OBJECTIVES

- Create User Accounts
- Create Organizational Units and sort users
- Create and assign security groups based on OU and role
- Validate propagation across Windows and Linux clients

For the purposes of this exercise the default user accounts and folders will not be modified, but only added to.

OU SETUP

OU Structure:

- Main Forest
    - Domain (lab.local)
        - Company Site (PharmaTec)
            - HR
            - Manufacturing

USER CREATION

Users were created directly inside the containers, according to their individual designations, using the GUI interface.

Creation Criteria:

- Disabled by default
- Password change required on first logon
- Expiration date set for contractors; permanent accounts for in-house employees
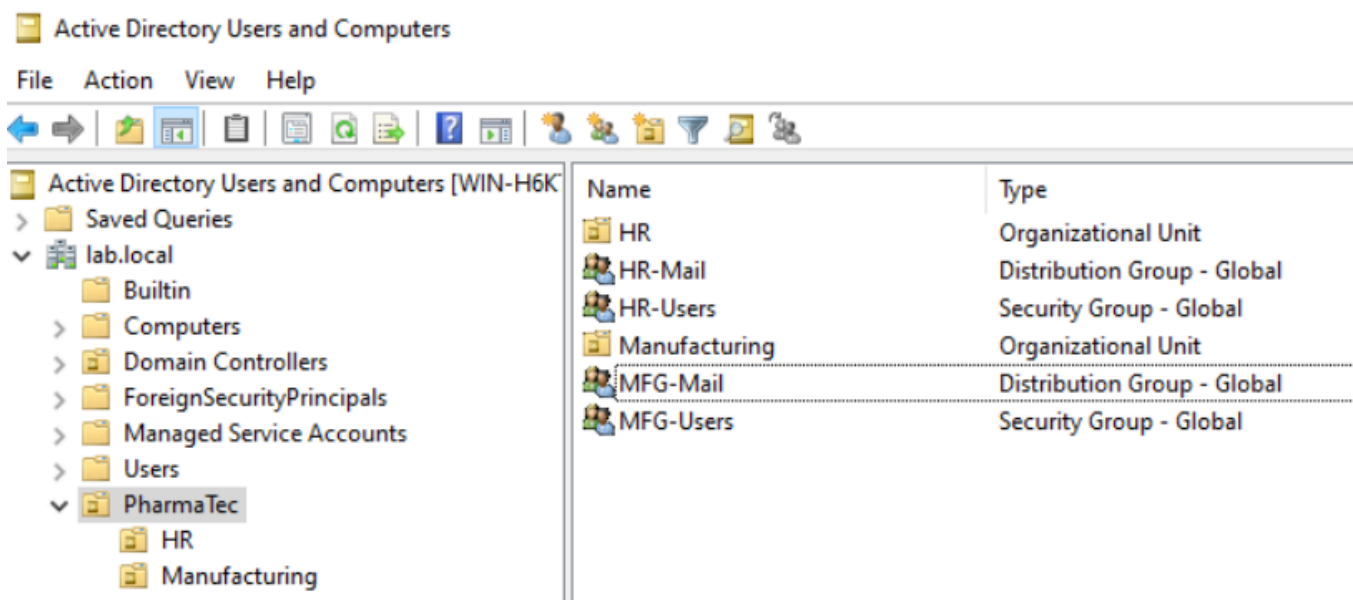- Logon hours restriction set per department
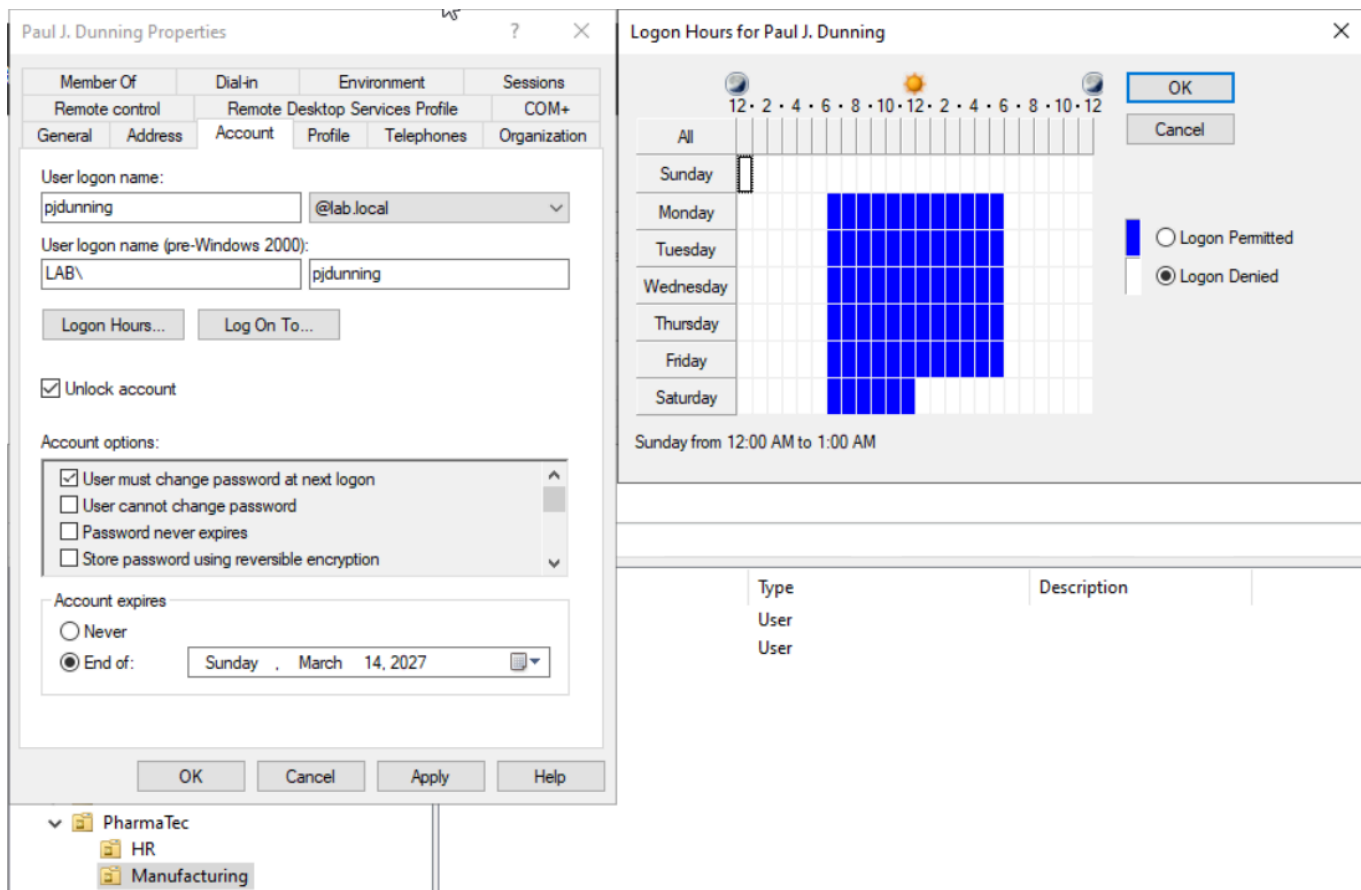
GROUP CREATION

Created departmental global security groups for permission management

- HR-Users
- MFG-Users

Created global distribution groups for departmental communications, separate from security groups used for permissions

- HR-Mail
- MFG-Mail

Active Directory Users and Computers

Name	Type
HR	Organizational Unit
HR-Mail	Distribution Group - Global
HR-Users	Security Group - Global
Manufacturing	Organizational Unit
MFG-Mail	Distribution Group - Global
MFG-Users	Security Group - Global

CLIENT VALIDATION

AlmaLinux

The AlmaLinux client was joined to the `lab.local` domain using SSSD.
Domain authentication succeeded, and the user was able to log in with AD credentials. Network connectivity and DNS resolution were also verified.


```
asmith@lab.local@alma01:~$ id asmith@lab.local
uid=1285201112(asmith@lab.local) gid=1285200513(domain users@lab.local) groups=1285200513(domain users@lab.local),12852011
08(hr-users@lab.local)
asmith@lab.local@alma01:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: enp1s0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 52:54:00:67:ea:ae brd ff:ff:ff:ff:ff:ff
    altname enx52540067eaae
    inet 10.10.10.101/24 brd 10.10.10.255 scope global dynamic noprefixroute enp1s0
       valid_lft 690847sec preferred_lft 690847sec
    inet6 fe80::5054:ff:fe67:eaae/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
asmith@lab.local@alma01:~$ nslookup google.com
Server:         10.10.10.10
Address:        10.10.10.10#53

Non-authoritative answer:
Name:    google.com
Address: 74.125.29.138
Name:    google.com
Address: 74.125.29.101
```

Win11 Corporate

After joining the workstation to the domain, the activated account for Amber Smith (member of the HR-Users group) was able to log in successfully using domain credentials.

```
Command Prompt

Microsoft Windows [Version 10.0.26200.7840]
(c) Microsoft Corporation. All rights reserved.

C:\Users\asmith>whoami
lab\asmith

C:\Users\asmith>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . : lab.local
   Link-local IPv6 Address . . . . . : fe80::7c1c:499e:5dde:bf9d%5
   IPv4 Address. . . . . . . . . . . : 10.10.10.100
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.10.10.10

C:\Users\asmith>nslookup google.com
Server:  UnKnown
Address:  10.10.10.10

Non-authoritative answer:
Name:    google.com
Addresses:  2a00:1450:400a:1009::8b
          2a00:1450:400a:1009::65
          2a00:1450:400a:1009::71
          2a00:1450:400a:1009::8a
          192.178.170.100
          192.178.170.139
          192.178.170.102
          192.178.170.101
          192.178.170.138
          192.178.170.113
```