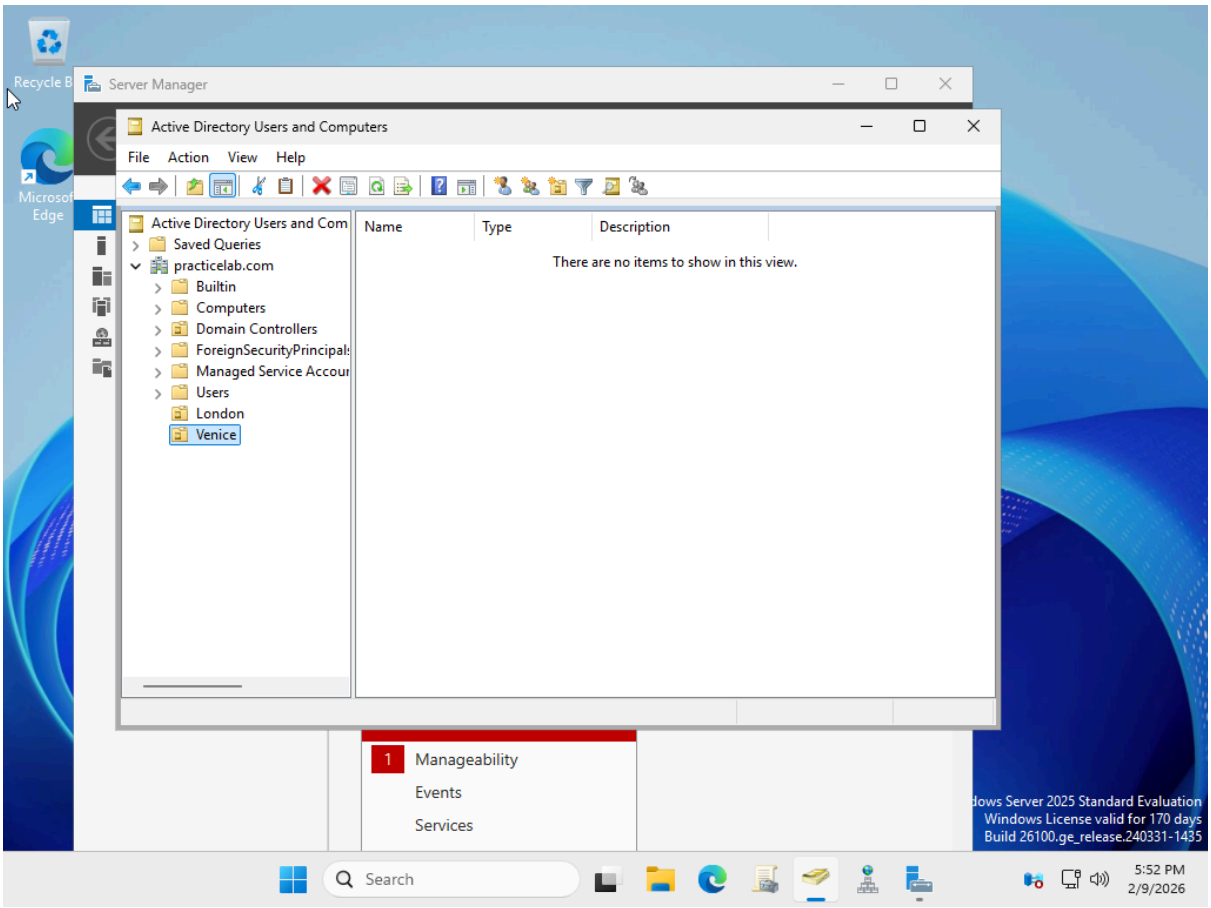
Active Directory instruments

The purpose of this lab was to demonstrate how users can be effectively managed using Active Directory tools while applying the principle of least privilege. This principle ensures that each user is granted only the permissions necessary to perform their job, reducing security risks caused by excessive access rights.

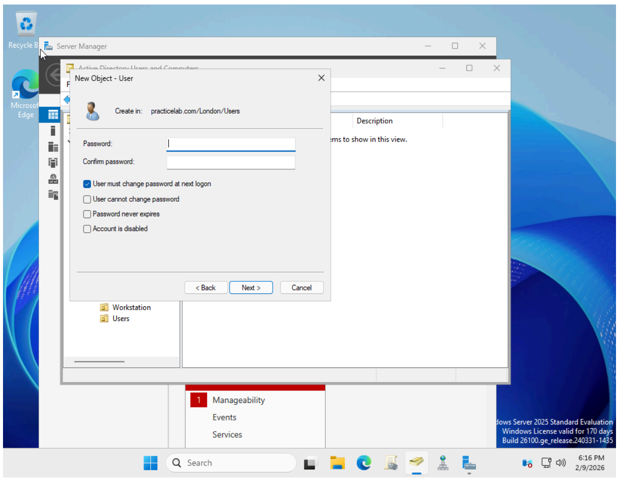
Using Active Directory Users and Computers, I designed a structure that simulates a real company environment with two locations, each containing two internal departments. To accurately represent the organizational structure, I created Organizational Units (OUs) for each location and, within them, separate OUs for departments such as HR and IT, as well as dedicated OUs for users and workstations. This approach provides a clear and organized hierarchy and makes it easier to apply delegations and security policies in a structured way.



There are no items to show in this view.

dows Server 2025 Standard Evaluation
Windows License valid for 170 days
Build 26100.ge_release.240331-1435

Within the OUs dedicated to users, I created test accounts by assigning a first name, last name, and an initial password. For security reasons, I configured the accounts so that users are required to change their password at first logon. Through the account properties, it is also possible to configure settings such as account expiration dates, which are useful for temporary staff, and logon hours to restrict access to specific time frames. Additionally, administrative actions such as resetting passwords or disabling accounts can be performed quickly when needed, which are essential tasks for day-to-day account management.



New Object - User

Create in: practicelab.com/London/Users

Password:

Confirm password:

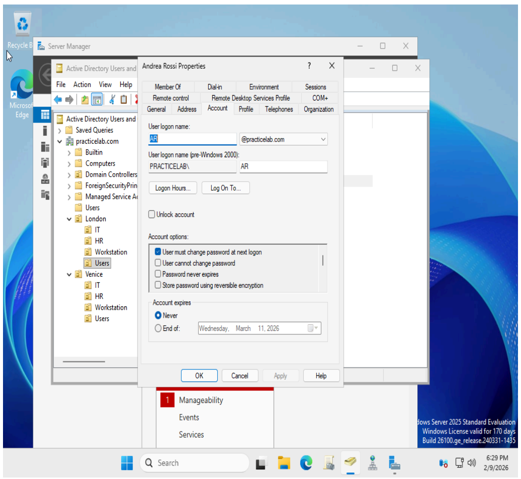
☑ User must change password at next logon

□ User cannot change password

□ Password never expires

□ Account is disabled

Server Manager
Active Directory Users and Computers
Description
ms to show in this view.
< Back
Next >
Cancel
Workstation
Users
1 Manageability
Events
Services
dows Server 2025 Standard Evaluation
Windows License valid for 170 days
Build 26100.ge_release.240331-1435
Search
6:16 PM
2/9/2026



Andrea Rossi Properties

Account

User logon name: AR @practicelab.com

User logon name (pre-Windows 2000): PRACTICELAB\ AR

□ Unlock account

Account options:

☑ User must change password at next logon

□ User cannot change password

□ Password never expires

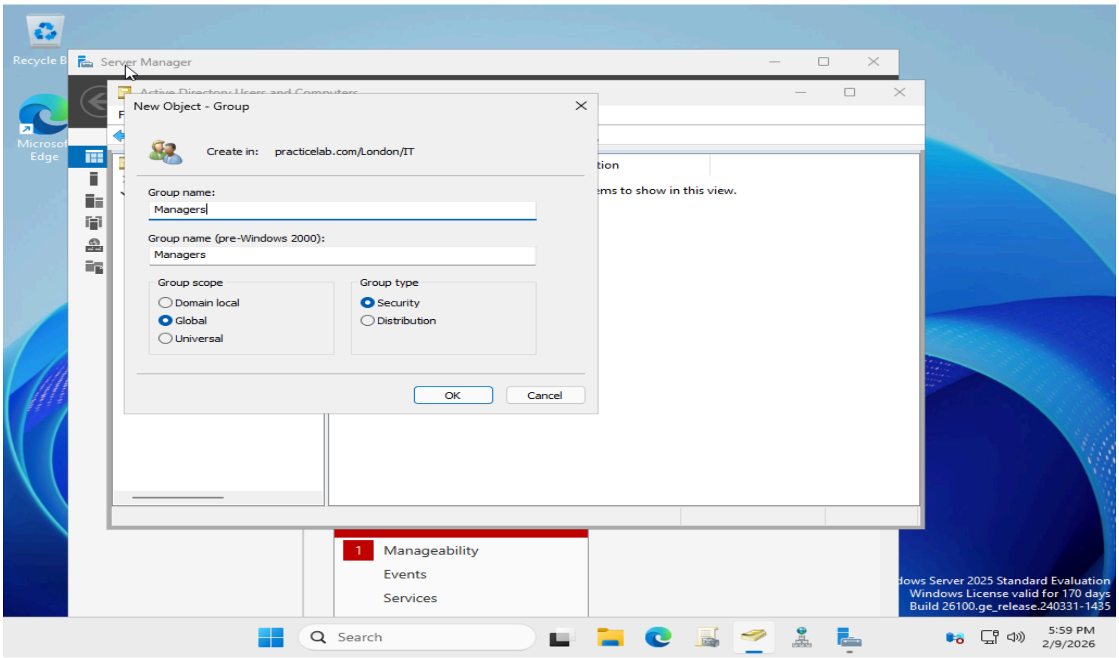
□ Store password using reversible encryption

Account expires

● Never

○ End of: Wednesday, March 11, 2026

Group management was an important part of the lab. I created groups by selecting the appropriate type and scope based on their purpose. Security groups were used to assign permissions and privileges, while distribution groups are intended only for email communication and do not provide security access. Departmental groups within each location were created as Global Security Groups, since they contain users from the same domain. Where needed, Universal Security Groups can be used to aggregate groups from multiple locations.



New Object - Group

Create in: practicelab.com/London/IT

Group name: Managers

Group name (pre-Windows 2000): Managers

Group scope

○ Domain local

● Global

○ Universal

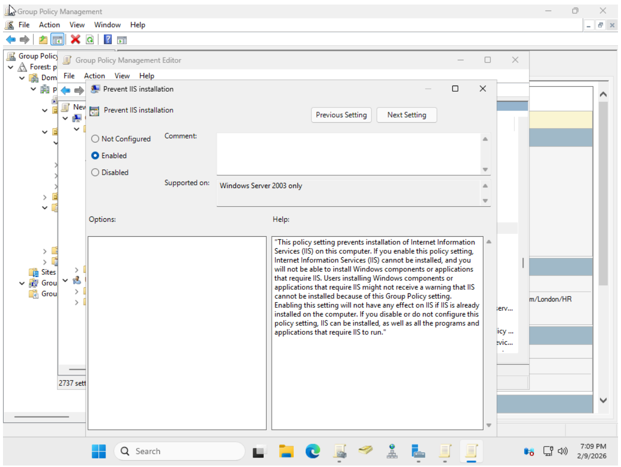
Group type

● Security

○ Distribution

Server Manager
Active Directory Users and Computers
tion
ms to show in this view.
OK
Cancel
1 Manageability
Events
Services
dows Server 2025 Standard Evaluation
Windows License valid for 170 days
Build 26100.ge_release.240331-1435
Search
5:59 PM
2/9/2026

Another key aspect of the lab was the use of Group Policy Objects (GPOs). Group Policy allows centralized control over security settings, system configurations, and the actions that users and computers are allowed to perform. As a practical example, I configured a policy to prevent the Human Resources department from installing the IIS role, since it is not a tool relevant to their responsibilities. This policy was linked to the HR Organizational Units and applied under the Computer Configuration section, showing how restrictions can be targeted based on job roles in line with the principle of least privilege.



Prevent IIS installation

○ Not Configured
● Enabled
○ Disabled

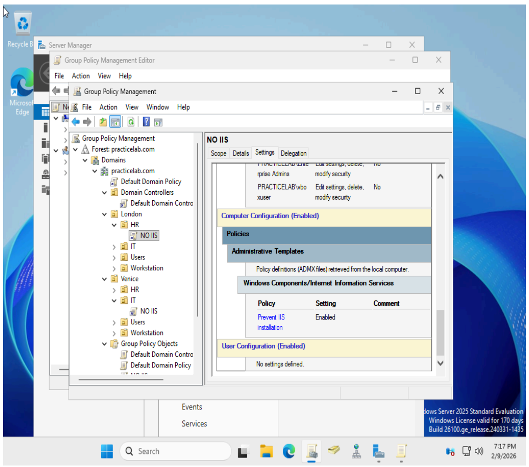
Comment:

Supported on: Windows Server 2003 only

Options:

Help:

"This policy setting prevents installation of Internet Information Services (IIS) on this computer. If you enable this policy setting, Internet Information Services (IIS) cannot be installed, and you will not be able to install Windows components or applications that require IIS. Users installing Windows components or applications that require IIS might not receive a warning that IIS cannot be installed because of this Group Policy setting. Enabling this setting will not have any effect on IIS if IIS is already installed on the computer. If you disable or do not configure this policy setting, IIS can be installed, as well as all the programs and applications that require IIS to run."


Recycle Bin
Microsoft Edge
Server Manager
Group Policy Management Editor
File Action View Help
Group Policy Management
File Action View Window Help
Scope
Details
Settings
Delegation
Events
Services
Windows Server 2025 Standard Evaluation
Windows License valid for 170 days
Build 26100.ge_release.240331-1435
Search
7:17 PM
2/9/2026

- Group Policy Management
  - Forest: practicelab.com
    - Domains
      - practicelab.com
        - Default Domain Policy
        - Domain Controllers
          - Default Domain Contro
        - London
          - HR
            - NO IIS
          - IT
          - Users
          - Workstation
        - Venice
          - HR
          - IT
            - NO IIS
          - Users
          - Workstation
        - Group Policy Objects
          - Default Domain Contro
          - Default Domain Policy

NO IIS

PRACTICELAB\Enterprise Admins	Edit settings, delete, modify security	No
PRACTICELAB\vboxuser	Edit settings, delete, modify security	No

Computer Configuration (Enabled)

Policies

Administrative Templates

Policy definitions (ADMX files) retrieved from the local computer.

Windows Components/Internet Information Services

Policy	Setting	Comment
Prevent IIS installation	Enabled	

User Configuration (Enabled)

No settings defined.

Overall, this lab demonstrates how Active Directory can be used to design a structured enterprise environment, manage users and devices logically, assign permissions through properly configured groups, and enforce centralized security controls through Group Policy. The result is an infrastructure that is organized, secure, and easier to manage in a real-world scenario.