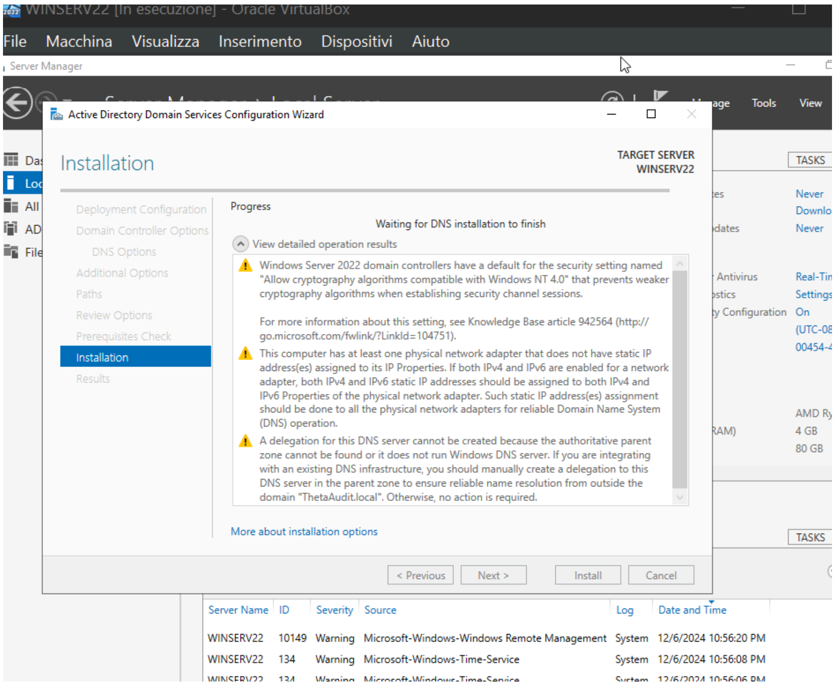
Introduction

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.



Progress

Waiting for DNS installation to finish

View detailed operation results

⚠ Windows Server 2022 domain controllers have a default for the security setting named "Allow cryptography algorithms compatible with Windows NT 4.0" that prevents weaker cryptography algorithms when establishing security channel sessions.

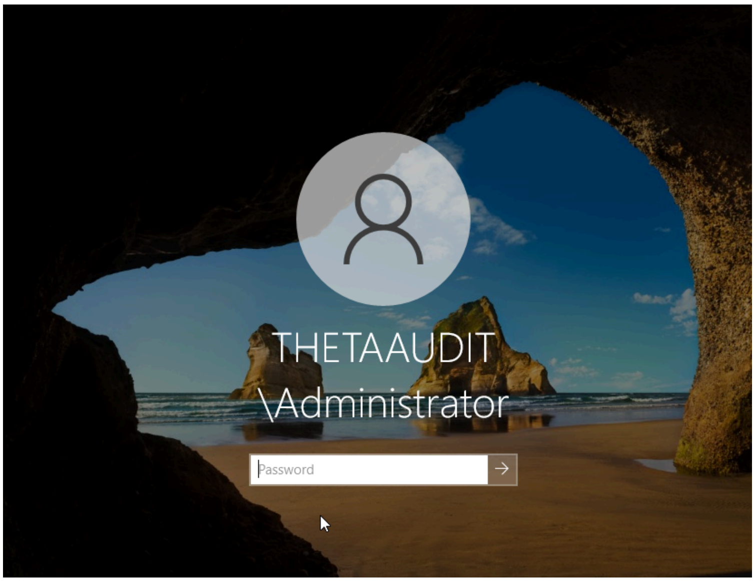
For more information about this setting, see Knowledge Base article 942564 (http://go.microsoft.com/fwlink/?LinkId=104751).

⚠ This computer has at least one physical network adapter that does not have static IP address(es) assigned to its IP Properties. If both IPv4 and IPv6 are enabled for a network adapter, both IPv4 and IPv6 static IP addresses should be assigned to both IPv4 and IPv6 Properties of the physical network adapter. Such static IP address(es) assignment should be done to all the physical network adapters for reliable Domain Name System (DNS) operation.

⚠ A delegation for this DNS server cannot be created because the authoritative parent zone cannot be found or it does not run Windows DNS server. If you are integrating with an existing DNS infrastructure, you should manually create a delegation to this DNS server in the parent zone to ensure reliable name resolution from outside the domain "ThetaAudit.local". Otherwise, no action is required.

More about installation options

Server Name	ID	Severity	Source	Log	Date and Time
WINSERV22	10149	Warning	Microsoft-Windows-Windows Remote Management	System	12/6/2024 10:56:20 PM
WINSERV22	134	Warning	Microsoft-Windows-Time-Service	System	12/6/2024 10:56:08 PM
WINSERV22	134	Warning	Microsoft-Windows-Time-Service	System	12/6/2024 10:56:06 PM



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.

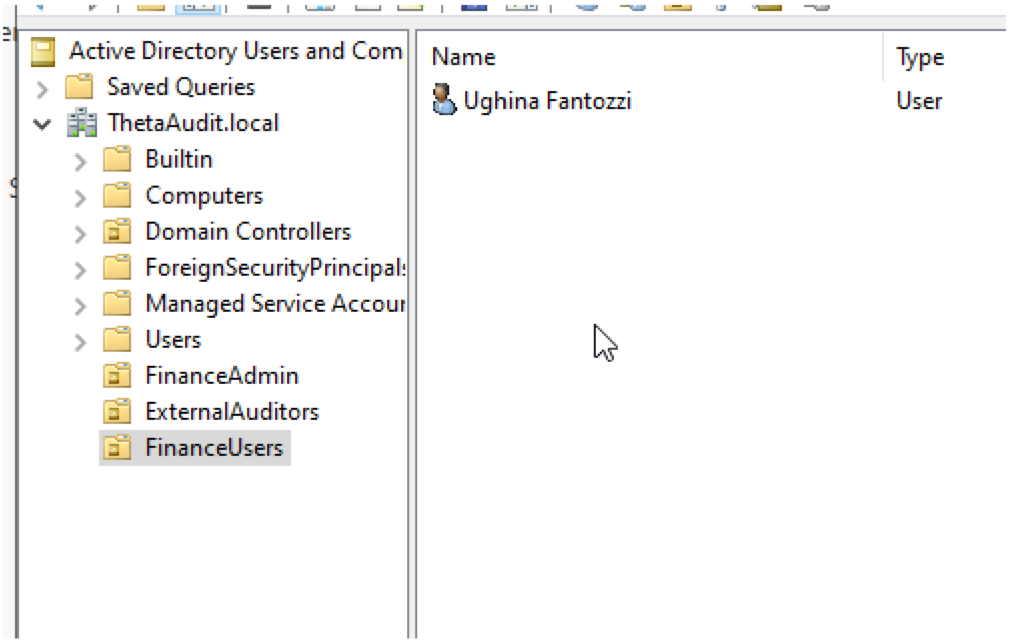
FinanceUsers

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.

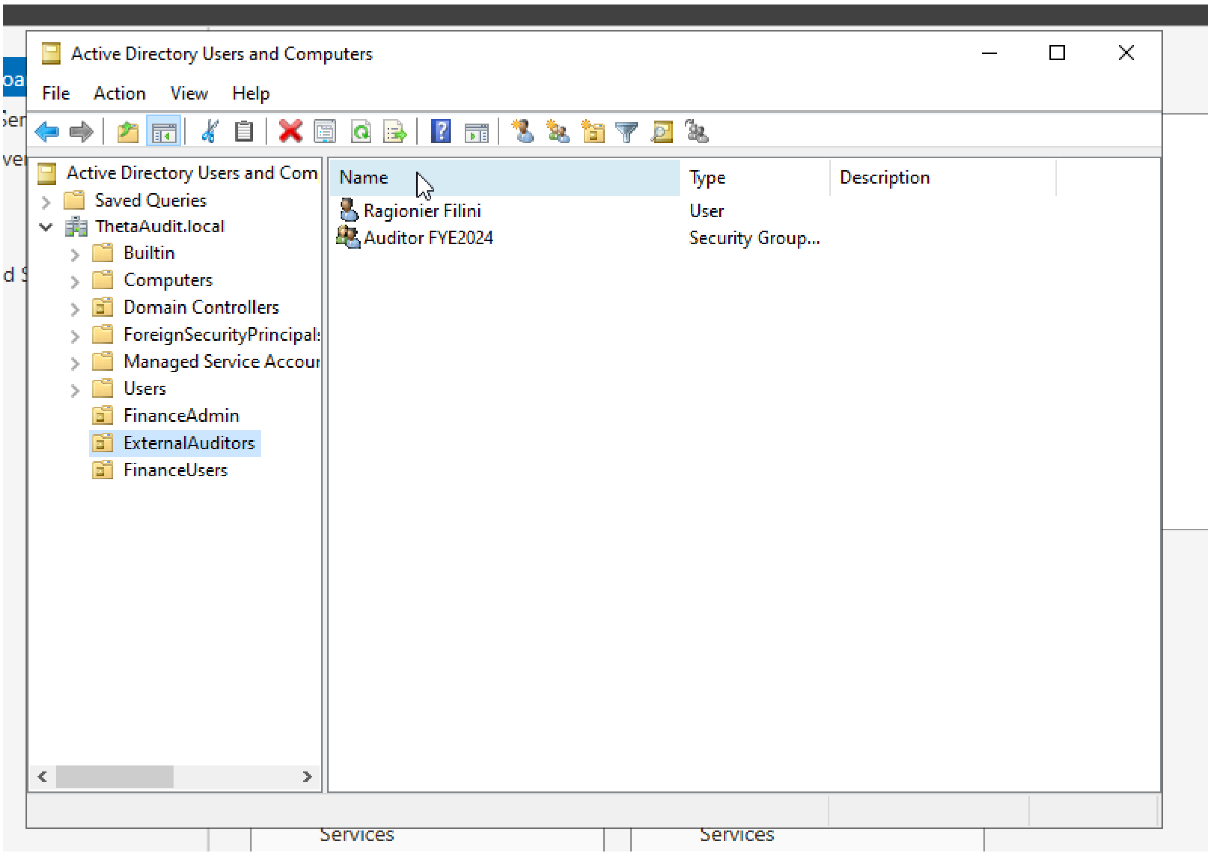
ExternalAuditors

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.

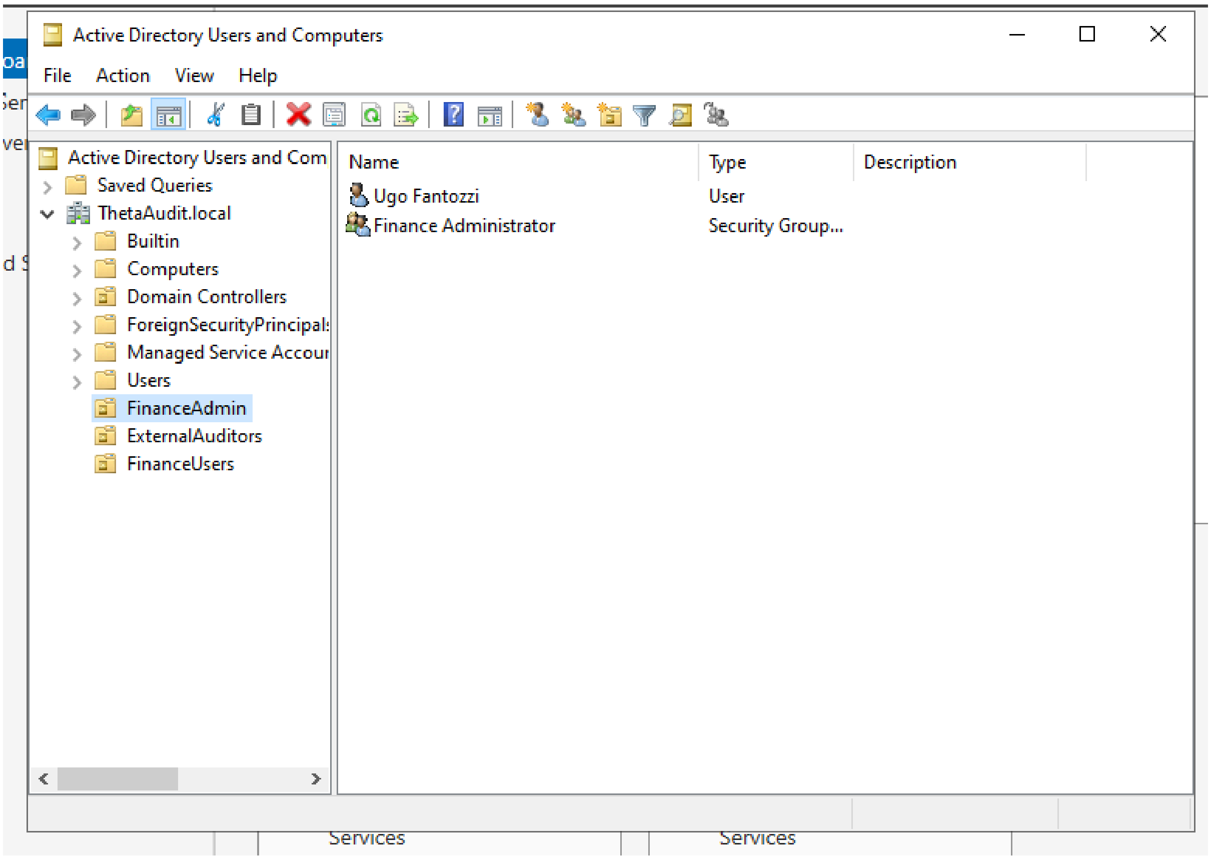
Additionally, remote desktop control was configured for the ExternalAuditors group, allowing Filini to perform the audit from home without needing to be physically present in the office. This was implemented to enhance flexibility and accommodate modern work practices.



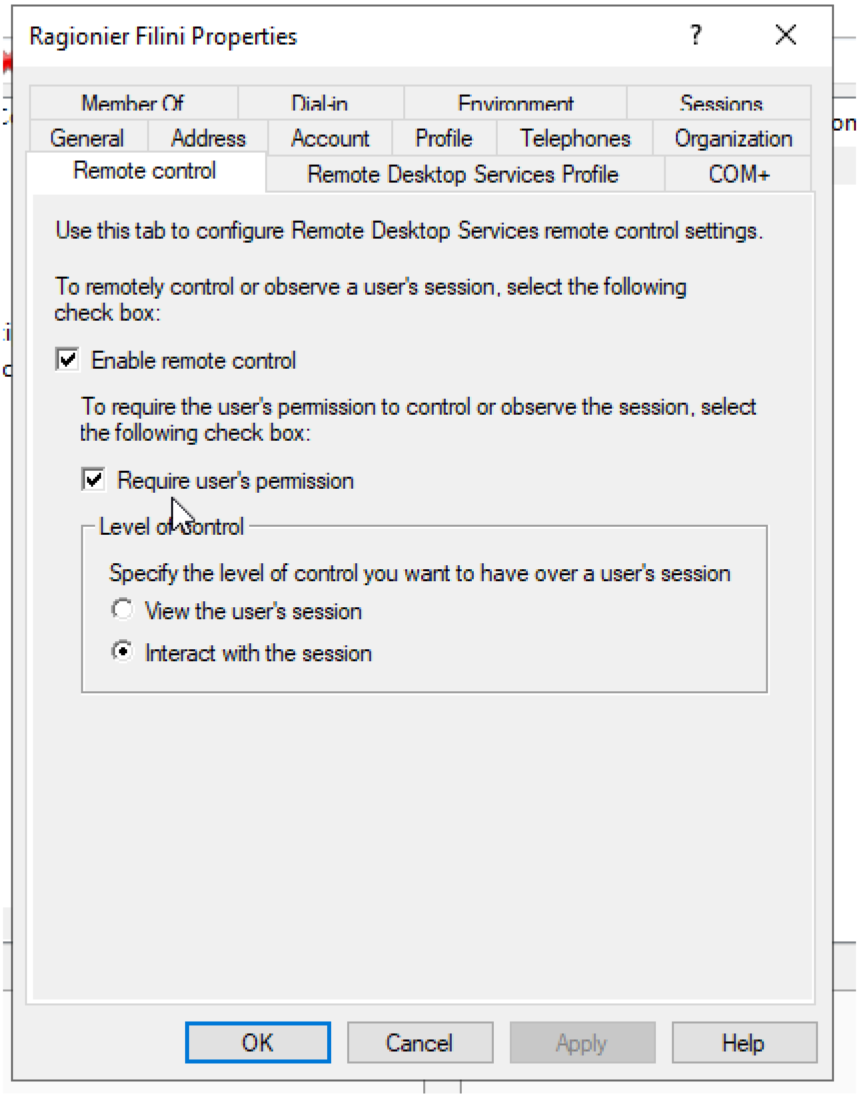
Name	Type
Ughina Fantozzi	User



Name	Type	Description
Ragionier Filini	User	
Auditor FYE2024	Security Group...	



Name	Type	Description
Ugo Fantozzi	User	
Finance Administrator	Security Group...	



Use this tab to configure Remote Desktop Services remote control settings.

To remotely control or observe a user's session, select the following check box:

☑ Enable remote control

To require the user's permission to control or observe the session, select the following check box:

☑ Require user's permission

Level of control

Specify the level of control you want to have over a user's session

○ View the user's session

● Interact with the session

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

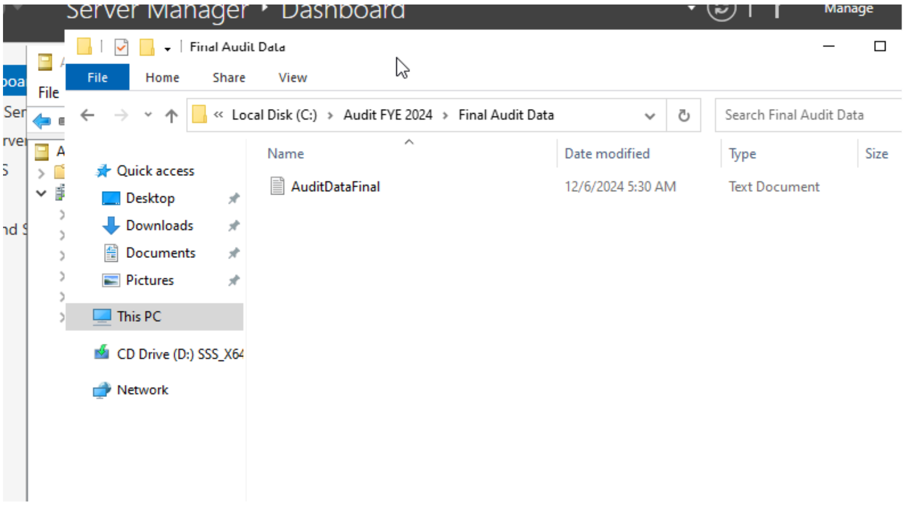
This directory housed sequential review files (e.g., Q1, Q2, Q3, and Q4 reports). The following permissions were assigned:

- **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

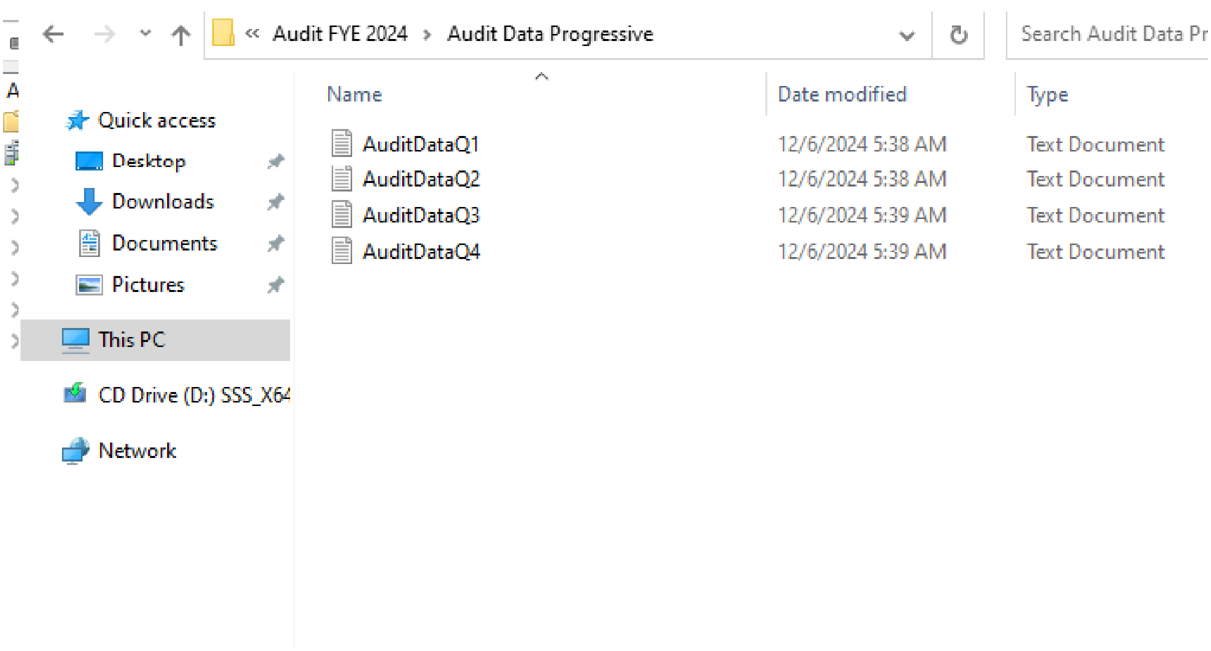
This directory contained the finalized fiscal year-end data. Permissions were as follows:

- **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.



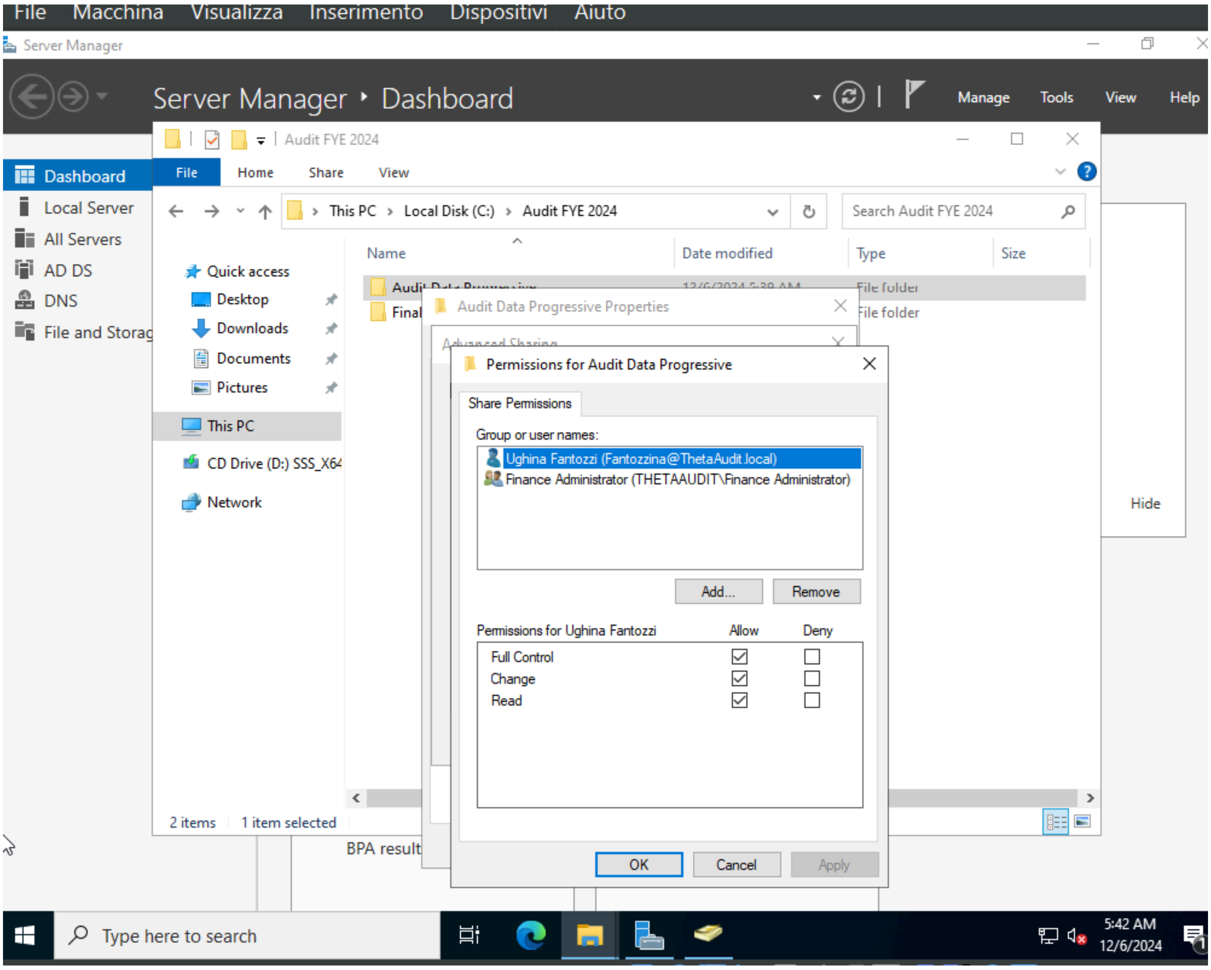
« Local Disk (C:) › Audit FYE 2024 › Final Audit Data

Name	Date modified	Type	Size
AuditDataFinal	12/6/2024 5:30 AM	Text Document	



« Audit FYE 2024 › Audit Data Progressive

Name	Date modified	Type
AuditDataQ1	12/6/2024 5:38 AM	Text Document
AuditDataQ2	12/6/2024 5:38 AM	Text Document
AuditDataQ3	12/6/2024 5:39 AM	Text Document
AuditDataQ4	12/6/2024 5:39 AM	Text Document



Permissions for Audit Data Progressive

Share Permissions

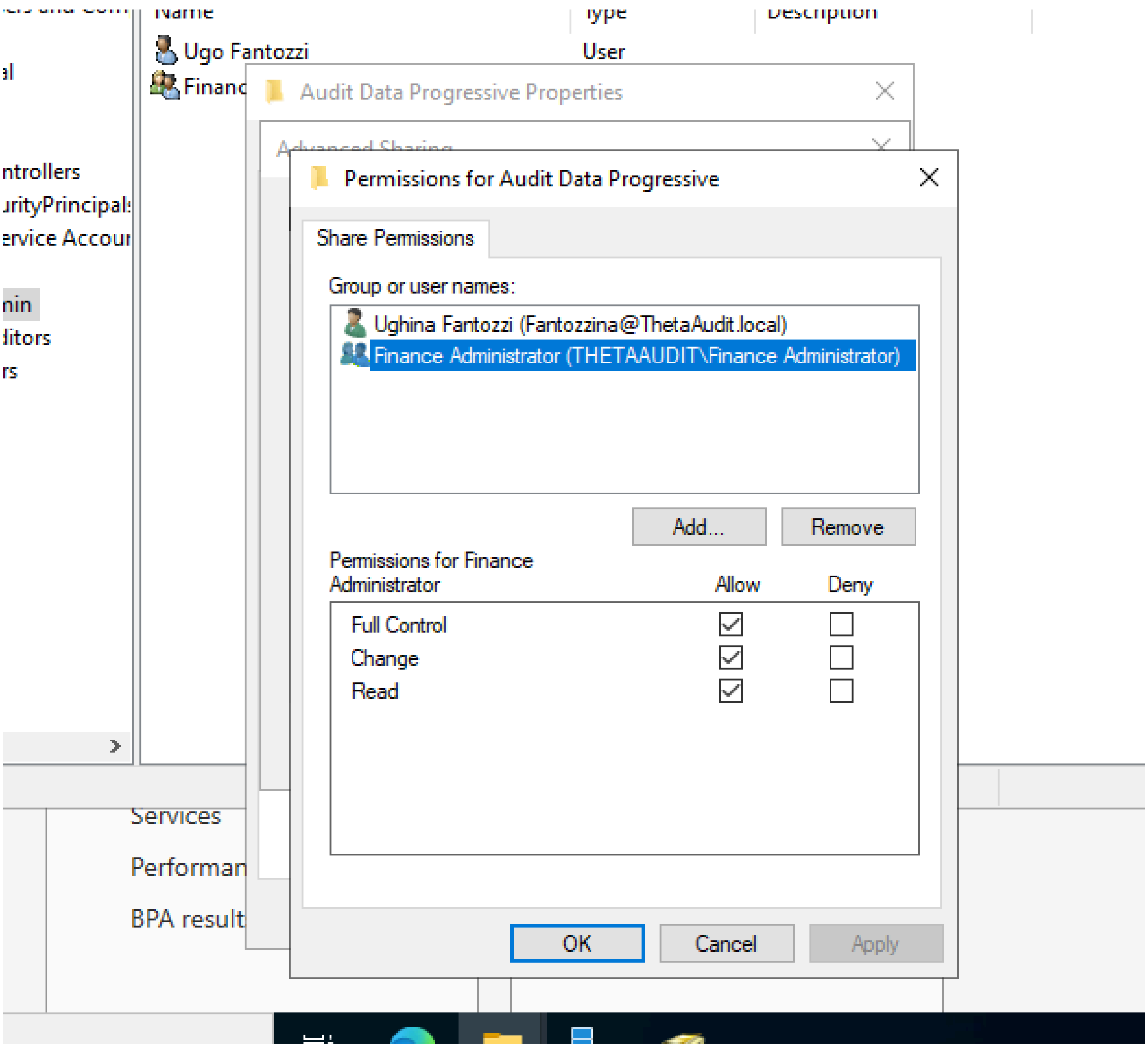
Group or user names:

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



Permissions for Audit Data Progressive

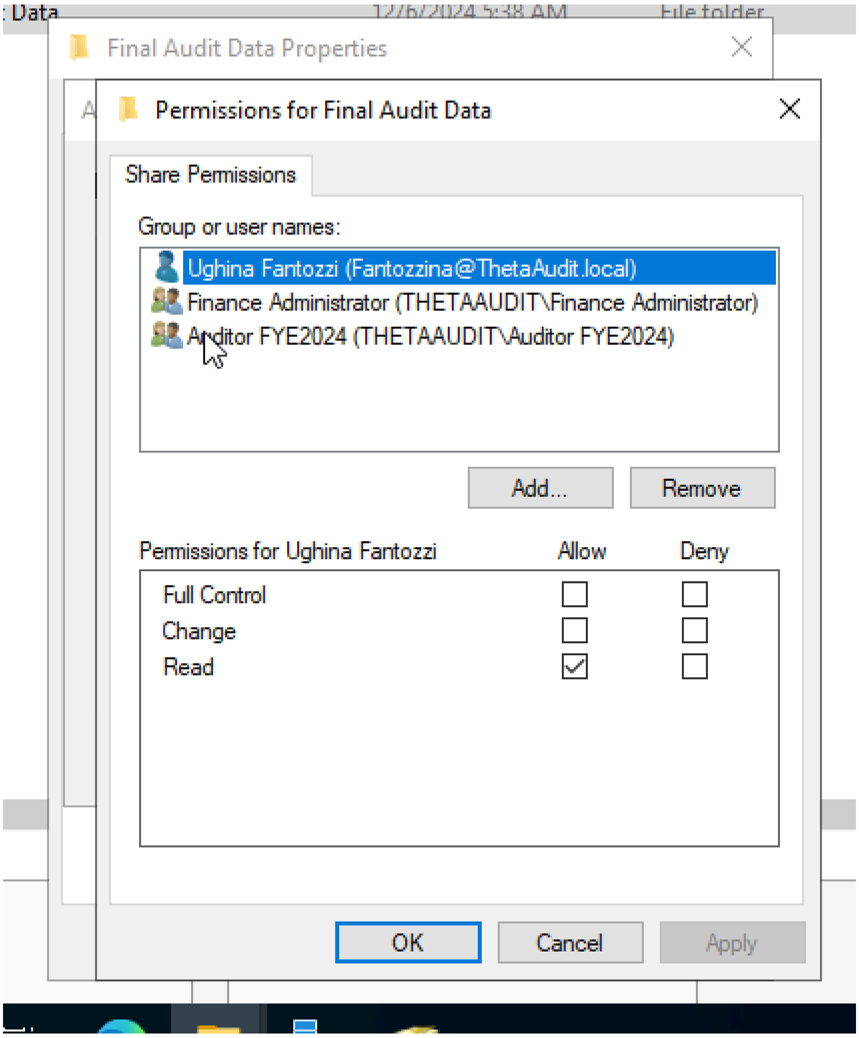
Share Permissions

Group or user names:

- Ughina Fantozzi (Fantozzina@ThetaAudit.local)
- Finance Administrator (THETAAUDIT\Finance Administrator)

Permissions for Finance Administrator

	Allow	Deny
Full Control	☑	□
Change	☑	□
Read	☑	□



: Data 12/6/2024 5:38 AM File folder

Final Audit Data Properties

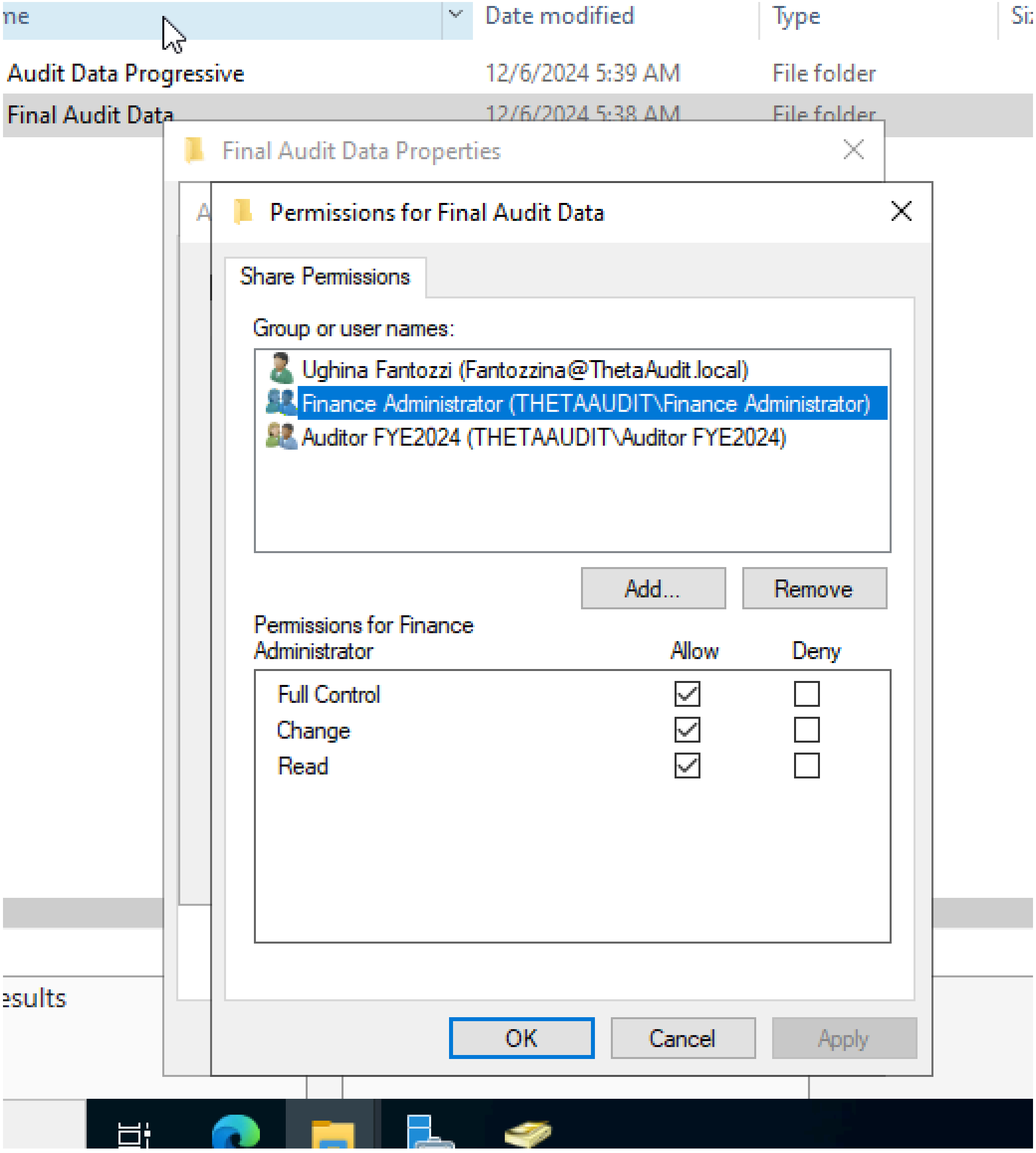
Permissions for Final Audit Data

Share Permissions

Group or user names:

- Ughina Fantozzi (Fantozzina@ThetaAudit.local)
- Finance Administrator (THETAAUDIT\Finance Administrator)
- Auditor FYE2024 (THETAAUDIT\Auditor FYE2024)

Permissions for Ughina Fantozzi	Allow	Deny
Full Control	□	□
Change	□	□
Read	☑	□



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

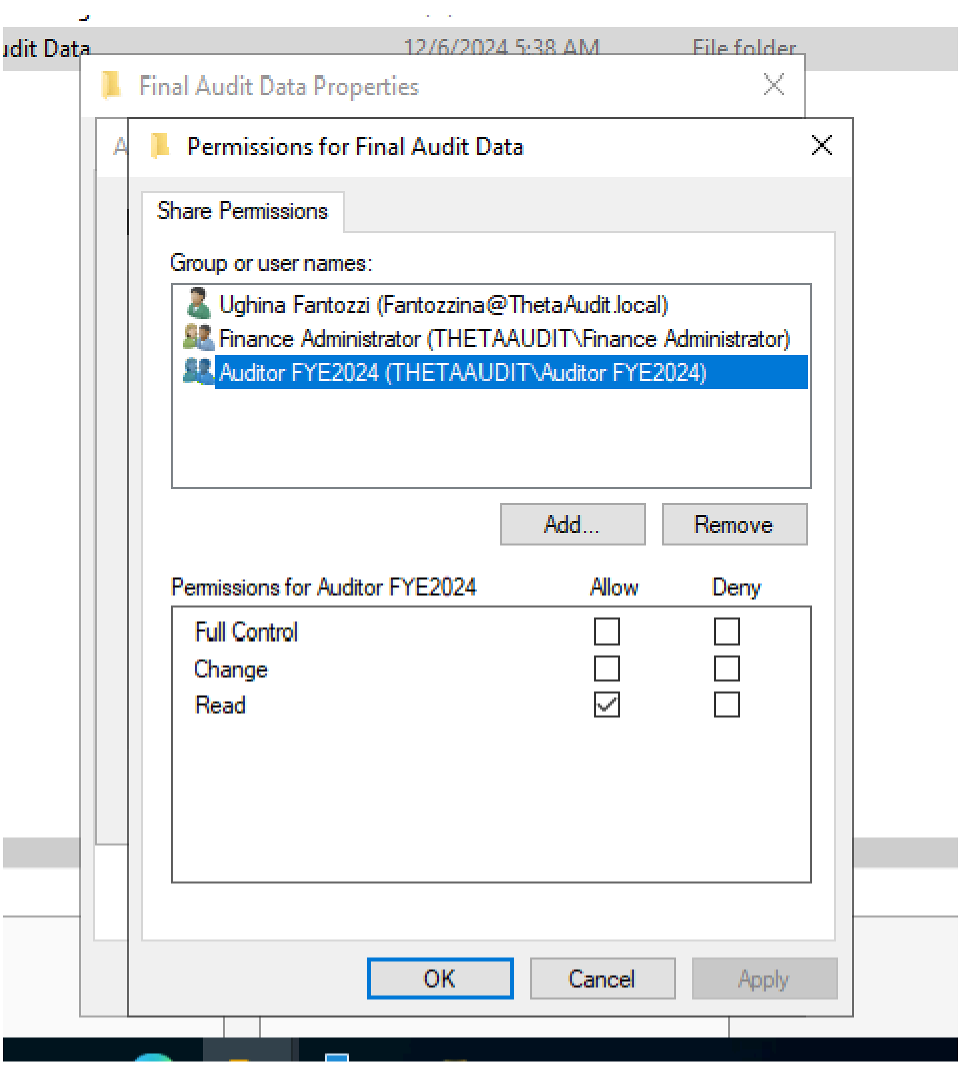
Permissions for Final Audit Data

Share Permissions

Group or user names:

- Ughina Fantozzi (Fantozzina@ThetaAudit.local)
- Finance Administrator (THETAAUDIT\Finance Administrator)
- Auditor FYE2024 (THETAAUDIT\Auditor FYE2024)

Permissions for Finance Administrator	Allow	Deny
Full Control	☑	□
Change	☑	□
Read	☑	□



udit Data 12/6/2024 5:38 AM File folder

Permissions for Final Audit Data

Group or user names:

- Ughina Fantozzi (Fantozzina@ThetaAudit.local)
- Finance Administrator (THETAAUDIT\Finance Administrator)
- Auditor FYE2024 (THETAAUDIT\Auditor FYE2024)

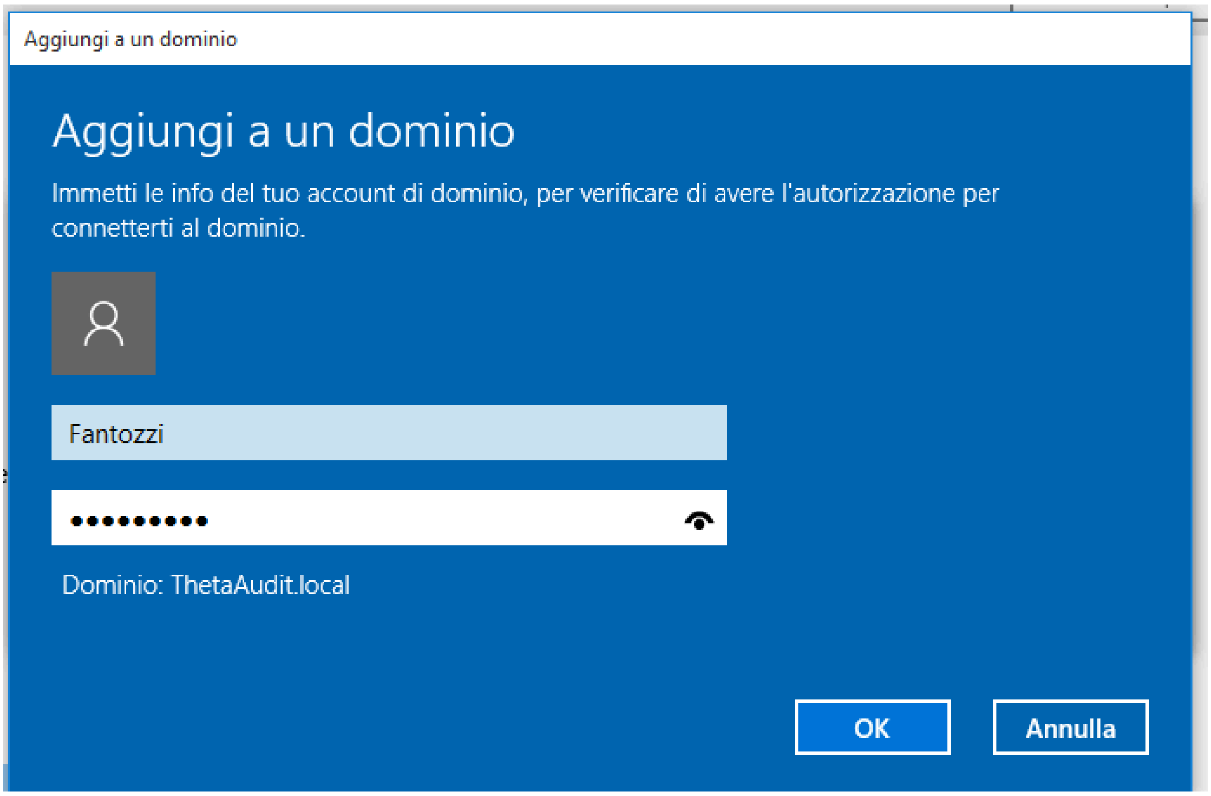
Permissions for Auditor FYE2024	Allow	Deny
Full Control	☐	☐
Change	☐	☐
Read	☑	☐

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.



Aggiungi a un dominio

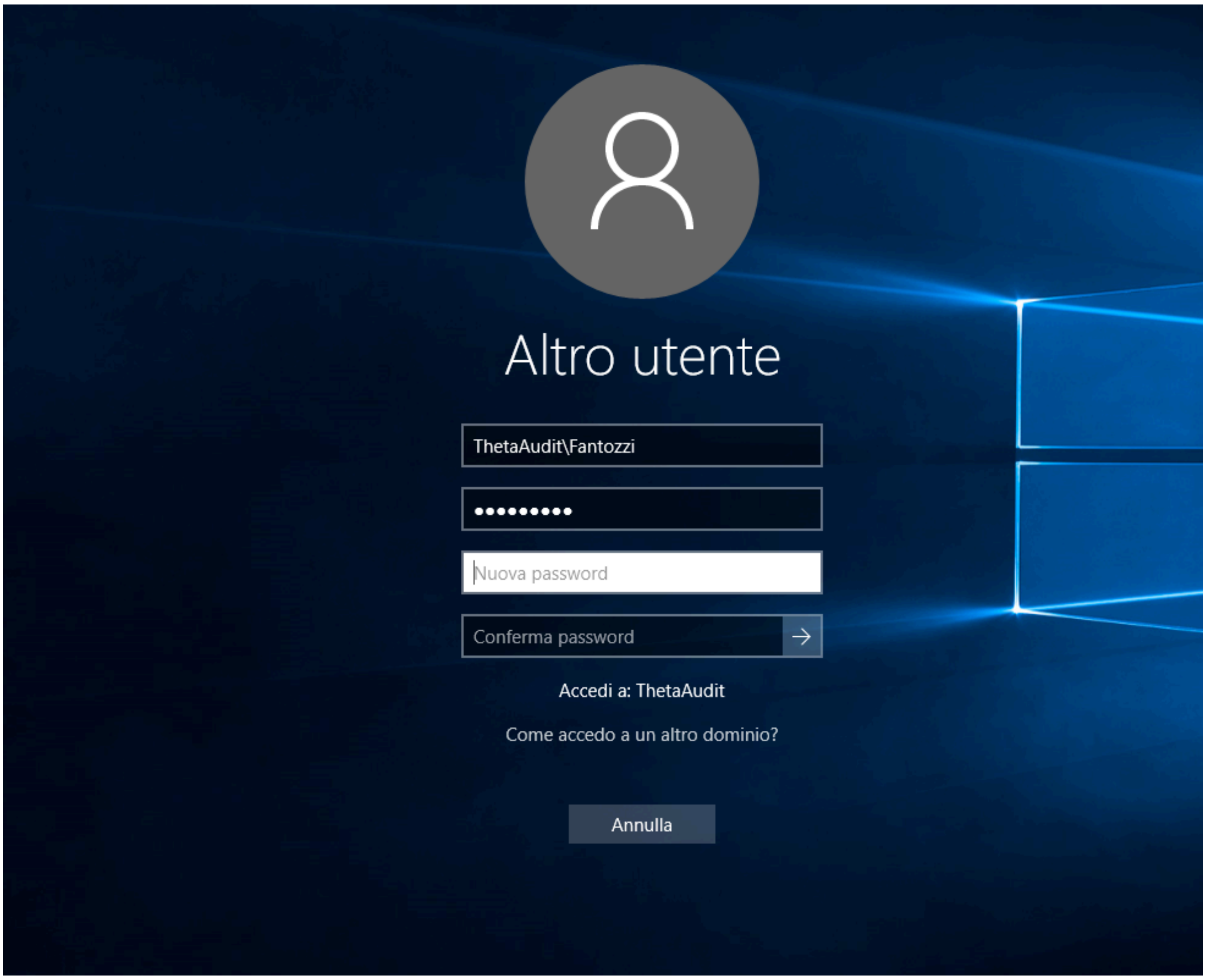
Aggiungi a un dominio

Immetti le info del tuo account di dominio, per verificare di avere l'autorizzazione per connetterti al dominio.

Fantozzi

••••••••••

Dominio: ThetaAudit.local



Altro utente

ThetaAudit\Fantozzi

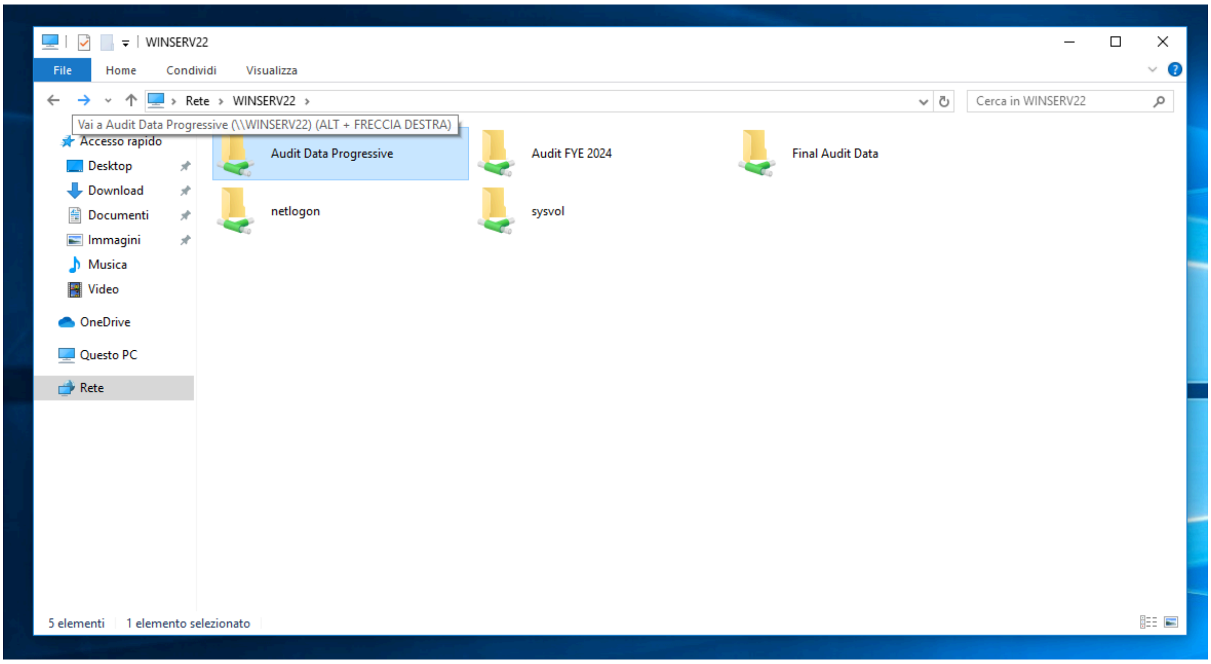
●●●●●●●●●

Nuova password

Conferma password

Accedi a: ThetaAudit

Come accedo a un altro dominio?



Vai a Audit Data Progressive (\\WINSERV22) (ALT + FRECCIA DESTRA)

Audit Data Progressive

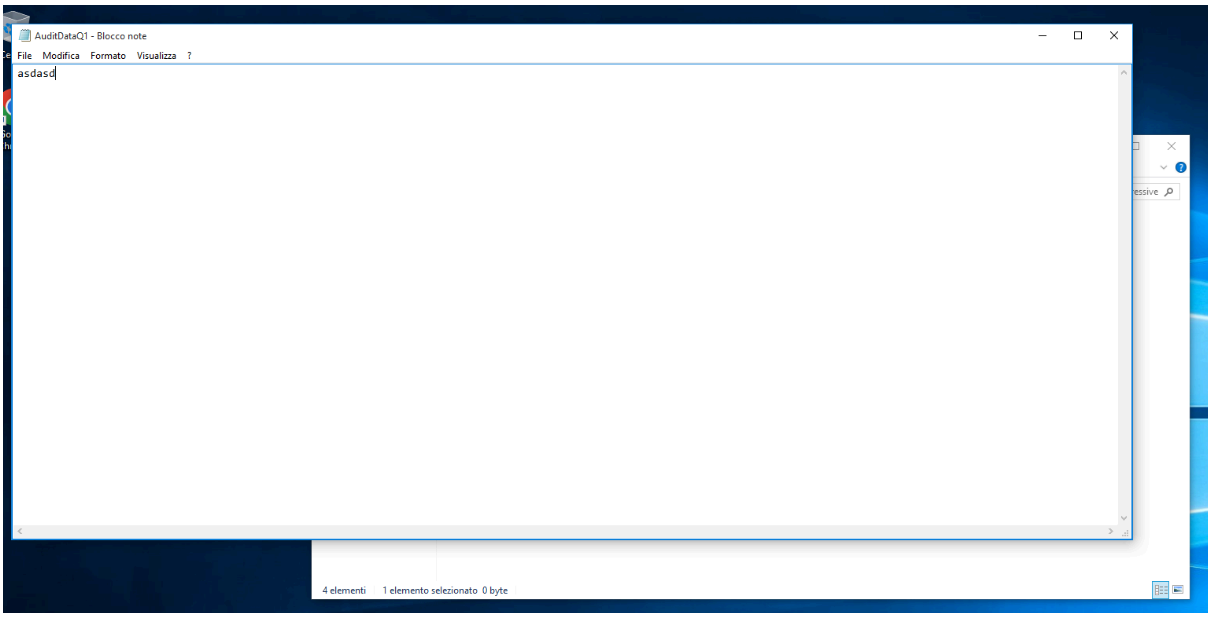
Audit FYE 2024

Final Audit Data

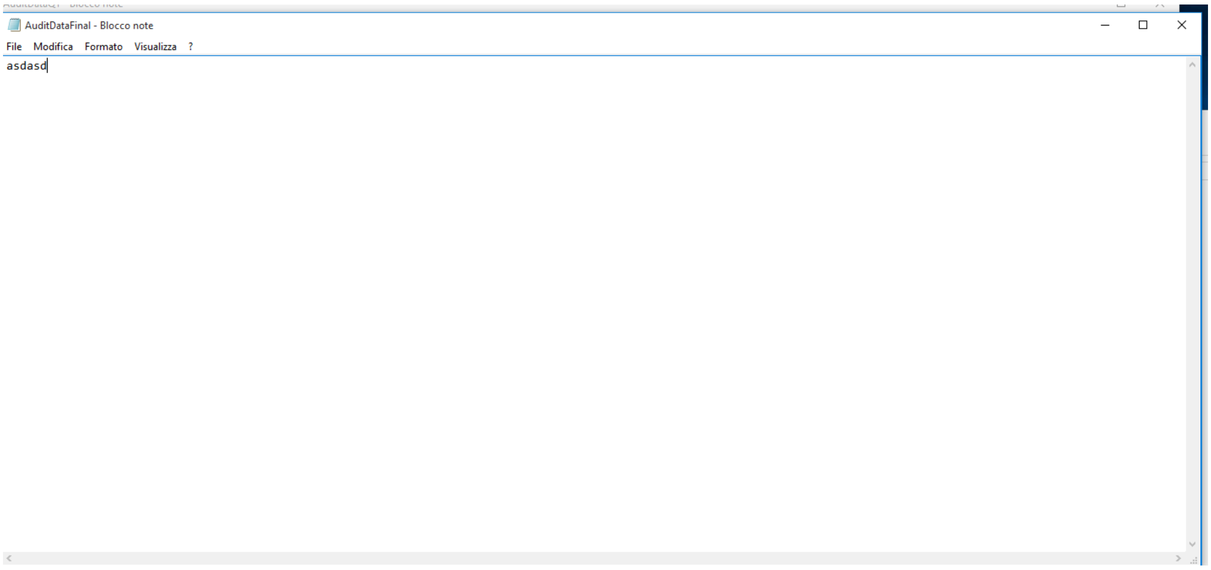
netlogon

sysvol

5 elementi 1 elemento selezionato


AuditDataQ1 - Blocco note
File Modifica Formato Visualizza ?
4 elementi
1 elemento selezionato 0 byte

asdasd


AuditDataFinal - Blocco note
File Modifica Formato Visualizza ?

asdasd

Step-by-Step Process

The process for creating groups and assigning permissions was systematic and involved the following steps:

Step 1: Active Directory and Organizational Unit Configuration

Using the Windows Server interface, an Active Directory forest was created, and three Organizational Units were defined for FinanceAdmin, FinanceUsers, and ExternalAuditors.

This structure helped segregate users based on their roles and ensured clarity during group and permission assignment.

Step 2: Group Creation

Groups were created within their respective contexts:

- Navigated to Active Directory Users and Computers.
- Right-clicked on the appropriate Organizational Unit (e.g., FinanceAdmin) and selected **New Group**.
- Assigned meaningful names and added the appropriate users to each group.

Step 3: Folder Creation and Permission Assignment

Folders were created directly on the server, and permissions were configured via the Security tab in folder properties:

- Added each group to the folder's permissions list.
- Configured access levels (read, write, modify) for each group based on their functional requirements.

Step 4: Configuring Remote Desktop Control

To enable remote auditing, Remote Desktop was configured for the ExternalAuditors group. This setup involved:

- Enabling Remote Desktop services on the server.
- Adding Filini's user account to the Remote Desktop Users group.
- Testing connectivity to ensure that Filini could securely log in and access the Final Audit Data folder from an external location.

Step 5: Verification

The configuration was verified by creating test users for each group and attempting actions based on the assigned permissions. For example:

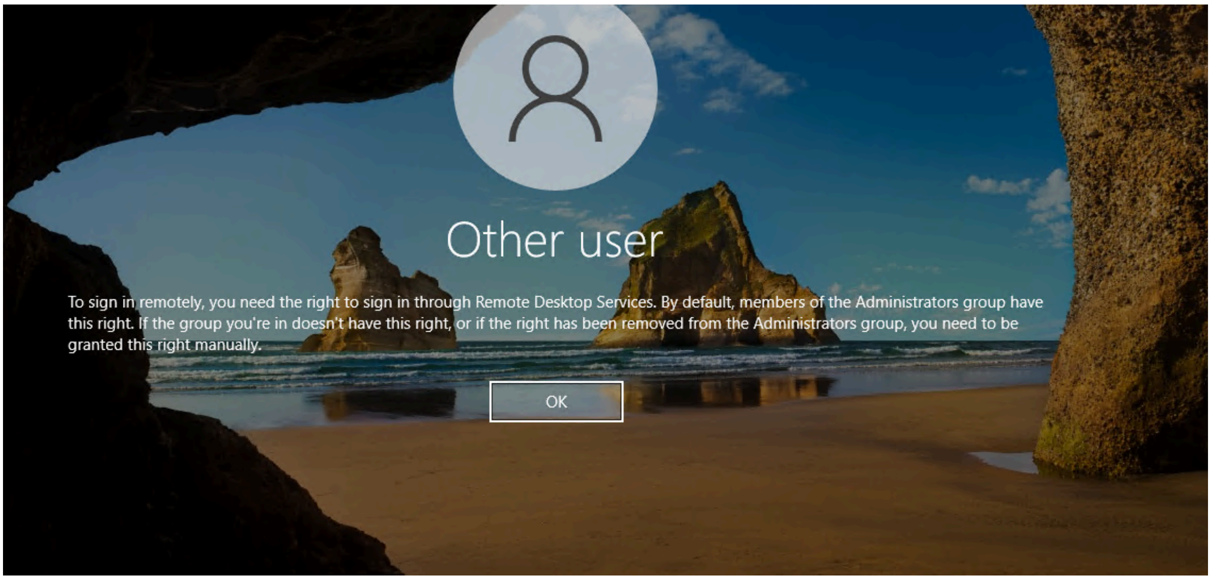
- Test users in FinanceAdmin successfully modified files in both directories.
- Test users in FinanceUsers accessed and edited files in the Audit Progressive folder but could only view files in the Final Audit Data folder.
- Test users in ExternalAuditors accessed the Final Audit Data folder and confirmed their ability to log in via Remote Desktop, though they could not modify files.

Challenges and Solutions

During the project, a few challenges were encountered:

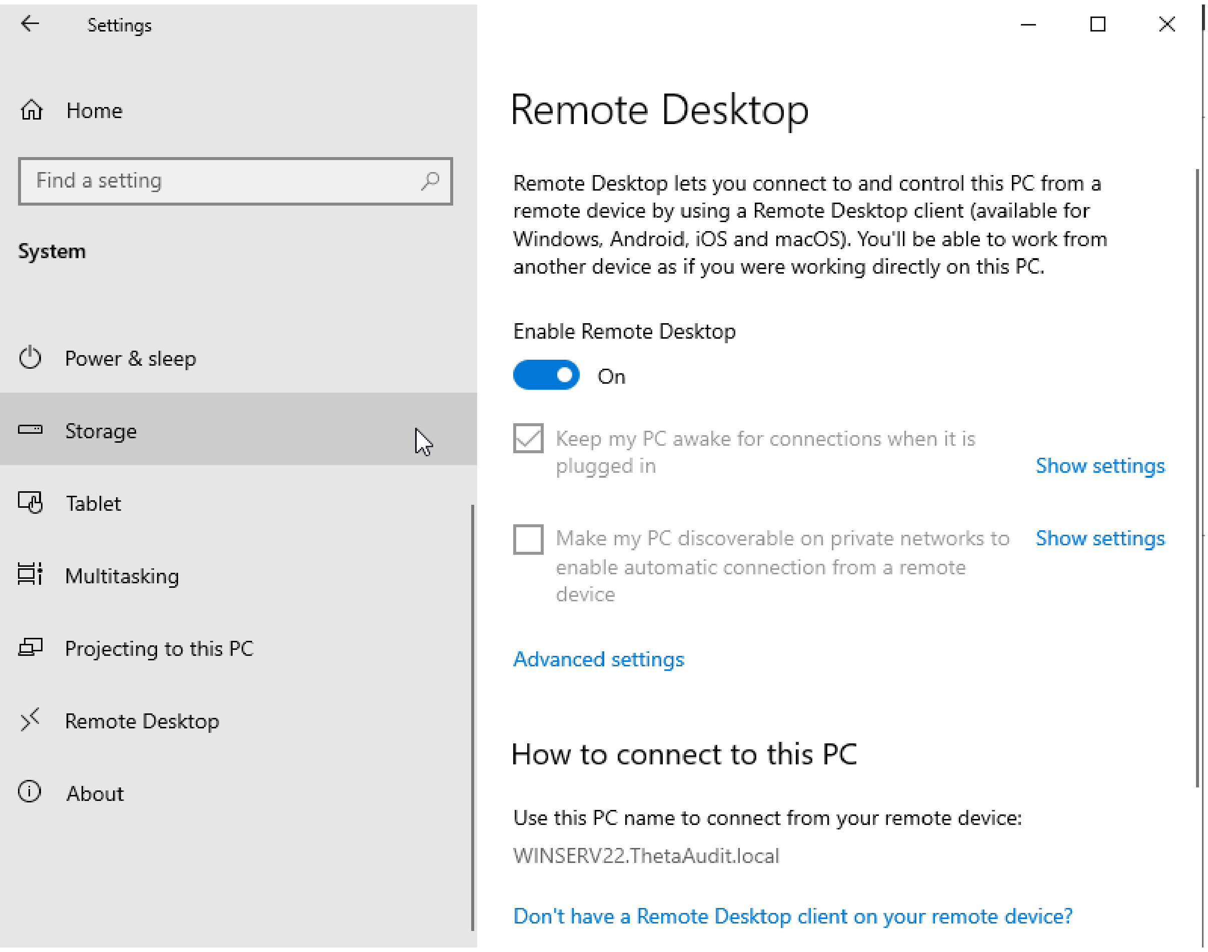
1. **Conflict Between Permissions:** Initial configurations inadvertently allowed ExternalAuditors to modify files in the Final Audit Data folder. This was resolved by revisiting the Security tab and explicitly setting the group's access level to "Read-only."

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.



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

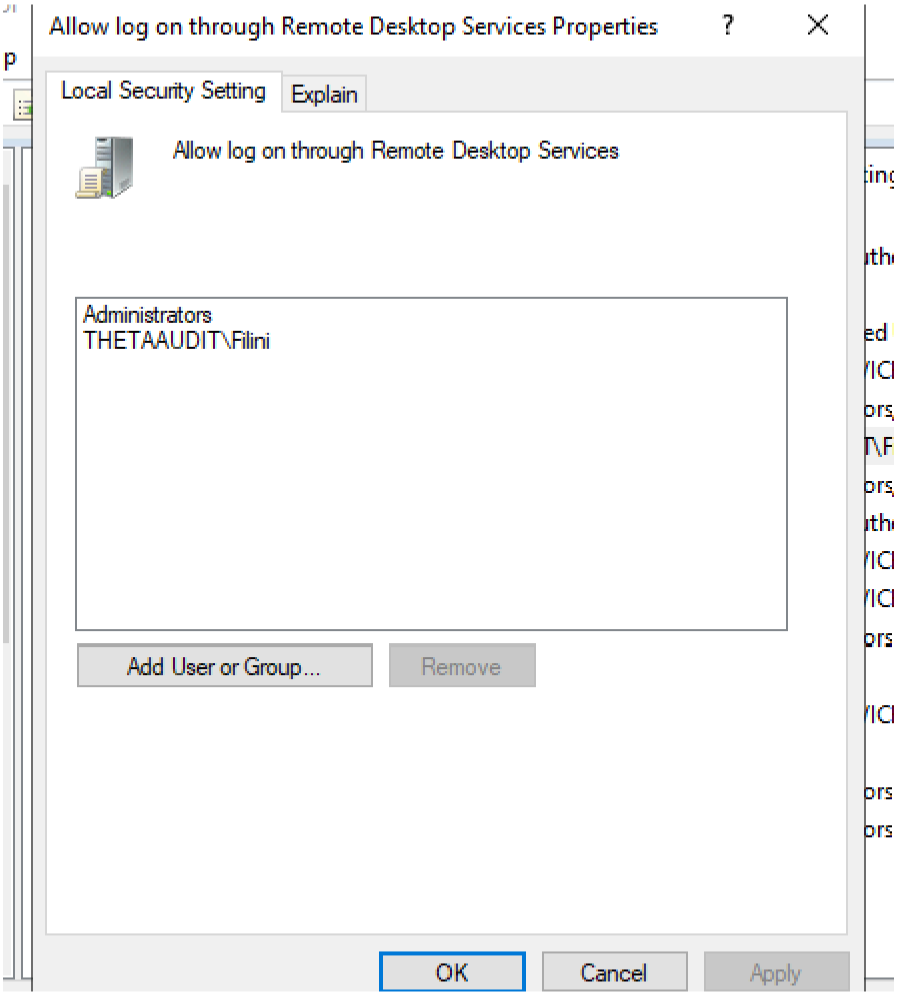
Advanced settings

How to connect to this PC

Use this PC name to connect from your remote device:

WINSERV22.ThetaAudit.local

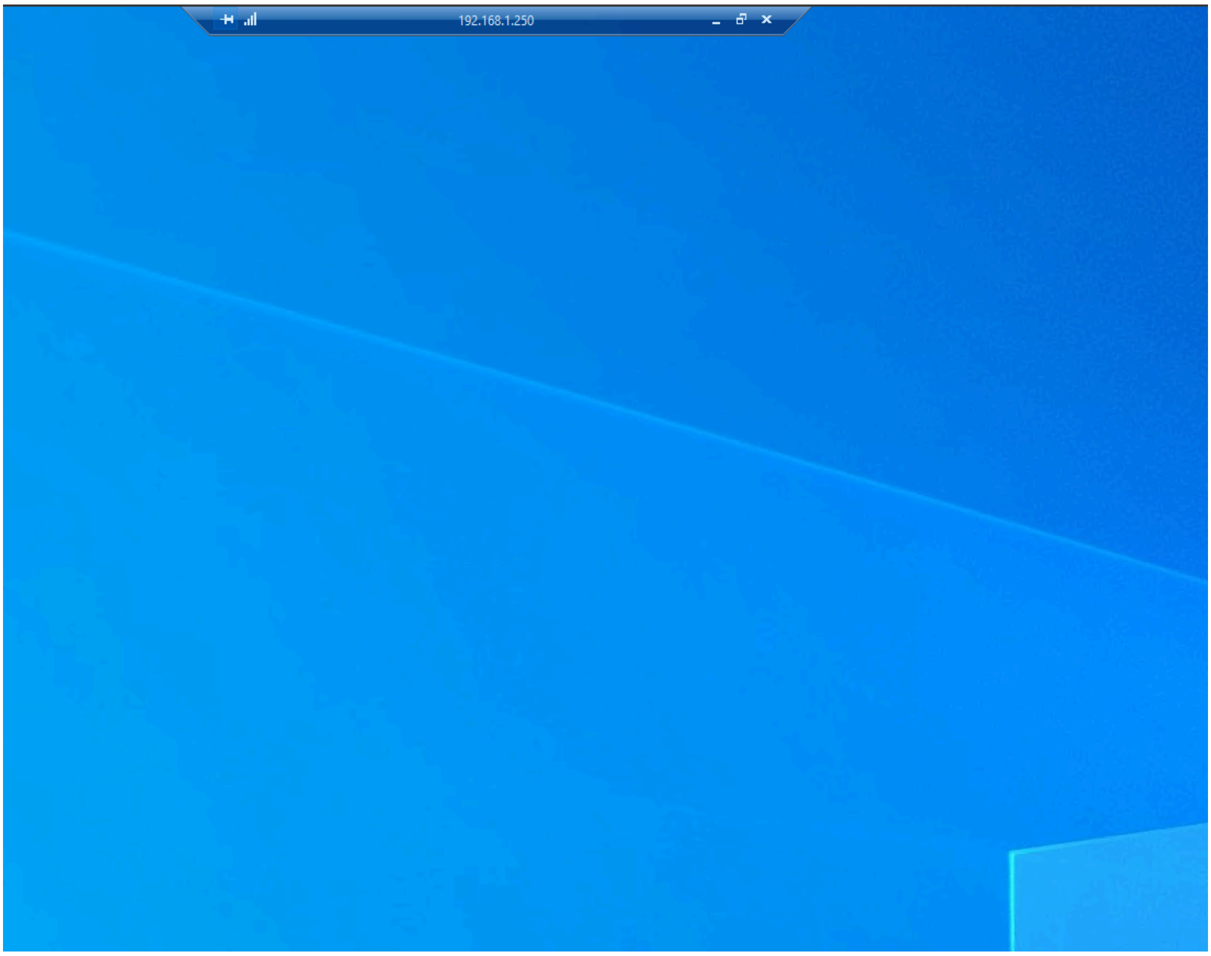
Don't have a Remote Desktop client on your remote device?

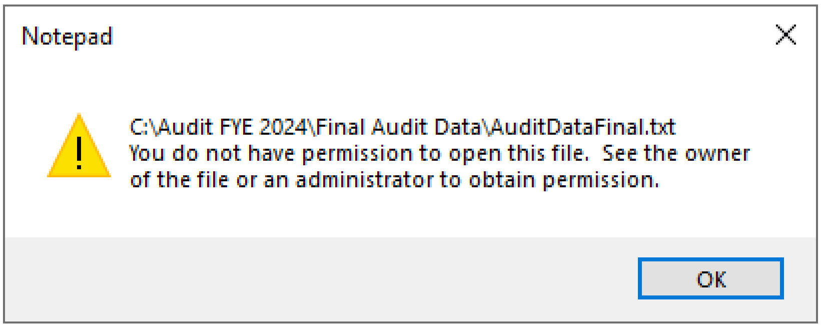


Allow log on through Remote Desktop Services Properties

Allow log on through Remote Desktop Services

Administrators
THETAAUDIT\Filini





C:\Audit FYE 2024\Final Audit Data\AuditDataFinal.txt
You do not have permission to open this file. See the owner of the file or an administrator to obtain permission.

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.