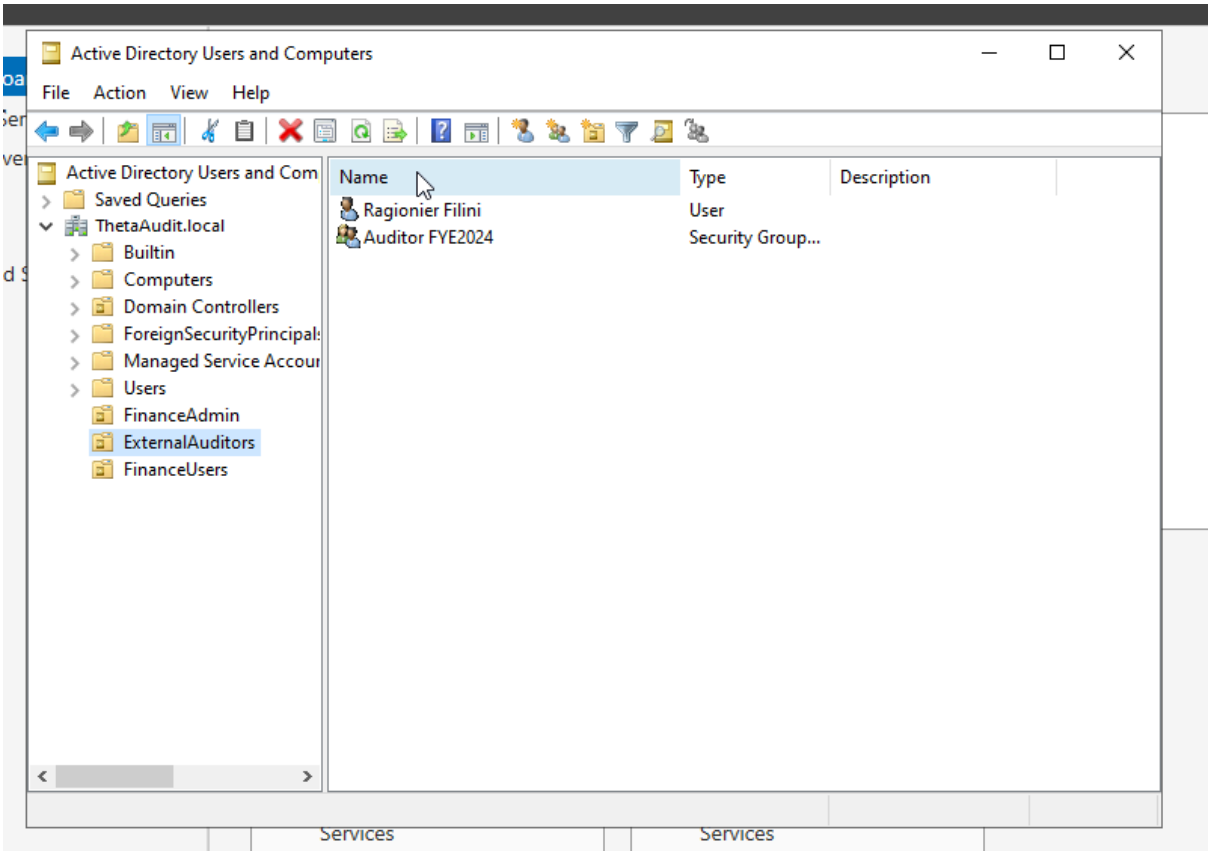
This group included team members like Fantozzina, who were responsible for supporting administrative staff. They were given permission to access and modify working files in specific directories, facilitating collaboration within the department.

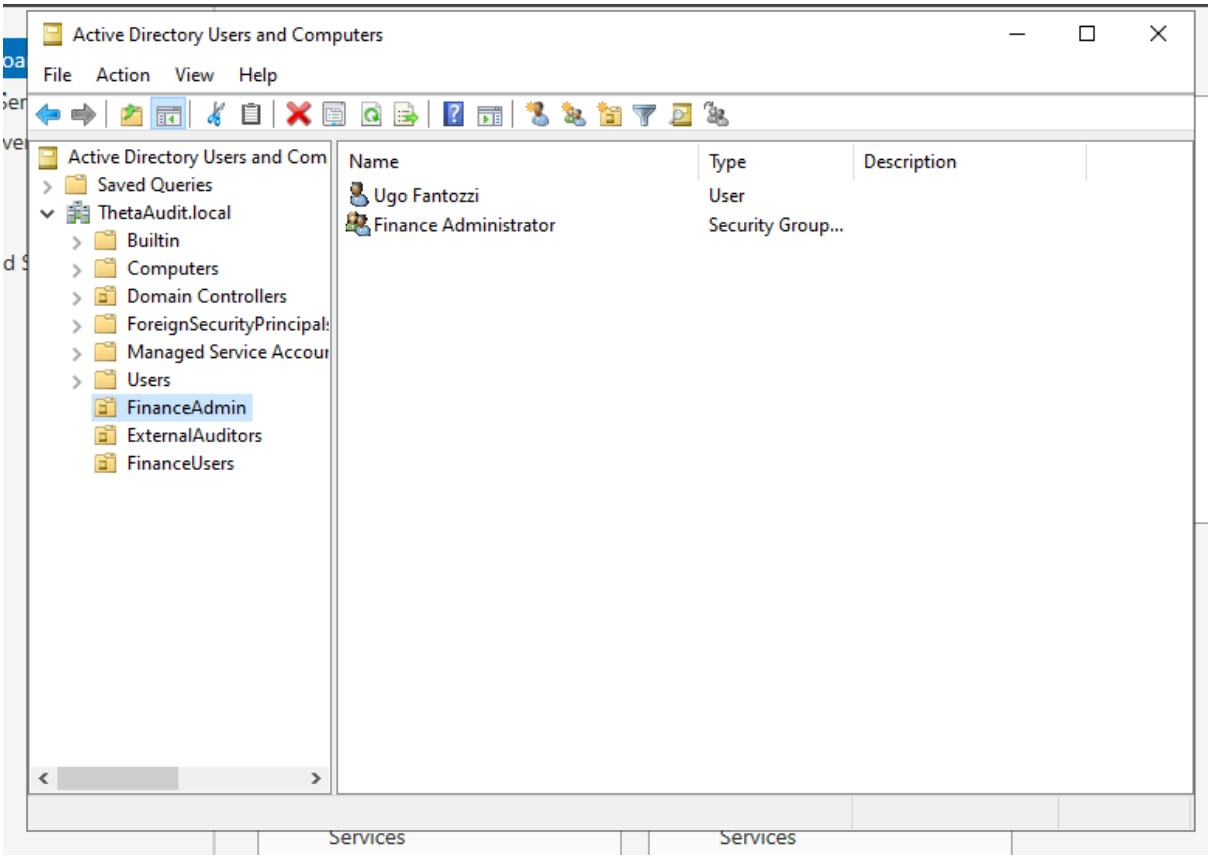
ExternalAuditors

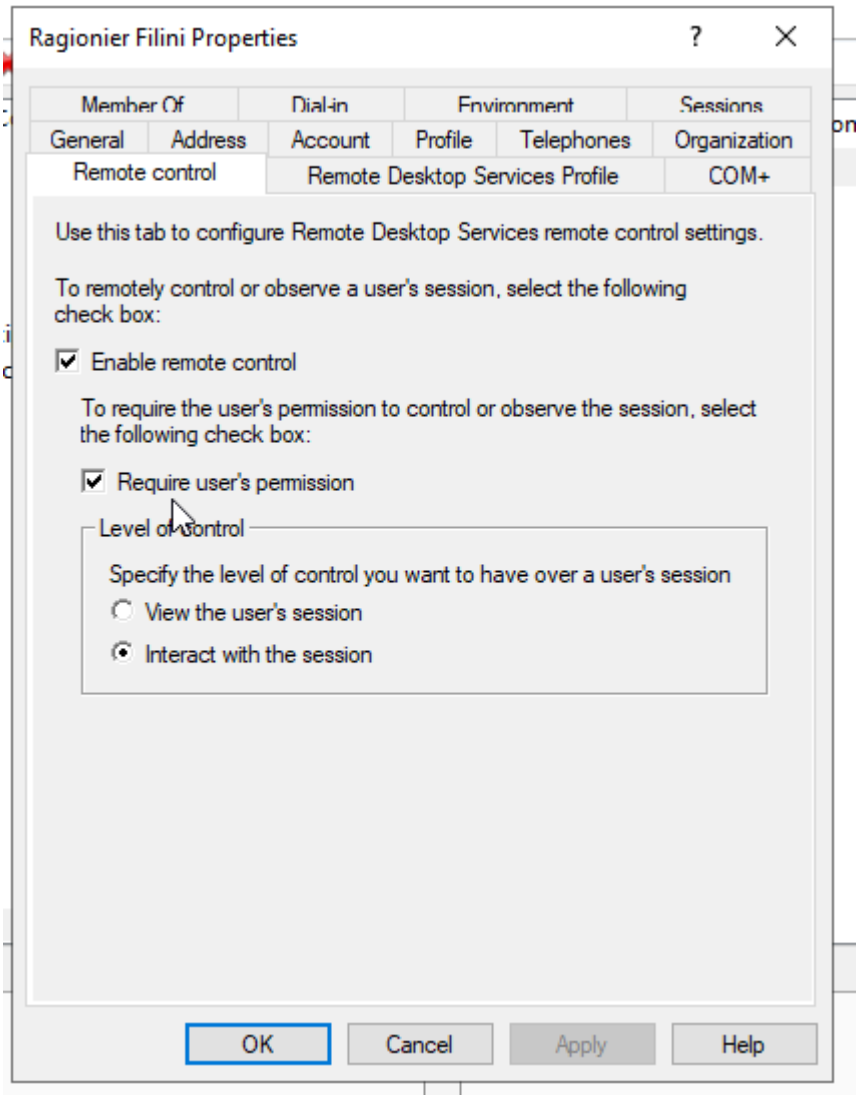
This group was limited to read-only permissions on finalized documents. This restriction ensured that external auditors, such as Filini, could access the necessary data without altering it, preserving its integrity during the review process.

Additionally, remote desktop control was configured for the ExternalAuditors group, allowing Filini to perform the audit from home without needing to be physically present in the office. This was implemented to enhance flexibility and accommodate modern work practices.




Active Directory Users and Computers
File Action View Help
Active Directory Users and Com
Saved Queries
ThetaAudit.local
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipal:
Managed Service Accour
Users
FinanceAdmin
ExternalAuditors
FinanceUsers
Name
Type
Description
Ragionier Filini
User
Auditor FYE2024
Security Group...
Services
Services


Active Directory Users and Computers
File Action View Help
Active Directory Users and Com
Saved Queries
ThetaAudit.local
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipal:
Managed Service Accour
Users
FinanceAdmin
ExternalAuditors
FinanceUsers
Name
Type
Description
Ugo Fantozzi
User
Finance Administrator
Security Group...
Services
Services



Folder Structure and Permissions

The next step involved creating a folder structure that reflected the workflows and access requirements of the fiscal review process. Two main directories were created:

Audit Progressive Folder

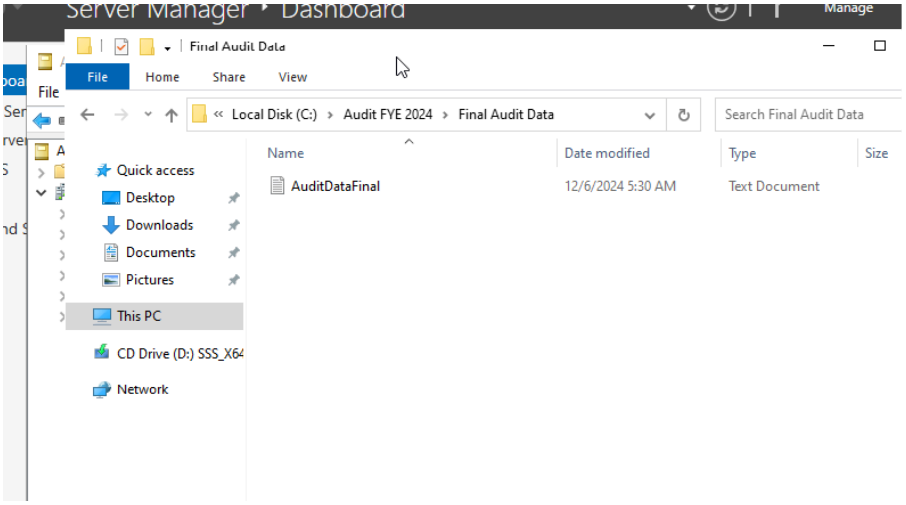
This directory housed sequential review files (e.g., Q1, Q2, Q3, and Q4 reports). The following permissions were assigned:

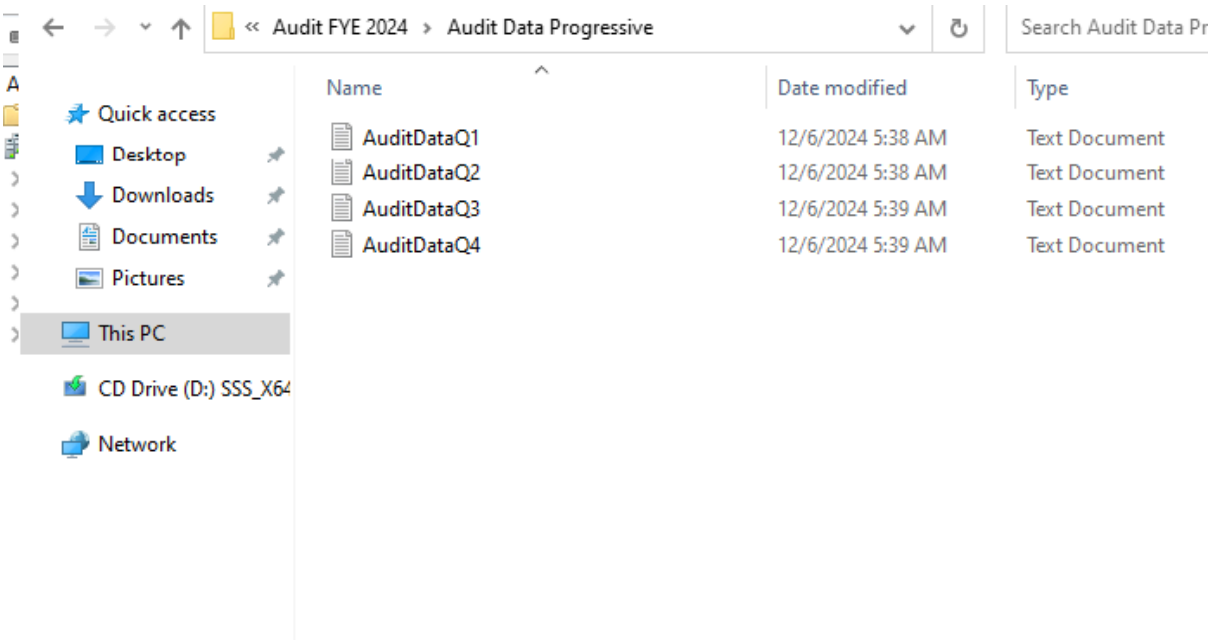
- **FinanceAdmin Group:** Full read and write access to manage, edit, and organize documents.
- **FinanceUsers Group:** Read and write access to contribute to the progressive review process.
- **ExternalAuditors Group:** No access, as auditors only required finalized data.

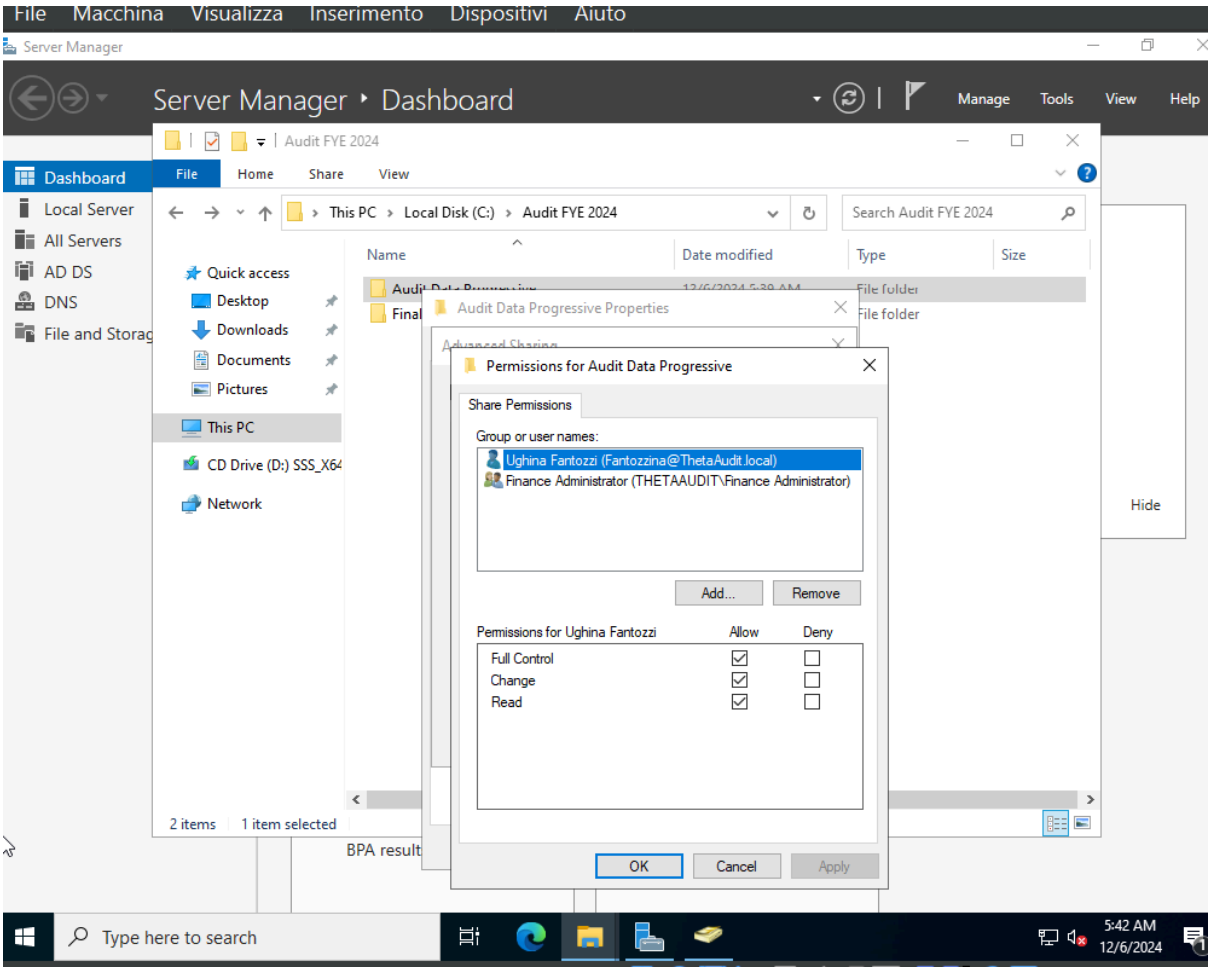
Final Audit Data Folder

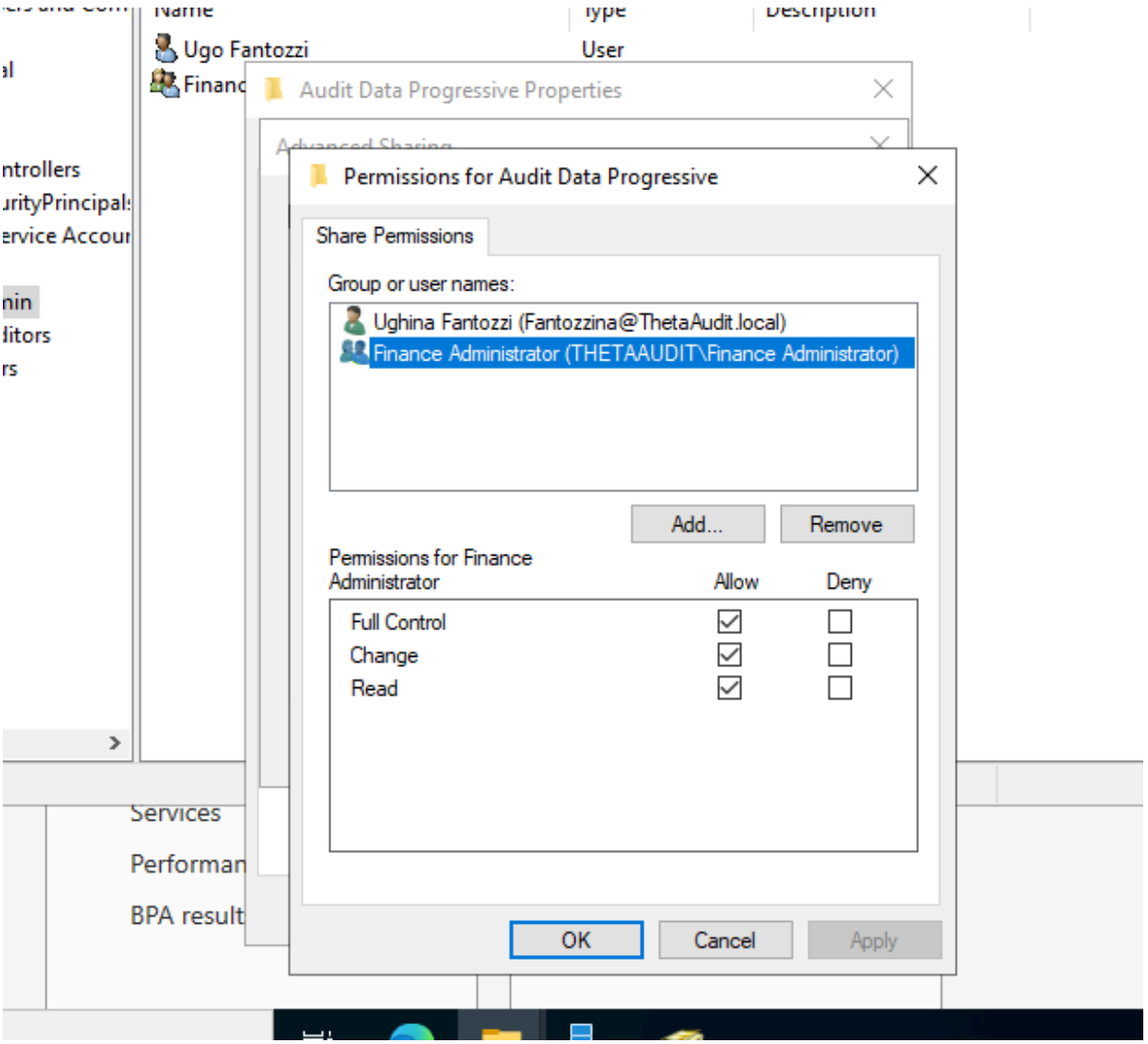
This directory contained the finalized fiscal year-end data. Permissions were as follows:

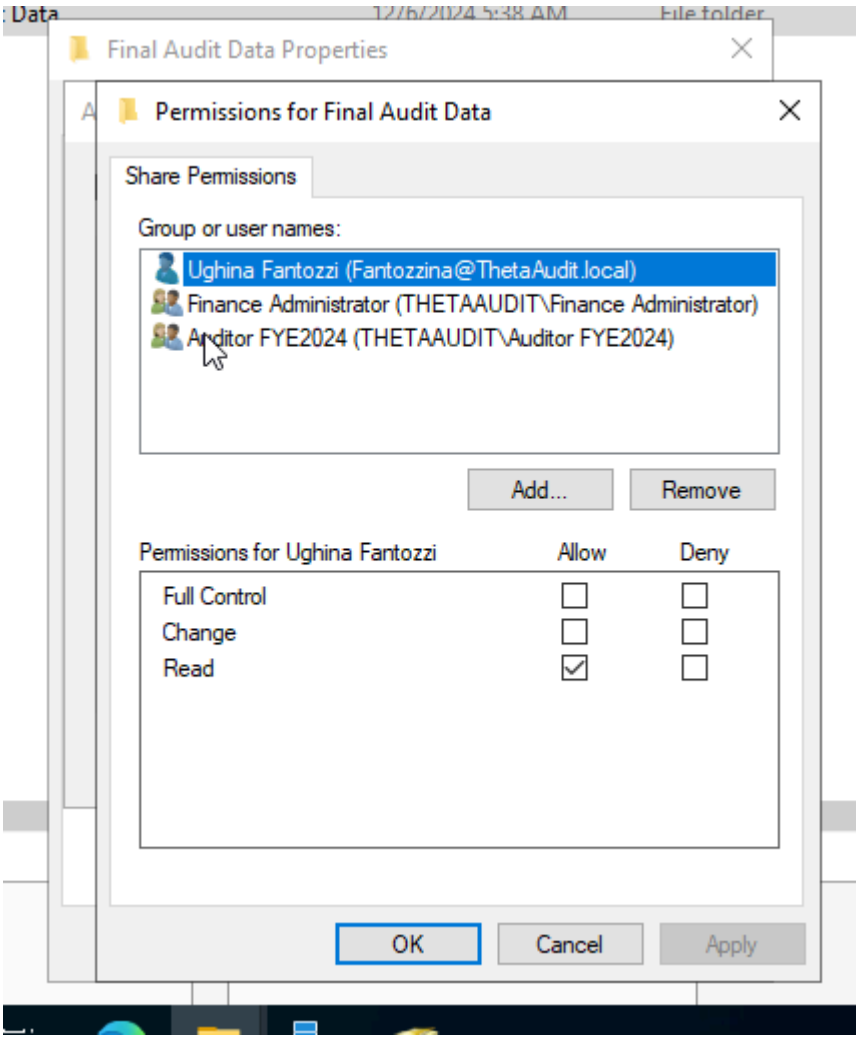
- **FinanceAdmin Group:** Full access, allowing administrators to make final edits and adjustments.
- **FinanceUsers Group:** Read-only access to review the final data without making changes.
- **ExternalAuditors Group:** Read-only access, ensuring they could review the necessary documents without the ability to modify them.

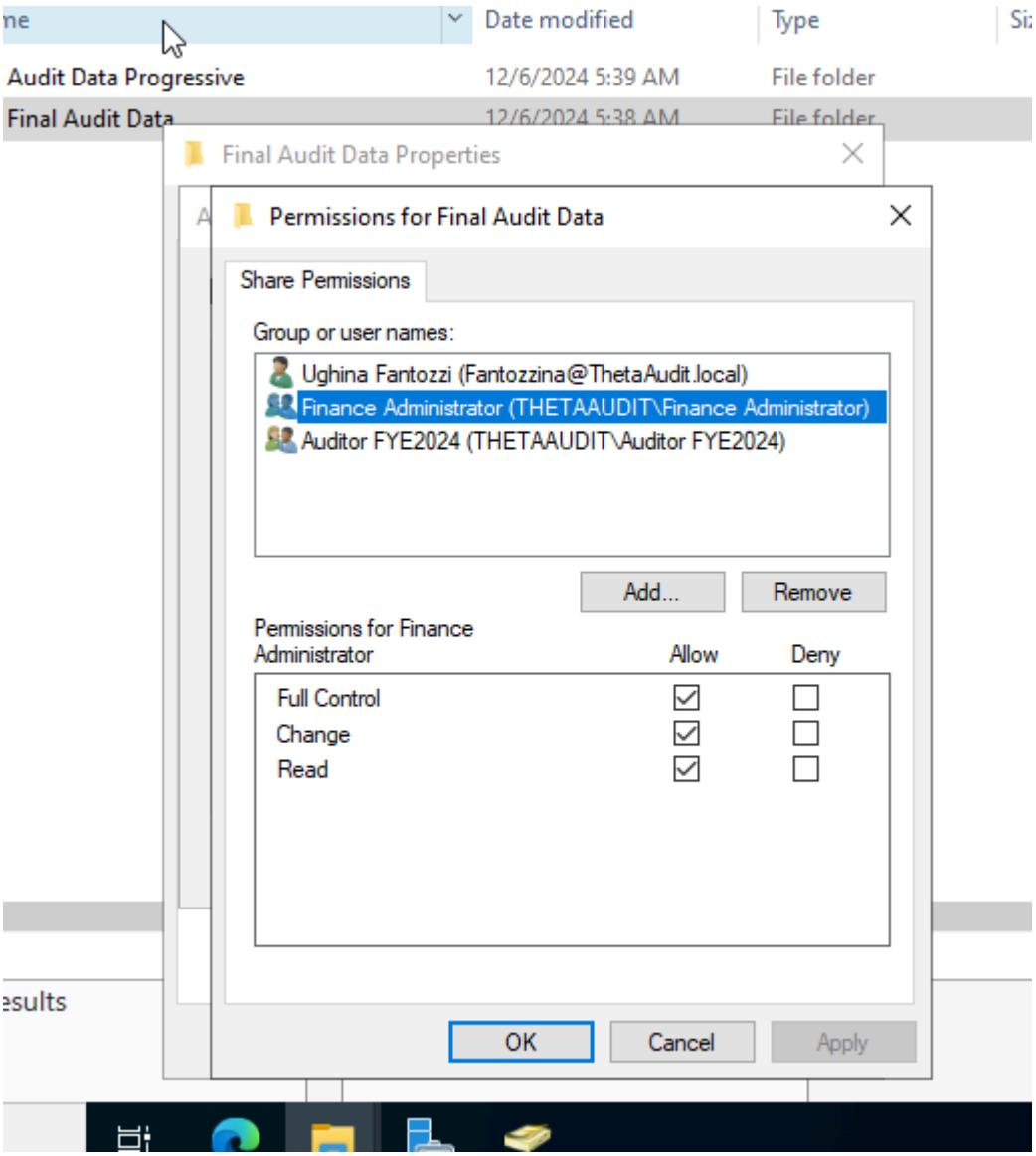


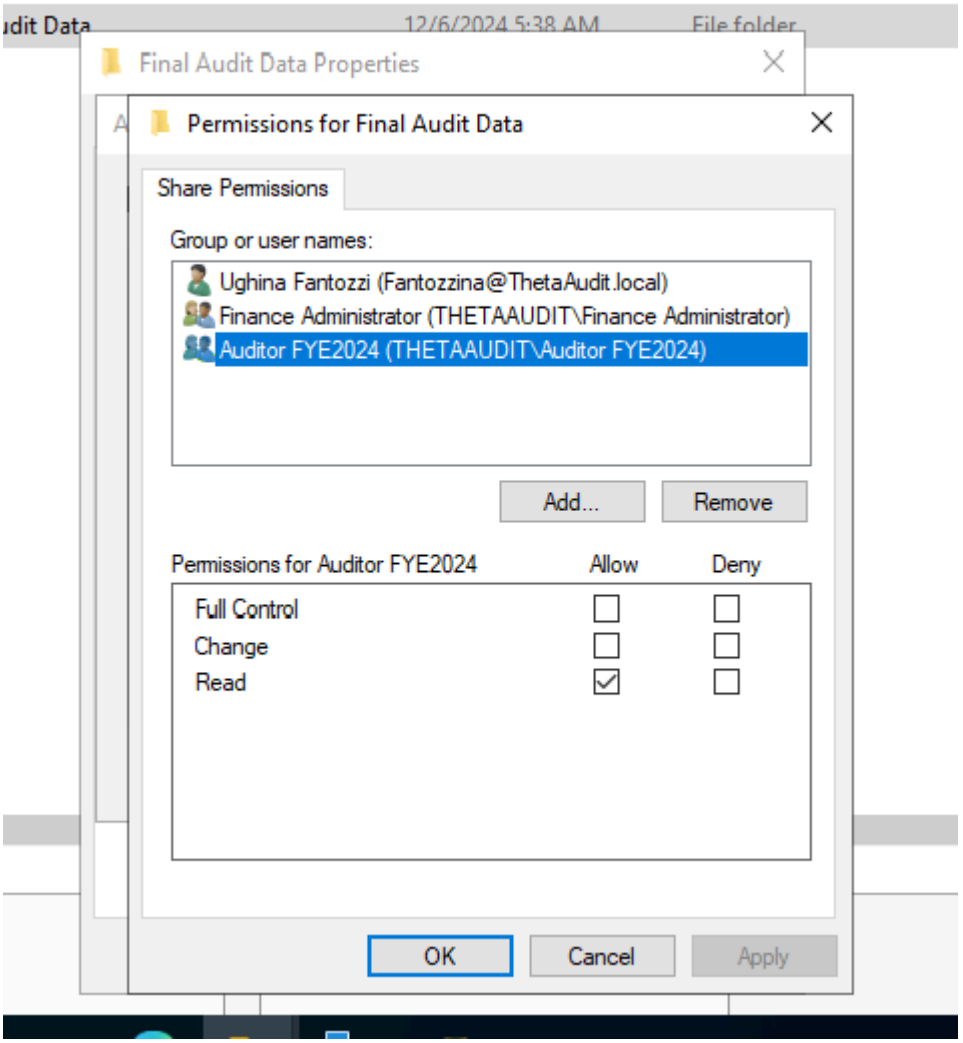



File Macchina Visualizza Inserimento Dispositivi Aiuto
Server Manager
Server Manager • Dashboard
Manage Tools View Help
Dashboard
Local Server
All Servers
AD DS
DNS
File and Storag
Audit FYE 2024
File Home Share View
This PC › Local Disk (C:) › Audit FYE 2024
Search Audit FYE 2024
Quick access
Desktop
Downloads
Documents
Pictures
This PC
CD Drive (D:) SSS_X64
Network
Name
Date modified
Type
Size
File folder
Audit Data Progressive Properties
Permissions for Audit Data Progressive
Share Permissions
Group or user names:
Ughina Fantozzi (Fantozzina@ThetaAudit.local)
Finance Administrator (THETAAUDIT\Finance Administrator)
Add...
Remove
Permissions for Ughina Fantozzi
Allow
Deny
Full Control
Change
Read
OK
Cancel
Apply
Hide
2 items
1 item selected
BPA result
Type here to search
5:42 AM
12/6/2024


Name
Type
Description
Ugo Fantozzi
User
Audit Data Progressive Properties
Permissions for Audit Data Progressive
Share Permissions
Group or user names:
Ughina Fantozzi (Fantozzina@ThetaAudit.local)
Finance Administrator (THETAAUDIT\Finance Administrator)
Add...
Remove
Permissions for Finance Administrator
Allow
Deny
Full Control
Change
Read
OK
Cancel
Apply
Services
Performan
BPA result


Data
12/6/2024 5:38 AM
File folder
Final Audit Data Properties
Permissions for Final Audit Data
Share Permissions
Group or user names:
Ughina Fantozzi (Fantozzina@ThetaAudit.local)
Finance Administrator (THETAAUDIT\Finance Administrator)
Auditor FYE2024 (THETAAUDIT\Auditor FYE2024)
Add...
Remove
Permissions for Ughina Fantozzi
Allow
Deny
Full Control
Change
Read
OK
Cancel
Apply


ne
Date modified
Type
Si
Audit Data Progressive
12/6/2024 5:39 AM
File folder
Final Audit Data
12/6/2024 5:38 AM
File folder
Final Audit Data Properties
Permissions for Final Audit Data
Share Permissions
Group or user names:
Ughina Fantozzi (Fantozzina@ThetaAudit.local)
Finance Administrator (THETAAUDIT\Finance Administrator)
Auditor FYE2024 (THETAAUDIT\Auditor FYE2024)
Add...
Remove
Permissions for Finance Administrator
Allow
Deny
Full Control
Change
Read
OK
Cancel
Apply
esults

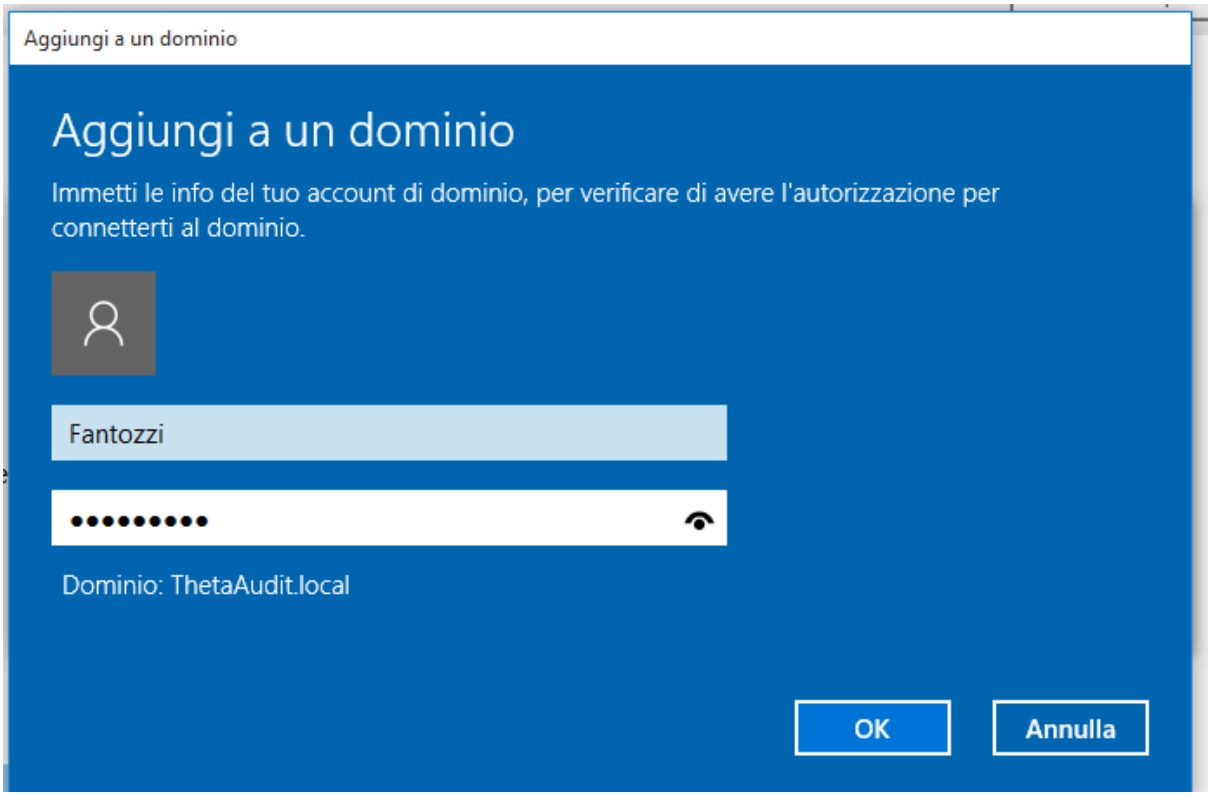

udit Data
12/6/2024 5:38 AM
File folder
Final Audit Data Properties
Permissions for Final Audit Data
Share Permissions
Group or user names:
Ughina Fantozzi (Fantozzina@ThetaAudit.local)
Finance Administrator (THETAAUDIT\Finance Administrator)
Auditor FYE2024 (THETAAUDIT\Auditor FYE2024)
Add...
Remove
Permissions for Auditor FYE2024
Allow
Deny
Full Control
Change
Read
OK
Cancel
Apply

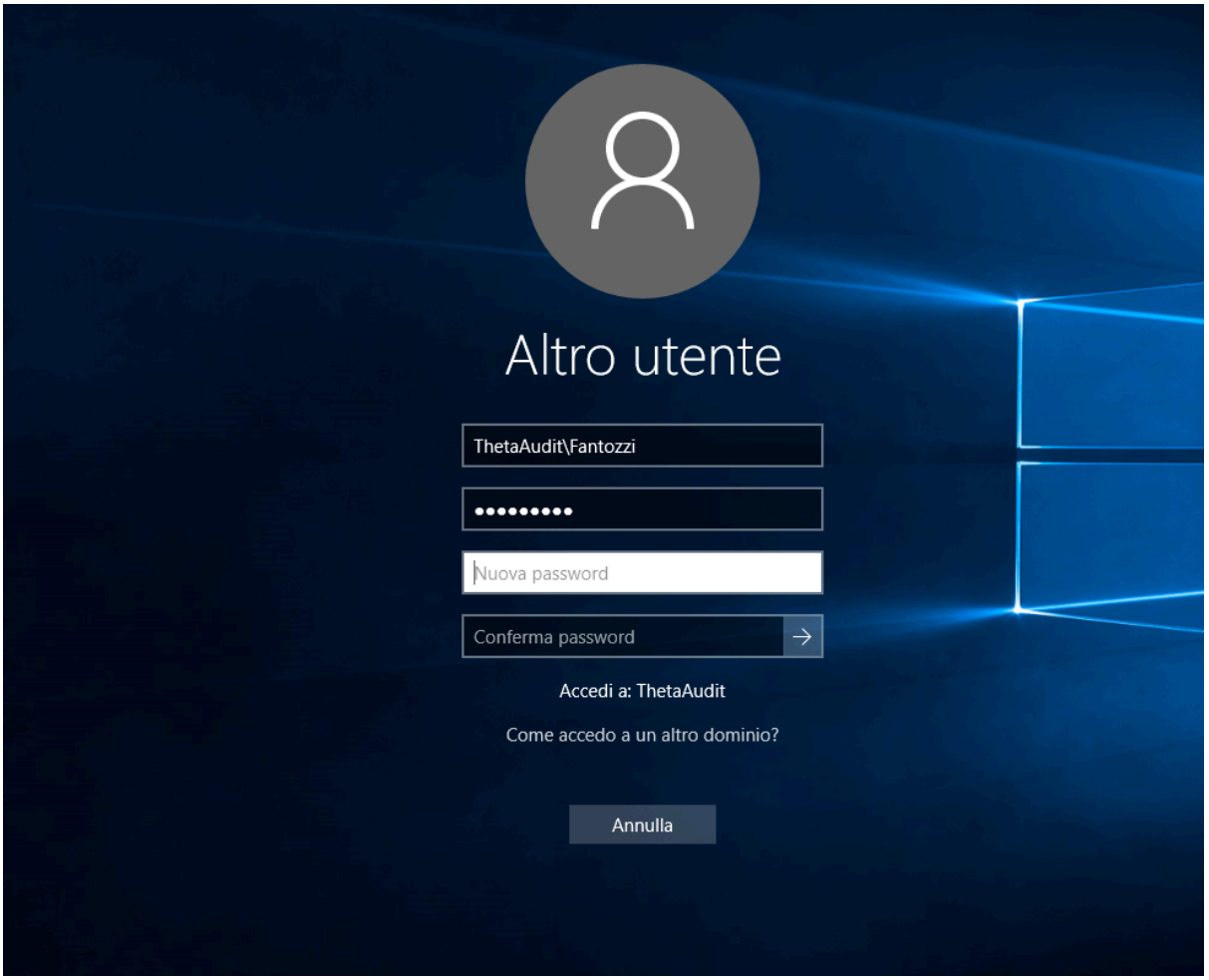
Demonstration for Finance Administrator

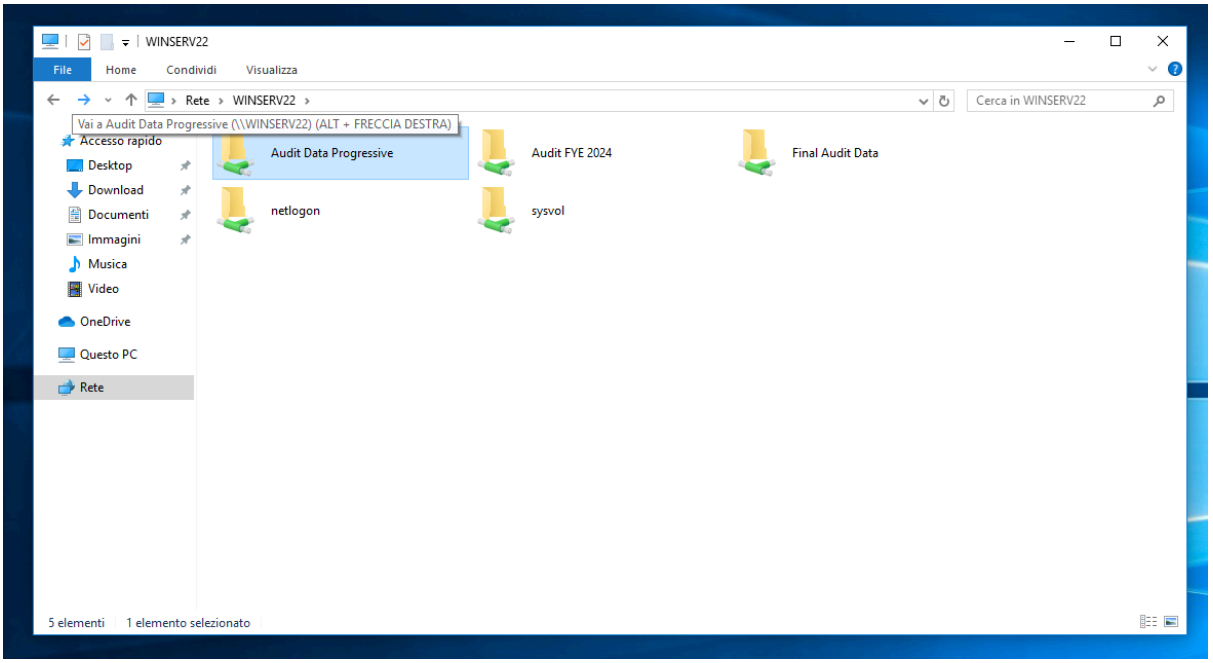
During the final phase of the project, the system was demonstrated to Fantozzi, the finance administrator. He was shown how he could:

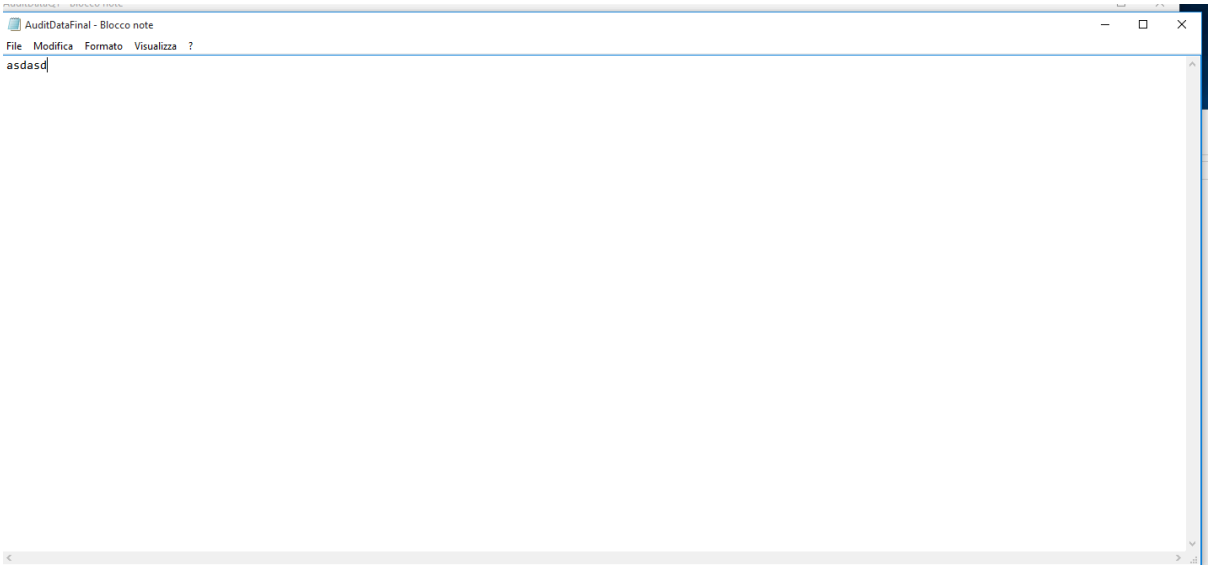
1. Navigate to the Audit Progressive and Final Audit Data folders.
2. Open, edit, and save documents in the Audit Progressive folder.
3. Review finalized data in the Final Audit Data folder, ensuring that all necessary adjustments were made before granting read-only access to auditors.

Fantozzi's ability to successfully perform these tasks validated the configurations. His feedback was positive, particularly regarding the seamless access to files and the added convenience of segregated permissions, which ensured security and minimized the risk of accidental data modification.




Altro utente
ThetaAudit\Fantozzi
Nuova password
Conferma password
Accedi a: ThetaAudit
Come accedo a un altro dominio?
Annulla


WINSERV22
File
Home
Condividi
Visualizza
Rete › WINSERV22 ›
Cerca in WINSERV22
Vai a Audit Data Progressive (\\WINSERV22) (ALT + FRECCIA DESTRA)
Accesso rapido
Desktop
Download
Documenti
Immagini
Musica
Video
OneDrive
Questo PC
Rete
Audit Data Progressive
Audit FYE 2024
Final Audit Data
netlogon
sysvol
5 elementi
1 elemento selezionato



6. Detailed Step-by-Step Process

The process of creating groups and assigning permissions within Windows Server 2022 was carried out in several well-defined phases, utilizing advanced server administration tools and Active Directory. Each phase was designed to ensure that user roles and responsibilities were clearly defined and securely managed throughout the system. Below is a detailed breakdown of each step involved:

Step 1: Active Directory and Organizational Unit Configuration

The first step was the configuration of the Active Directory (AD) environment, which is the backbone of user and resource management within Windows Server. Setting up Active Directory correctly is crucial for ensuring that all user and group configurations are structured, secure, and easily scalable.

- **Creating the Active Directory Forest**: The Active Directory forest serves as the foundational framework for managing organizational resources. In this project, an Active Directory forest was established on the Windows Server 2022 environment to organize and manage users, groups, and resources efficiently. The forest acts as a logical grouping of domains that share a common schema, global catalog, and directory partitions, allowing centralized management.

- **Configuring Organizational Units (OUs)**: Organizational Units are containers within Active Directory that allow administrators to group users, groups, and computers based on common attributes, such as department or role. Three OUs were created for this project:

    - **FinanceAdmin**: This OU was dedicated to high-level finance administrators who require full control over sensitive financial data and systems.
    - **FinanceUsers**: This OU was designated for general finance department members who need access to working documents but not full administrative rights.
    - **ExternalAuditors**: This OU was created to manage external auditors who need restricted access to finalized financial documents, without altering any data.

- The OUs were carefully structured to ensure clear distinctions between roles and responsibilities, reducing the risk of unauthorized access to sensitive information.

- **Assigning Users to OUs**: After the OUs were set up, users were assigned to their respective OUs based on their roles:
    - **Fantozzi** was assigned to the **FinanceAdmin** OU, as the primary finance administrator.
    - **Fantozzina** was placed in the **FinanceUsers** OU, where she would assist with document management and other finance-related tasks.
    - **Filini** was assigned to the **ExternalAuditors** OU, ensuring that only the necessary permissions were granted for external audit purposes.

Step 2: Group Creation

Once the OUs were created and users assigned, the next step was to define and create the specific user groups that would govern access to various resources within the server environment.

- **Creating Groups in Active Directory**: Groups are essential for managing permissions effectively within Windows Server. Instead of assigning permissions to individual users, groups allow administrators to manage access at a broader level, simplifying ongoing user management. The groups created for this project were:
    - **FinanceAdmin Group**: This group included Fantozzi and other senior finance administrators who required full control over financial documents.
    - **FinanceUsers Group**: This group included Fantozzina and other finance team members who needed access to working files, but with limited control.
    - **ExternalAuditors Group**: This group included Filini and other external auditors, granted only read access to finalized documents.
- The process to create these groups involved navigating to **Active Directory Users and Computers** on the Windows Server 2022 interface:
    - Right-clicking on the relevant Organizational Unit (e.g., FinanceAdmin), selecting **New Group**, and providing a meaningful name for each group.
    - Each group was then populated with users who needed specific access rights based on their roles.
- **Setting Group Scopes and Types**: When creating the groups, it was also essential to determine the group scope and type. In this case, all groups were created as **Global** and **Security** groups:
    - **Global Groups**: These groups contain users from a single domain and are typically used to grant access permissions to resources across the network.
    - **Security Groups**: Security groups are used to assign permissions to resources, such as files, folders, and applications. Each of the three groups (FinanceAdmin, FinanceUsers, and ExternalAuditors) was created as a security group to define access rights on critical documents and systems.

Step 3: Folder Creation and Permission Assignment

With the groups created, the next step was to set up the necessary folder structure and assign permissions. A key part of the project was ensuring that the right people had the right access to the right data while maintaining strict security protocols.

- **Creating Folders on the Server**: Two main directories were created on the server:
    - **Audit Progressive Folder**: This folder contained the files that were continuously being worked on for the fiscal year review (e.g., quarterly reports). Since this data was still being reviewed, it required ongoing access from the finance team.
    - **Final Audit Data Folder**: This folder contained the finalized fiscal year-end data, which needed to be locked down to prevent modifications. Only the necessary parties had access to this folder.

- **Configuring Permissions Using the Security Tab**: Permissions were assigned to these folders using the **Security** tab in the folder properties dialog box. Each group was granted the appropriate permissions for each folder:
    - **FinanceAdmin Group**: Full control permissions on both folders, including the ability to read, write, and modify files.
    - **FinanceUsers Group**: Read and write access to the Audit Progressive Folder to allow collaboration, but read-only access to the Final Audit Data Folder to prevent any accidental modifications.
    - **ExternalAuditors Group**: Read-only access to the Final Audit Data Folder, ensuring that auditors could review the finalized documents without making changes.
- By leveraging the **NTFS (New Technology File System)** permissions, access was managed at a granular level, ensuring the highest level of security for sensitive financial data.

Step 4: Configuring Remote Desktop Control

To enable external auditors, such as Filini, to work remotely, a critical part of the configuration was enabling **Remote Desktop** access. This allowed Filini to access the Final Audit Data Folder from an external location without needing to be physically present in the office, which enhanced flexibility and supported modern remote work practices.

- **Enabling Remote Desktop Services**: The Remote Desktop feature was activated on the server to allow external users to securely log in and access specific resources. This involved ensuring that the **Remote Desktop Services** were enabled in the system settings and that all necessary ports were open on the server's firewall to facilitate remote connections.
- **Adding Filini to the Remote Desktop Users Group**: Filini's user account was added to the **Remote Desktop Users** group, which grants the necessary permissions to log into the server remotely. This configuration was tested to ensure that Filini could securely connect to the server and access the Final Audit Data Folder without being able to modify the documents.
- **Testing Remote Connectivity**: Once the configuration was complete, thorough testing was conducted to confirm that Filini could access the server and the required folder remotely. This involved ensuring that the Remote Desktop session was properly authenticated and that only read-only access was granted for the necessary files.

Step 5: Verification

To ensure that all configurations were properly implemented, the final step involved verification through a series of tests. These tests were designed to confirm that each group had the correct permissions and could perform the necessary tasks as intended.

- **Testing Permissions**: Test users were created for each group (FinanceAdmin, FinanceUsers, ExternalAuditors) to validate that the permissions were set correctly:

    - **FinanceAdmin Test Users**: Successfully modified files in both the Audit Progressive Folder and the Final Audit Data Folder.
    - **FinanceUsers Test Users**: Were able to access and edit files in the Audit Progressive Folder but could only view the files in the Final Audit Data Folder.
    - **ExternalAuditors Test Users**: Verified that they could access the Final Audit Data Folder remotely and had read-only permissions, ensuring that no modifications could be made.

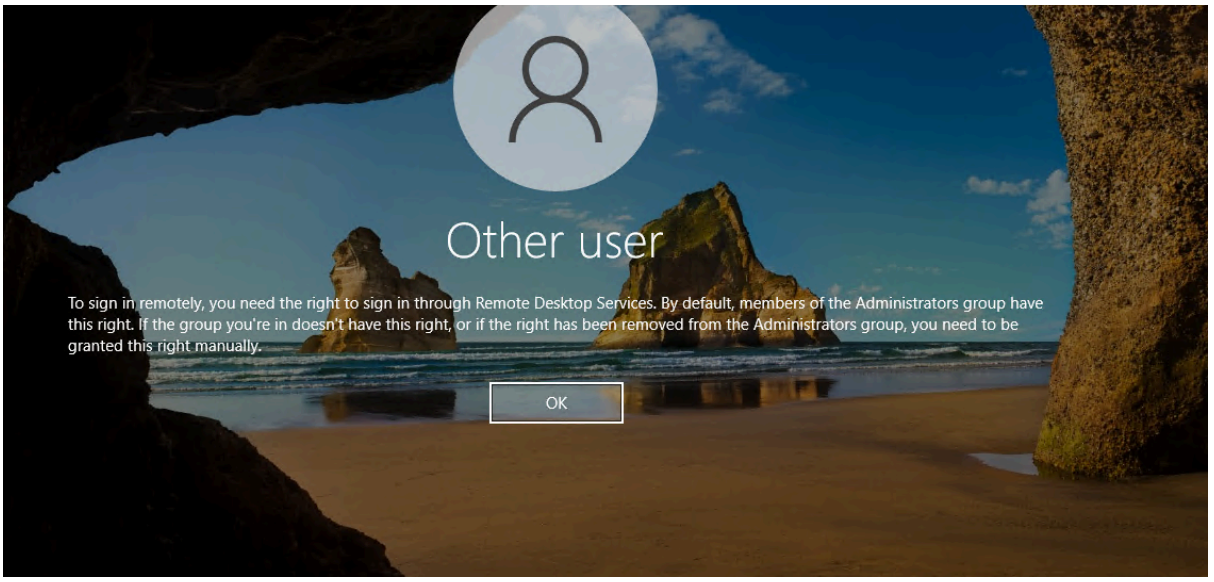
- **Final Testing:** After completing the test scenarios, the system was reviewed by Fantozzi, the finance administrator, who performed a series of tasks to ensure that the system met expectations. This final step helped confirm the integrity of the permissions and the smooth functioning of the Remote Desktop configuration for external auditors.

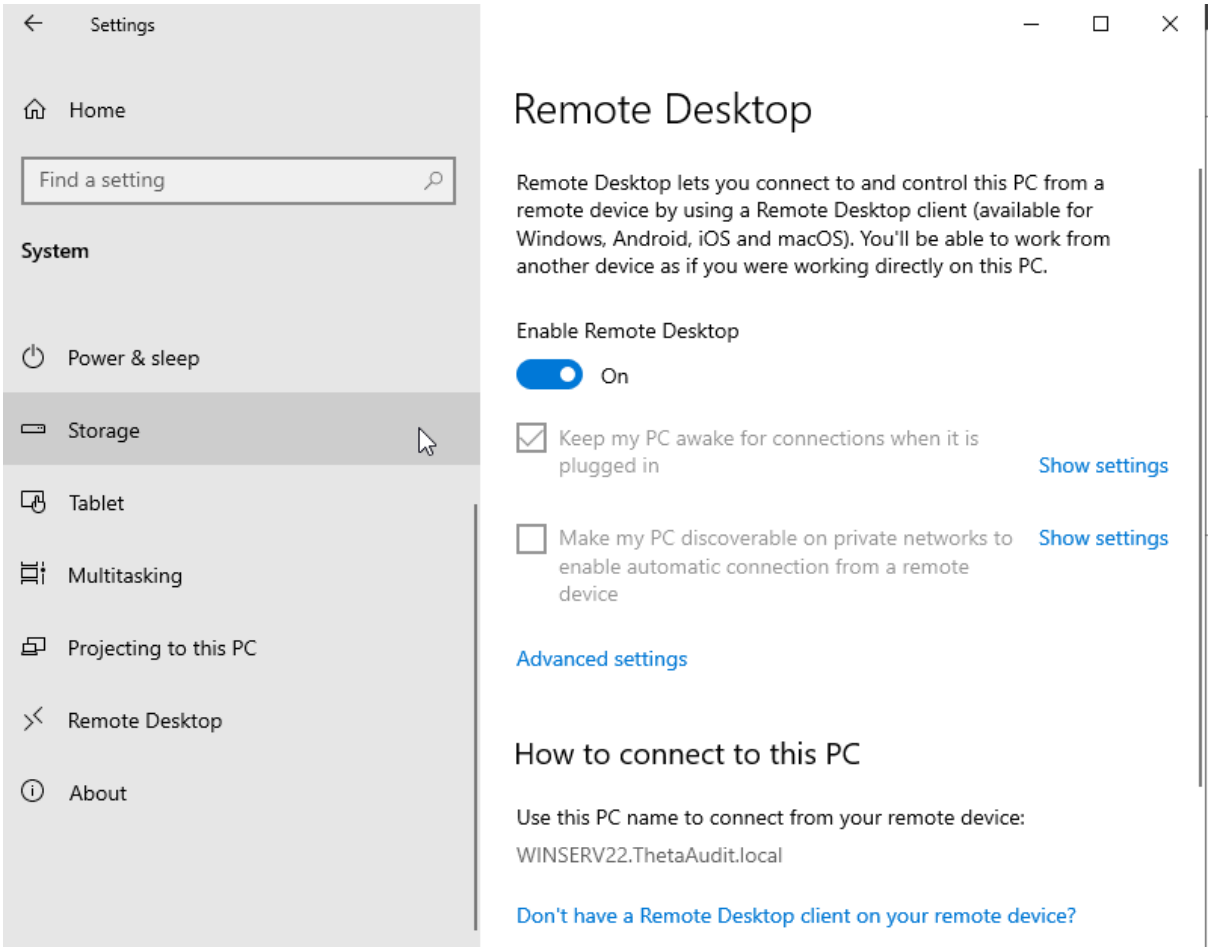
Challenges and Solutions

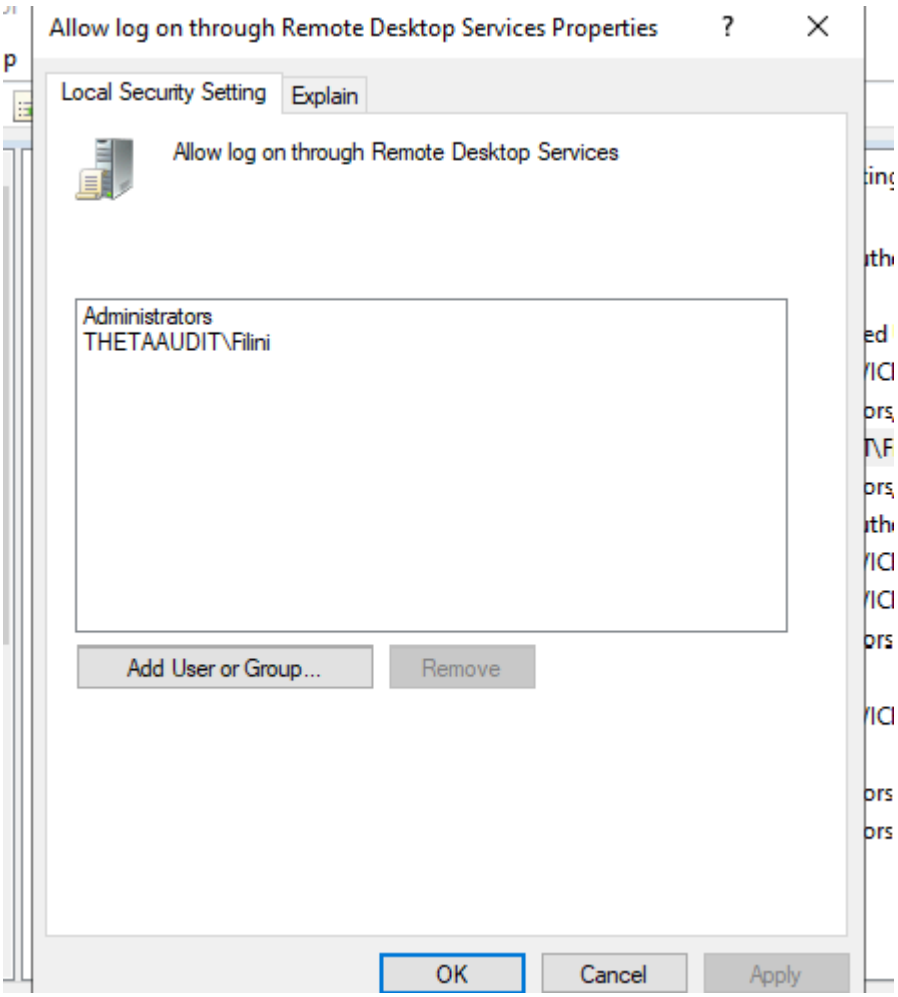
During the project, a few challenges were encountered:

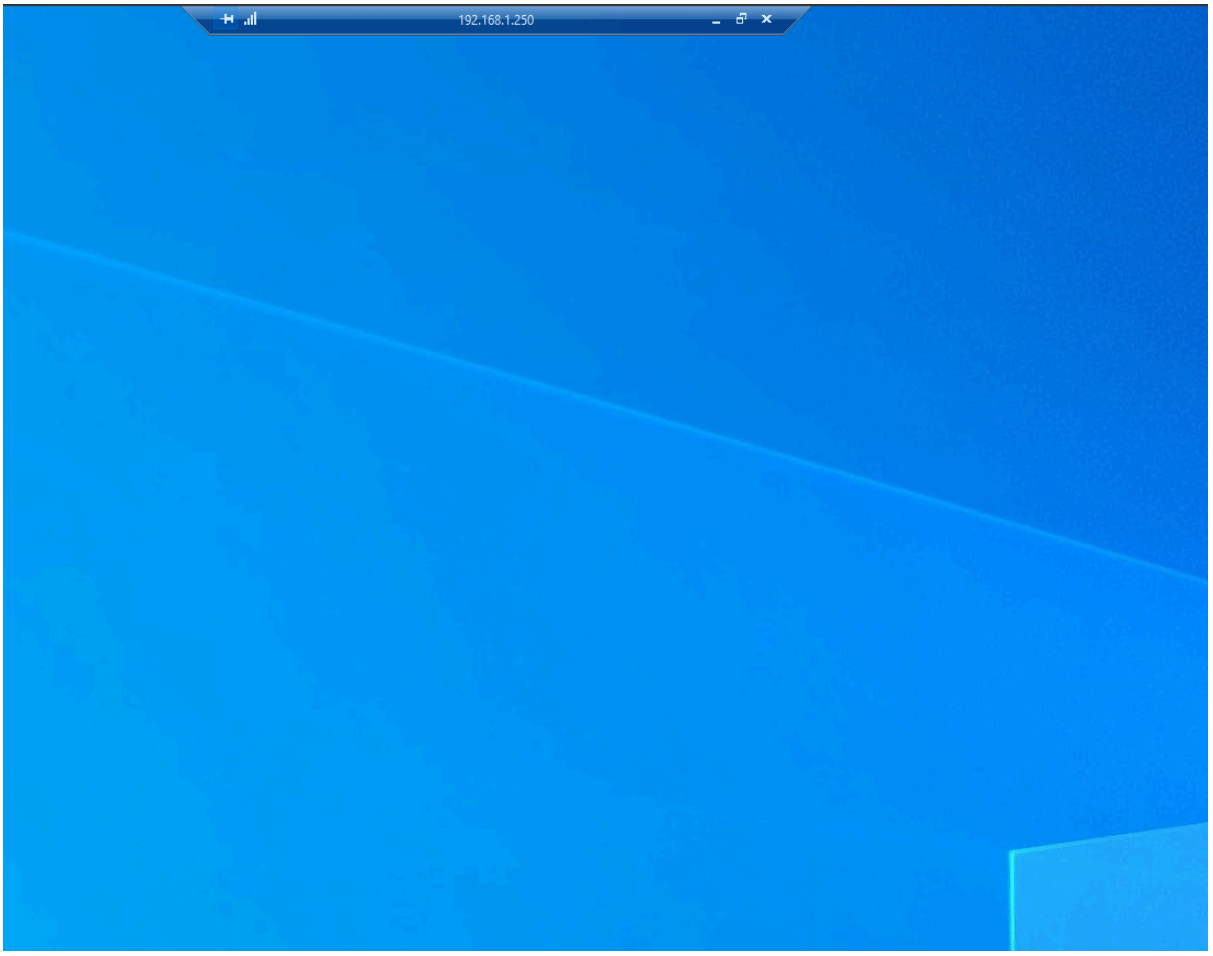
1. **Conflict Between Permissions:** Initial configurations inadvertently allowed ExternalAuditors to modify files in the Final Audit Data folder. This was resolved by revisiting the Security tab and explicitly setting the group's access level to "Read-only."

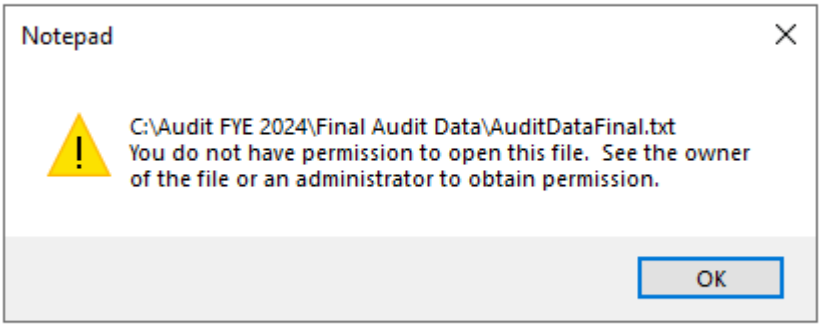
2. **Remote Desktop Configuration:** Initially, Filini experienced connectivity issues when attempting to access the server remotely. Troubleshooting revealed that the Remote Desktop Services were only partially enabled, and only Administrators were enabled access even though it was correctly configured through the Active Directory library. A quick correction of the system settings fixed the issue and Filini was able to log-in and also confirming that there was no option to modify the Audit Final Data file.


Other user
To sign in remotely, you need the right to sign in through Remote Desktop Services. By default, members of the Administrators group have this right. If the group you're in doesn't have this right, or if the right has been removed from the Administrators group, you need to be granted this right manually.
OK


Settings
Home
Find a setting
System
Power & sleep
Storage
Tablet
Multitasking
Projecting to this PC
Remote Desktop
About
Remote Desktop
Remote Desktop lets you connect to and control this PC from a remote device by using a Remote Desktop client (available for Windows, Android, iOS and macOS). You'll be able to work from another device as if you were working directly on this PC.
Enable Remote Desktop
On
Keep my PC awake for connections when it is plugged in
Show settings
Make my PC discoverable on private networks to enable automatic connection from a remote device
Show settings
Advanced settings
How to connect to this PC
Use this PC name to connect from your remote device:
WINSERV22.ThetaAudit.local
Don't have a Remote Desktop client on your remote device?


Allow log on through Remote Desktop Services Properties
Local Security Setting
Explain
Allow log on through Remote Desktop Services
Administrators
THETAAUDIT\Filini
Add User or Group...
Remove
OK
Cancel
Apply





3. **User Role Clarity:** Differentiating between FinanceUsers and FinanceAdmin roles required a clear understanding of their functional boundaries. Additional documentation was created to ensure proper alignment of responsibilities.

Observations and Best Practices

This project emphasized the importance of structured group management in maintaining organizational security. Key observations included:

- **Role-based access control:** Assigning permissions based on roles streamlined the process and reduced the likelihood of unauthorized access.
- **Documentation:** Maintaining a detailed record of permissions and their rationale aided in troubleshooting and future audits.
- **Testing:** Verifying configurations with test users ensured that permissions aligned with expectations.
- **Remote Access Configuration:** Enabling Remote Desktop access for specific users enhanced flexibility without compromising security.

Conclusion

The project successfully demonstrated the creation and management of user groups in Windows Server 2022 for Theta. By following a systematic approach, the setup ensured that each group's permissions were tailored to their roles while maintaining security and efficiency. The addition of Remote Desktop access for auditors further enhanced the system's flexibility, aligning with modern remote work practices.

This initiative provided valuable insights into managing organizational resources, underscoring the need for clarity, precision, and rigorous testing in system administration. The implemented system stands as a robust solution to Theta's specific requirements for secure and efficient fiscal review processes.