# NETWORK APPLICATIONS

## QHO443 — Module Study Notes

*Week 2: Workgroup Configuration, Local Users & Groups*

Digitally signed by Baba Shaheer Gutappa
Date: 2026.03.02 11:19:25 Z

| | |
|---|---|
| **Module** | QHO443 Network Applications |
| **Week** | Week 2 |
| **Topic** | Workgroup Setup, Local Users & Groups (Department-Based) |
| **Prepared By** | Babashaheer |
| **Version** | 1.0 |

### Learning Outcomes

*By the end of this week, students will be able to:*

1. Configure a Workgroup environment on Windows Server 2019
2. Create and manage Local Users and Groups using Computer Management
3. Design a department-based organisational structure for access control
4. Understand how Windows authentication and authorisation work
5. Troubleshoot Remote Desktop Services (RDP) access issues

# 1. Introduction to Windows Server Network Models

Windows Server supports two primary network models for managing users and resources. Understanding the difference between these two models is essential before configuring any server environment.

| Feature | Workgroup | Domain (Active Directory) |
|---|---|---|
| Management | Decentralised — each PC manages its own users | Centralised — domain controller manages all users |
| Scale | Suitable for small networks (10–20 computers) | Suitable for large enterprise networks |
| User Database | Stored locally in SAM (Security Account Manager) | Stored centrally in Active Directory (AD DS) |
| Authentication | Each machine handles its own login | Domain Controller handles authentication |
| Administration | Each machine must be configured separately | Administered centrally from one location |
| Cost & Complexity | Simple and low cost | Requires server infrastructure, more complex |

*Key Point: In this module, Week 2 focuses on the Workgroup model, which forms the foundation for understanding authentication before progressing to domain-based environments.*

# 2. Workgroup — Concept and Theory

## 2.1 What is a Workgroup?

A Workgroup is a peer-to-peer (P2P) network model where each computer is an independent unit. There is no centralised server managing logins — each machine maintains its own list of users and passwords locally.

Key characteristics of a Workgroup:

- Each computer stores user accounts in its own SAM (Security Account Manager) database.
- A user must have a separate account on every machine they wish to access.
- No single point of control — ideal for small offices or lab environments.
- The default Windows Workgroup name is WORKGROUP; this can be customised.

## 2.2 SAM Database — How Local Accounts are Stored

When you create a local user on Windows Server, the credentials are stored in the Security Account Manager (SAM) database, located at:

```
C:\Windows\System32\config\SAM
```

The SAM database stores:

- Username (plain text identifier)
- Password hash (NTLM hash — never stored in plain text)
- Security Identifier (SID) — unique number assigned to every user
- Group memberships

*Security Note: The SAM file is locked while Windows is running and cannot be accessed directly. Attackers use tools such as Mimikatz or SAMDump to extract hashes — which is why we study these concepts in COM398 System Security.*

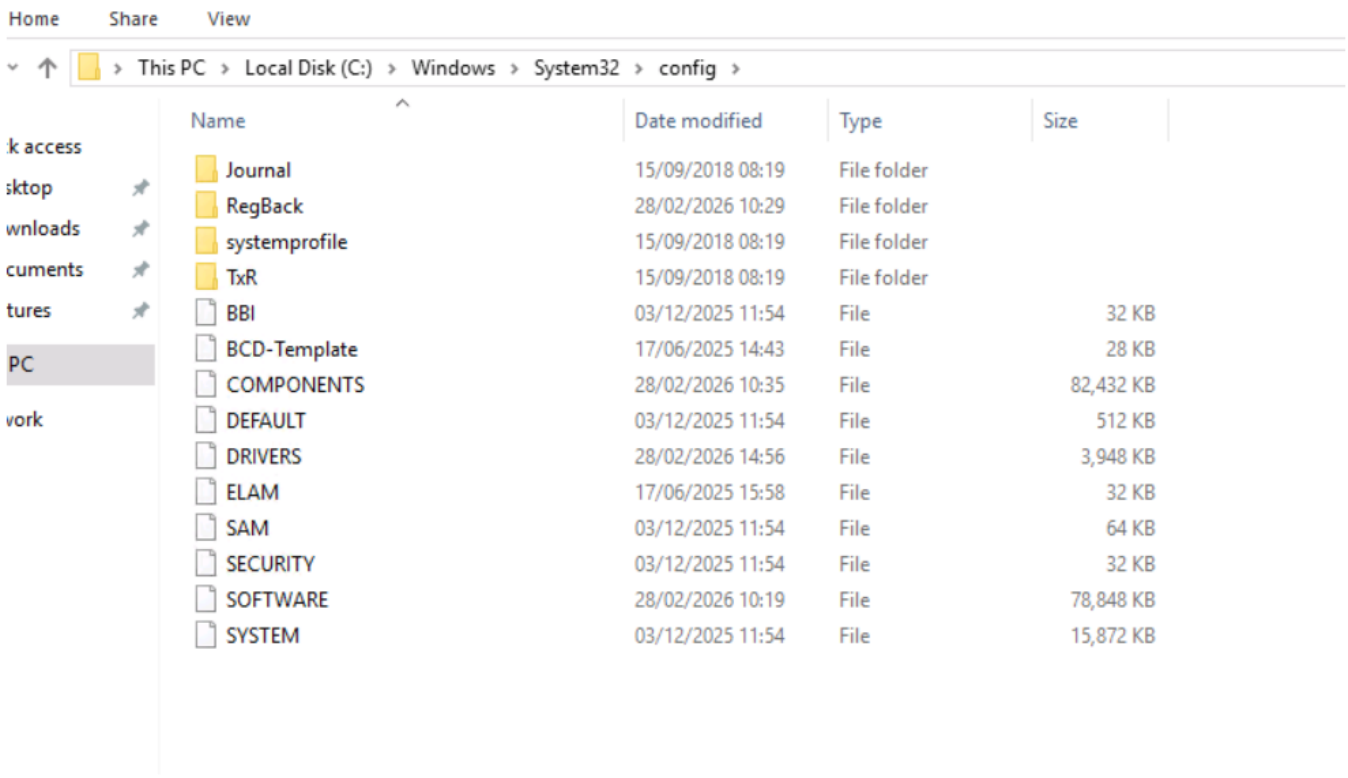
## 2.3 Security Identifier (SID)

Every user account on Windows is assigned a unique Security Identifier (SID). The SID is the real identity Windows uses — not the username. This means:

- If you delete and recreate a user with the same name, they get a NEW SID.
- File permissions assigned to the old SID are lost.
- The SID format appears as: S-1-5-21-xxxxxxxxxx-xxxxxxxxxx-xxxxxxxxxx-XXXX

You can view SIDs using Command Prompt:

```
wmic useraccount get name,sid
```




# 3. Practical Lab — Department-Based Workgroup Setup

## 3.1 Lab Scenario

You are the System Administrator of a company. The company has three departments:

- IT Department — responsible for network and server infrastructure
- Finance Department — manages financial records and accounts
- HR Department — manages employee data and records

Your task is to configure Windows Server 2019 with proper departmental structure.

| Configuration Item | Value |
|---|---|
| Server Name | SERVER01 |
| Operating System | Windows Server 2019 |
| Network Type | Workgroup |
| Workgroup Name | COMPANY |
| Lab Users | 6 users across 3 departments |

## 3.2 Part 1 — Configure Workgroup

## Step 1: Open System Properties

Press the keyboard shortcut:

```
Windows + R
```

In the Run dialog, type:

```
sysdm.cpl
```

Press Enter to open System Properties.

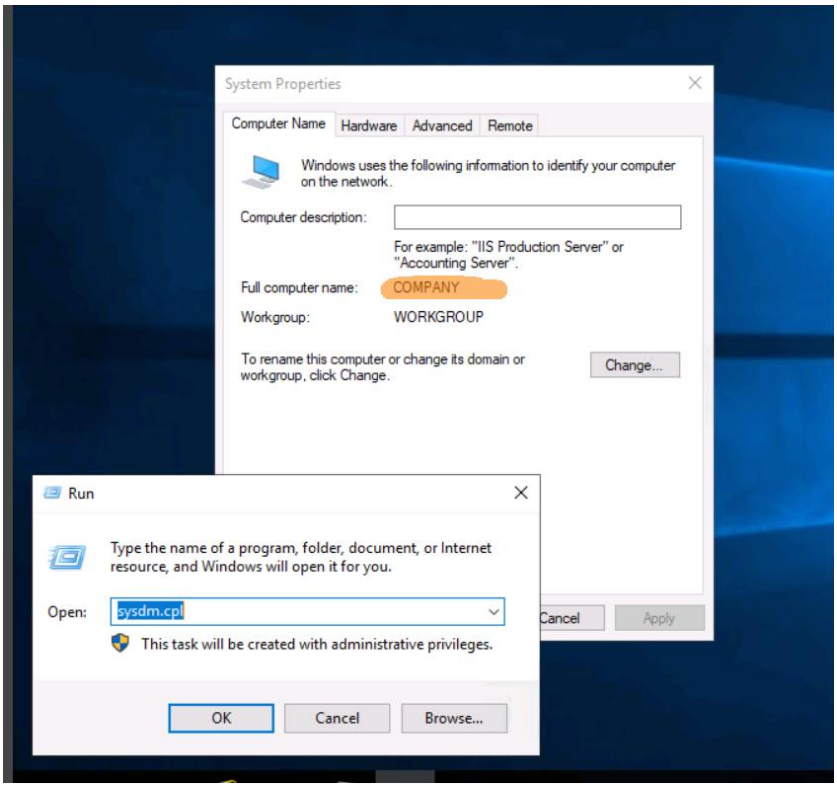
## Step 2: Change the Workgroup Name

In the System Properties window:

6. Click the Computer Name tab.
7. Click the Change button.
8. Select Workgroup (not Domain).
9. Enter the workgroup name: COMPANY
10. Click OK.

## Step 3: Restart the Server

*A restart is required for the workgroup change to take effect. Save all work before restarting.*



## 3.3 Part 2 — Open Local User Management (Computer Management)

Press:

```
Windows + R
```

Type:

```
compmgmt.msc
```

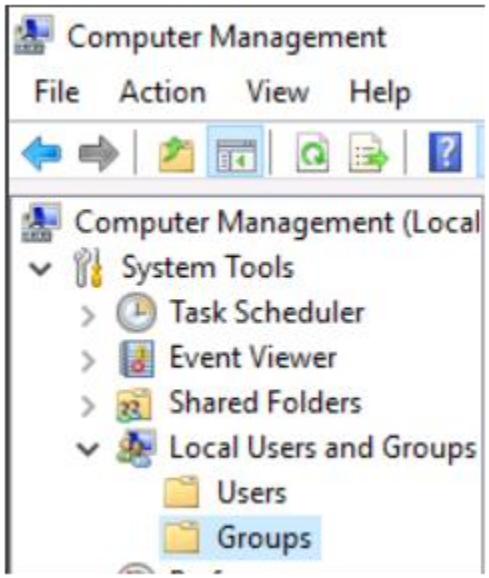
Navigate the left panel to:

```
Computer Management > Local Users and Groups
```

You will see two folders:

- Users — where individual user accounts are created
- Groups — where department groups are created

> *Teaching Point: Think of Users as individual employees and Groups as departments within the company. Permissions are always assigned to Groups, not individuals — this is industry best practice.*



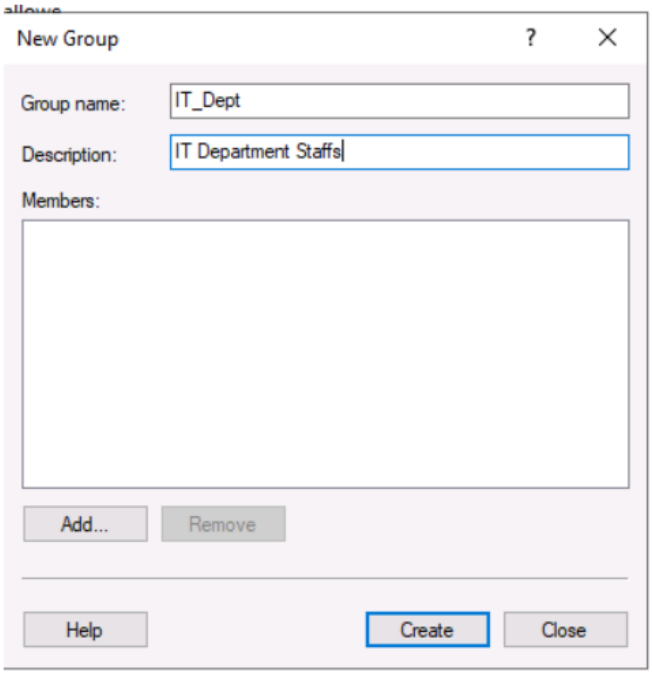

## 3.4 Part 3 — Create Department Groups

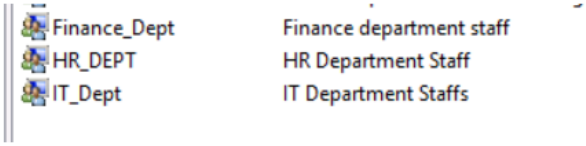
Industry best practice: Always create Groups first, then create Users and assign them to Groups.

Right-click the Groups folder and select New Group.

| Group Name | Description | Department |
|---|---|---|
| IT_Dept | IT Department Staff | Information Technology |
| Finance_Dept | Finance Department Staff | Finance & Accounts |
| HR_Dept | Human Resource Staff | Human Resources |

For each group, enter the Group Name and Description, then click Create.




## 3.5 Part 4 — Create Users Per Department

Navigate to the Users folder. Right-click and select New User for each account below.

### IT Department Users

| Username | Full Name | Password | Department Group |
|---|---|---|---|
| IT_User1 | IT Support Staff | P@ssword123 | IT_Dept |
| IT_User2 | Network Technician | P@ssword123 | IT_Dept |

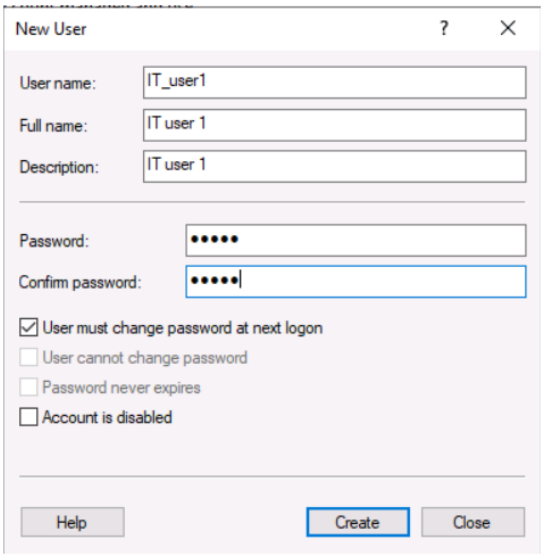
### Finance Department Users

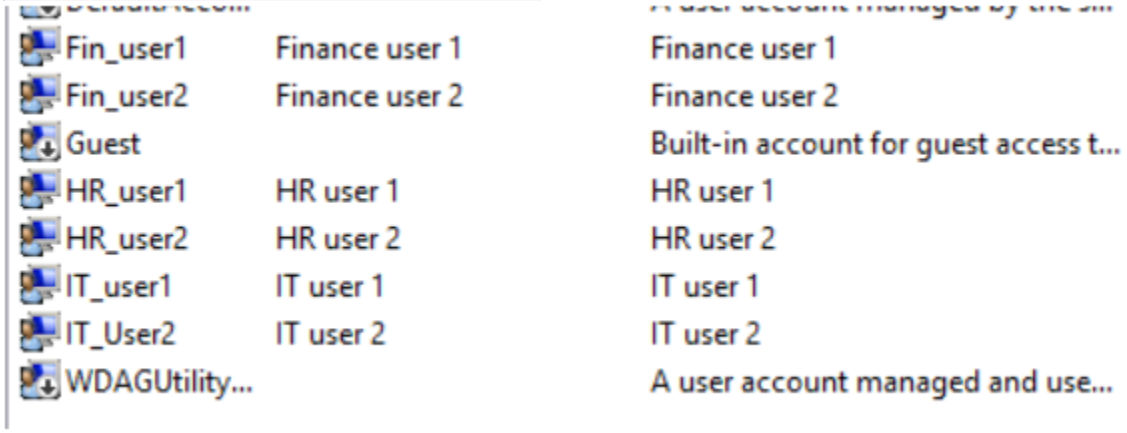
| Username | Full Name | Password | Department Group |
|---|---|---|---|
| Fin_User1 | Accountant | P@ssword123 | Finance_Dept |
| Fin_User2 | Finance Assistant | P@ssword123 | Finance_Dept |

### HR Department Users

| Username | Full Name | Password | Department Group |
|---|---|---|---|
| HR_User1 | HR Manager | P@ssword123 | HR_Dept |
| HR_User2 | HR Executive | P@ssword123 | HR_Dept |

*Lab Settings: For all users, UNCHECK 'User must change password at next logon' and CHECK 'Password never expires'. This is appropriate for lab environments only — never use these settings in production.*

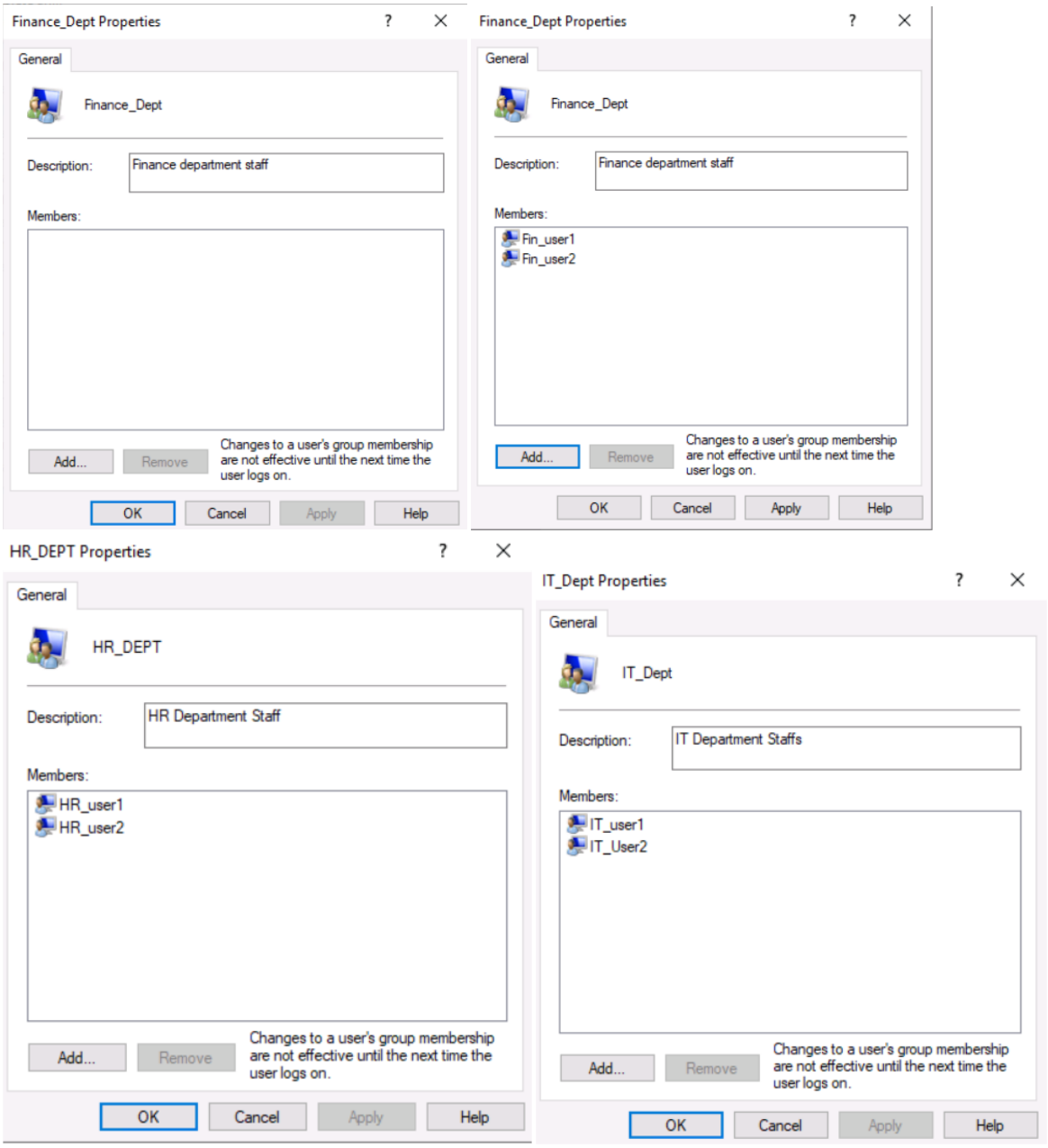



## 3.6 Part 5 — Add Users to Their Department Groups

Now link users to their respective department groups:

11. Open the IT_Dept group. Click Add. Enter IT_User1 and IT_User2. Click Check Names > OK > Apply.
12. Open the Finance_Dept group. Click Add. Enter Fin_User1 and Fin_User2. Click Check Names > OK > Apply.
13. Open the HR_Dept group. Click Add. Enter HR_User1 and HR_User2. Click Check Names > OK > Apply.




## 3.7 Part 6 — Verify Group Membership via Command Prompt

Open Command Prompt and verify each department group:

```
net localgroup IT_Dept
net localgroup Finance_Dept
net localgroup HR_Dept
```

Each command should list the users belonging to that department. This confirms the user-to-group mapping is correctly configured.

```
C:\Users\Administrator>net localgroup IT_Dept
Alias name     IT_Dept
Comment        IT Department Staffs

Members

-------------------------------------------------------------------------------
IT_user1
IT_User2
The command completed successfully.


C:\Users\Administrator>net localgroup HR_Dept
Alias name     HR_Dept
Comment        HR Department Staff

Members

-------------------------------------------------------------------------------
HR_user1
HR_user2
The command completed successfully.


C:\Users\Administrator>net localgroup Finance_Dept
Alias name     Finance_Dept
Comment        Finance department staff

Members

-------------------------------------------------------------------------------
Fin_user1
Fin_user2
The command completed successfully.


C:\Users\Administrator>_
```

## 3.8 Part 7 — Login Authentication Test

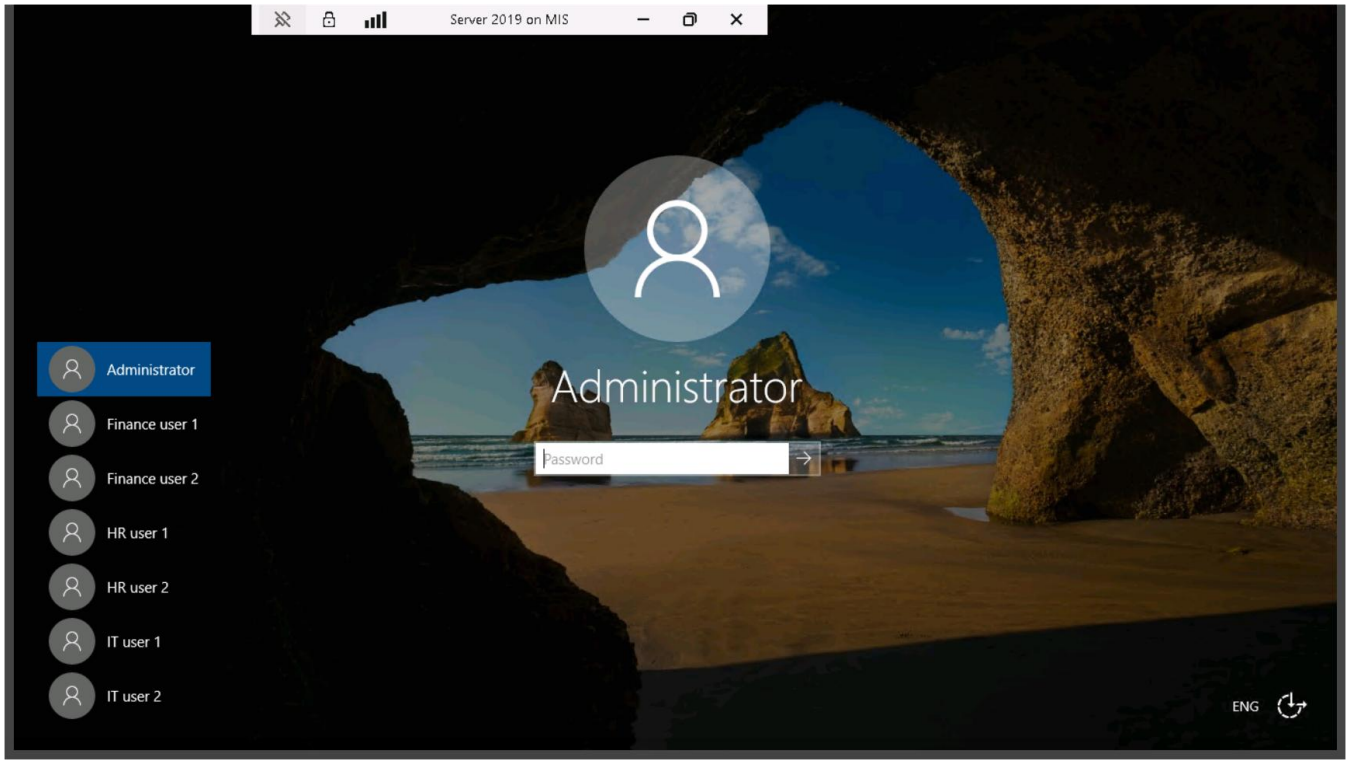
Sign out of the Administrator account. Then attempt to log in with a department user:

```
Username: IT_User1
```

```
Password: P@ssword123
```

During this login, Windows performs the following process:

14. Checks the SAM database for the username.
15. Verifies the NTLM password hash.
16. Identifies group membership (IT_Dept).
17. Creates an Access Token containing the user's SID and group memberships.
18. Grants access to resources permitted for that group.




## 3.9 Part 8 — Verify User Identity in Command Prompt

After logging in as IT_User1, open Command Prompt:

```
whoami
```

This shows the currently logged-in user. Then run:

```
whoami /groups
```

This displays all group memberships for the current user. You should see IT_Dept listed — confirming the user is properly assigned to their department.

# 4. Authentication vs. Authorisation — Core Security Concept

This is one of the most important concepts in network security. Many login failures are due to confusion between these two separate processes.

| Concept | Definition | What Happens | Example |
|---|---|---|---|
| Authentication | Verifying WHO you are | Windows checks username & password against SAM database | IT_User1 enters correct password — identity confirmed |
| Authorisation | Verifying WHAT you are allowed to do | Windows checks if the authenticated user has permission for the requested action | IT_User1 has RDP rights — access granted |
| Access Denied | Authentication passed but Authorisation failed | User is valid but lacks the required permission | Fin_User2 is valid but NOT in Remote Desktop Users group |

*Remember: Authentication success does NOT guarantee access. Authorisation is a separate check that must also succeed. This is why a correct password can still result in an 'Access Denied' error.*

# 5. Remote Desktop Services — Access & Troubleshooting

## 5.1 Understanding RDP Access Control

Remote Desktop Protocol (RDP) allows remote management of a Windows Server. However, creating a user account does NOT automatically grant RDP access. This is a deliberate security measure.

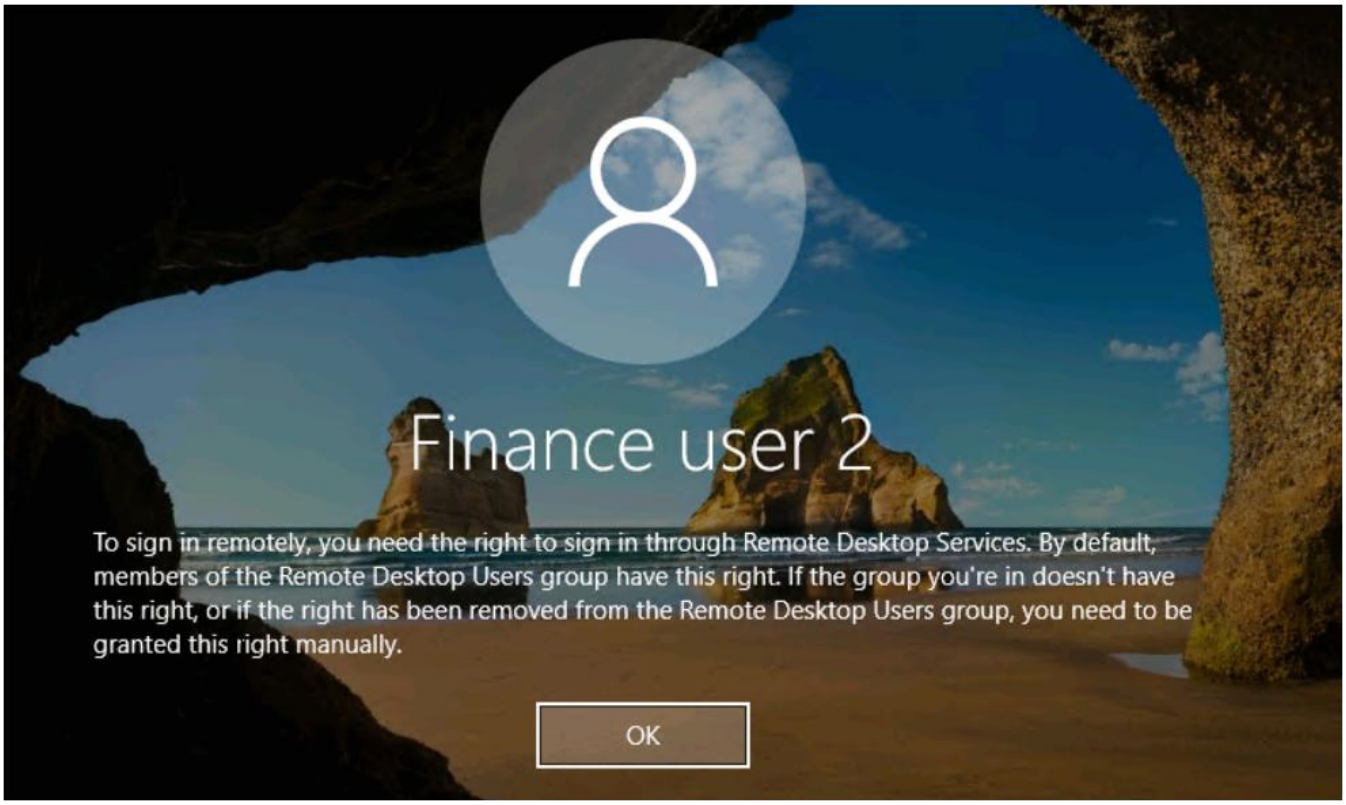
By default, only the following can log in via Remote Desktop:

- The built-in Administrator account
- Members of the Remote Desktop Users group

## 5.2 Common RDP Error

**Error Message:**
*"To sign in remotely, you need the right to sign in through Remote Desktop Services."*

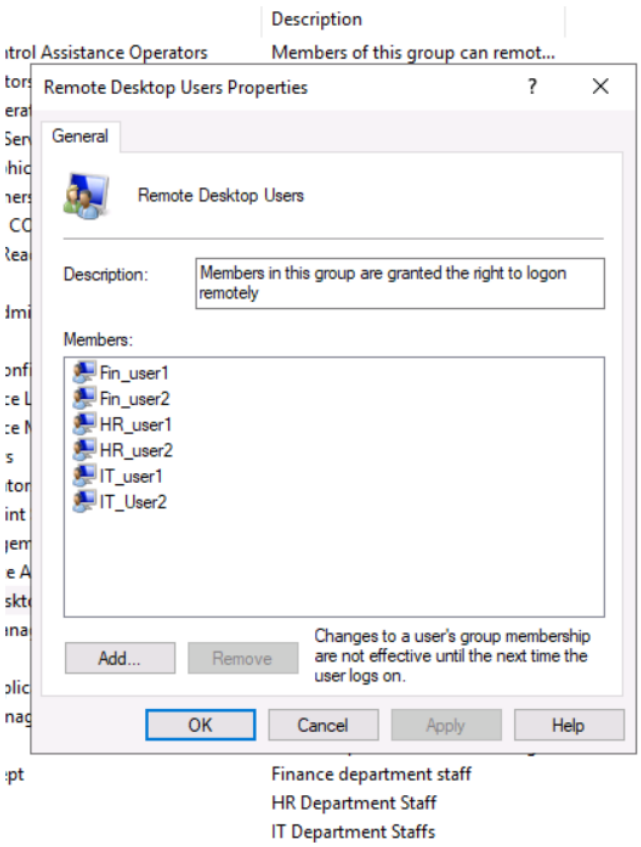
This means: Authentication succeeded but Authorisation failed. The user is valid but not in the Remote Desktop Users group.




## 5.3 Solution — Method 1: Add User to Remote Desktop Users Group

This is the recommended method for individual users:

1. Log in as Administrator.
2. Press Windows + R and type: compmgmt.msc
3. Navigate to: Local Users and Groups > Groups
4. Double-click Remote Desktop Users.
5. Click Add, enter the username (e.g., Fin_User2), click Check Names > OK.
6. Click Apply > OK.
7. Retry the Remote Desktop connection — login will now succeed.




## 5.4 Solution — Method 2: Security Policy (Group-Based — Advanced)

For assigning RDP rights to an entire department, use Local Security Policy:

```
Windows + R > secpol.msc
```

Navigate to:

```
Local Policies > User Rights Assignment > Allow log on through Remote Desktop Services
```

Add the department group (e.g., Finance_Dept) instead of individual users.

> *Best Practice: Always add Groups to permission lists, not individual users. When a new employee joins Finance, they automatically inherit Finance_Dept permissions — no individual configuration needed.*

## 5.5 RDP Troubleshooting Checklist

| Check | How to Verify | Fix if Failed |
|---|---|---|
| User account exists | compmgmt.msc > Users | Create the user account |
| Password is correct | Attempt local login first | Reset password via compmgmt.msc |

| Check | How to Verify | Fix if Failed |
|---|---|---|
| Remote Desktop enabled | System Properties > Remote tab | Enable Allow remote connections |
| User in Remote Desktop Users group | compmgmt.msc > Groups > Remote Desktop Users | Add user or group to Remote Desktop Users |
| Firewall allows RDP (port 3389) | Windows Firewall > Inbound Rules | Enable Remote Desktop rule |
| Network reachability | ping [server IP] from client | Check network configuration |

# 6. Windows Access Token — How Permissions Work Internally

When a user successfully logs in, Windows does not check permissions on every file access in real time. Instead, it creates an Access Token — a secure data structure containing the user's identity and group memberships.

## 6.1 Access Token Contents

| Element | Description |
|---|---|
| User SID | The unique Security Identifier of the logged-in user |
| Group SIDs | SIDs of all groups the user belongs to (e.g., IT_Dept, Users) |
| Privileges | Special rights assigned to the user or their groups |
| Integrity Level | Trust level (Low, Medium, High, System) |
| Logon Session ID | Unique identifier for this login session |

## 6.2 Authentication Flow Diagram

The complete authentication and authorisation process when a user logs in:

**1. User enters Username & Password**

**2. Windows reads SAM Database**

**3. NTLM Hash Comparison — Verify Password**

**4. SID Retrieved from SAM**

**5. Group Memberships Loaded**

**6. Access Token Created (contains SID + Group SIDs + Privileges)**

**7. Desktop Loaded — User Session Begins**

*This process prepares students for advanced topics: NTLM Authentication, Kerberos (in domain environments), NTFS file permissions, and Effective Access calculation.*

# 7. Real-World Application & Industry Context

## 7.1 Why Group-Based Access Control Matters

In real enterprise environments, individual-based permission assignment is considered poor practice. Group-based access control (also called Role-Based Access Control, or RBAC) provides:

| Benefit | Explanation |
|---|---|
| Scalability | Add one new employee to a group and they inherit all necessary permissions instantly |
| Consistency | All members of Finance_Dept have identical access — no accidental discrepancies |
| Auditability | Easier to audit who has access to what resources by reviewing group memberships |
| Security | Removing a user from a group immediately revokes all associated permissions |
| Compliance | Meets regulatory requirements (GDPR, ISO 27001) for access management |

## 7.2 Department Isolation — Why It Matters

A key security principle demonstrated in this lab is least privilege — users should only have access to the resources they need for their role.

- IT staff can access server management tools — Finance cannot.
- Finance staff access accounting systems — HR cannot view payroll unless explicitly permitted.
- HR staff access employee records — IT staff should not have access without authorisation.

*Discussion Question for Class: Can an IT_User access Finance files by default after today's lab? The answer is NO — unless permissions are explicitly granted. This will be explored in the next week's lab on NTFS permissions and shared folders.*

## 7.3 Workgroup vs. Domain in Enterprise

While this lab uses a Workgroup model for simplicity, real enterprise environments use Active Directory Domain Services (AD DS). However, the fundamental concepts are identical:

- SAM database in Workgroup = Active Directory database in Domain
- Local Groups in Workgroup = Security Groups in Active Directory
- Local user accounts = Domain user accounts
- Computer Management = Active Directory Users and Computers (ADUC)

# 8. Week 2 Summary — Key Takeaways

| Topic | Key Point |
|---|---|
| Workgroup | Peer-to-peer model; users managed locally in SAM database; no centralised control |
| SAM Database | Stores usernames, NTLM hashes, and SIDs; located in System32/config/SAM |
| SID | Every user has a unique Security Identifier; permissions are linked to SID not username |
| Groups First | Always create department groups before creating users — industry best practice |
| Authentication | Verifies who you are (username + password check against SAM) |
| Authorisation | Verifies what you can do (group membership check for the requested resource) |
| RDP Error | Correct password but no RDP permission = Authorisation failure, not Authentication failure |
| Access Token | Created after successful login; contains user SID, group SIDs, and privileges |
| RBAC | Always assign permissions to groups, never to individual users in enterprise environments |

# 9. References

Microsoft Corporation. (2023). Local Users and Groups [Microsoft Learn Documentation]. Microsoft. https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/manage/understand-security-identifiers

Microsoft Corporation. (2023). Remote Desktop Services — Allow Log On. Microsoft Learn. https://learn.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/allow-log-on-through-remote-desktop-services

Microsoft Corporation. (2023). Security Account Manager. Microsoft Learn. https://learn.microsoft.com/en-us/windows/security/identity-protection/access-control/security-identifiers

EC-Council. (2023). Certified Ethical Hacker (CEH) v13 Course Materials — System Hacking. EC-Council Press.

CompTIA. (2023). Security+ Study Guide: SY0-701. CompTIA Press.

Stallings, W. (2022). Network Security Essentials: Applications and Standards (7th ed.). Pearson Education.

Chapple, M., & Seidl, D. (2022). CompTIA Security+ Study Guide: Exam SY0-701. Sybex.

*These notes have been prepared by Babashaheer for QHO443 Network Applications — Week 2 at Southampton Solent University / QA Partnership. Materials are intended for educational use within the module.*