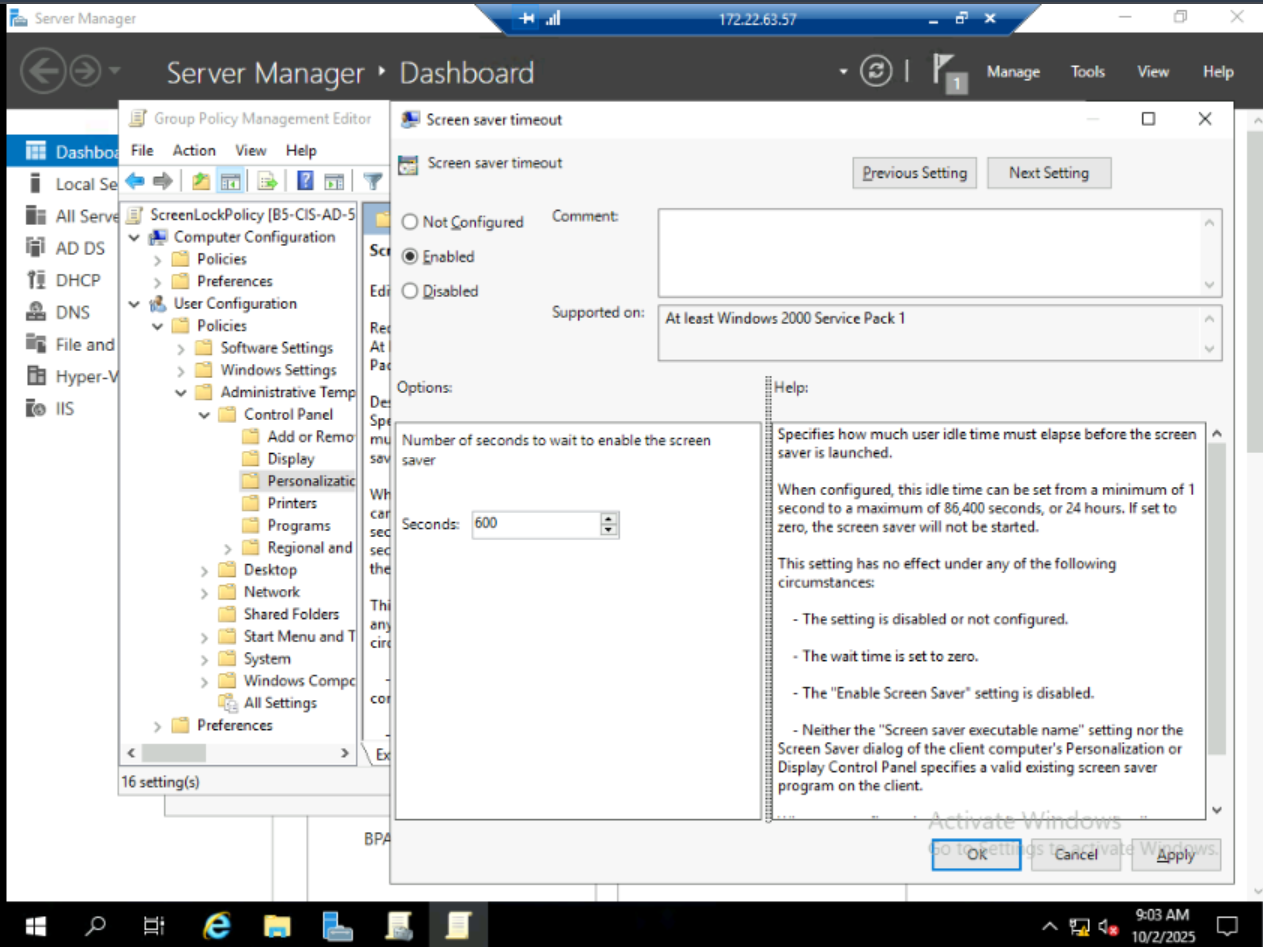
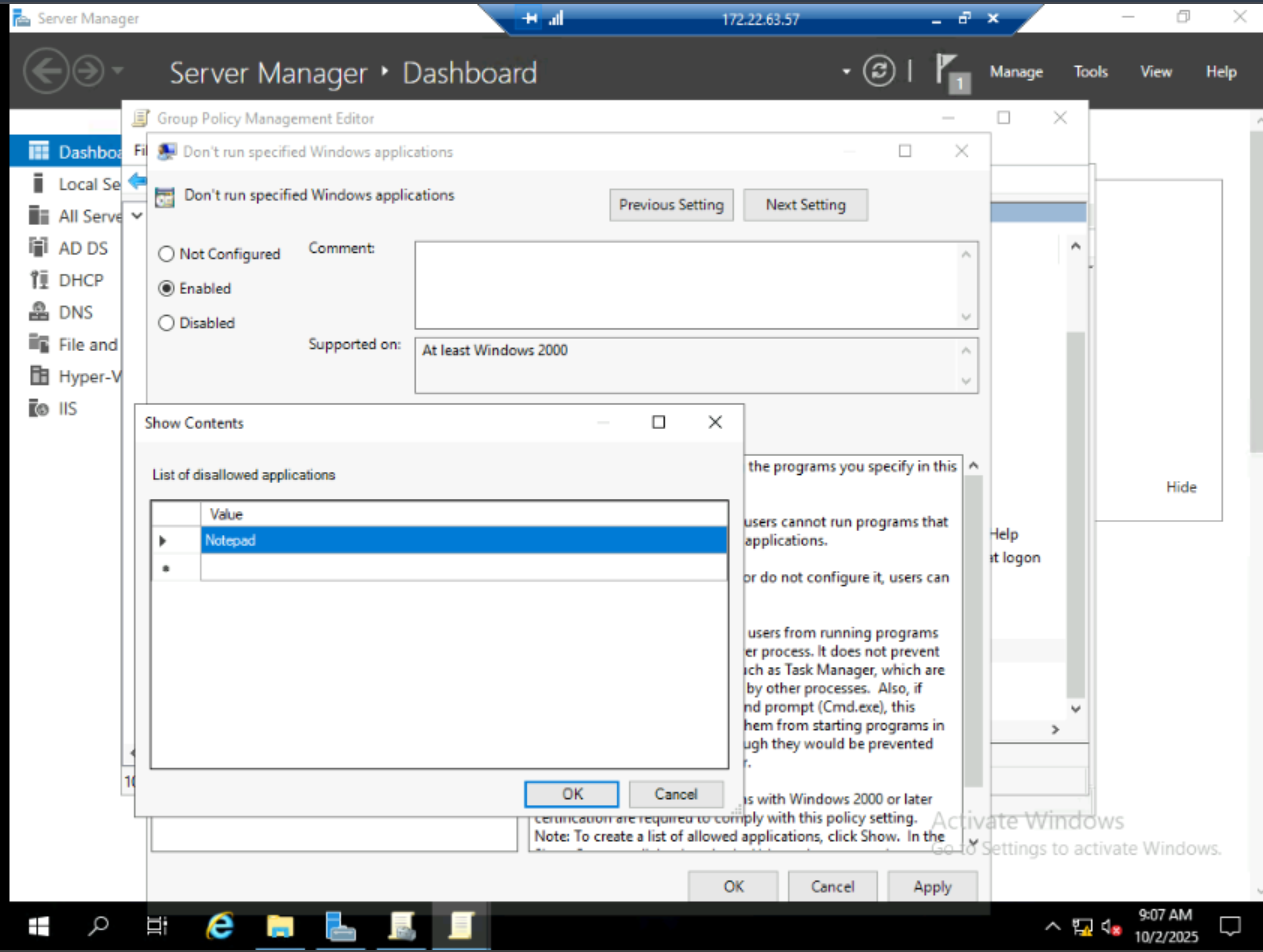
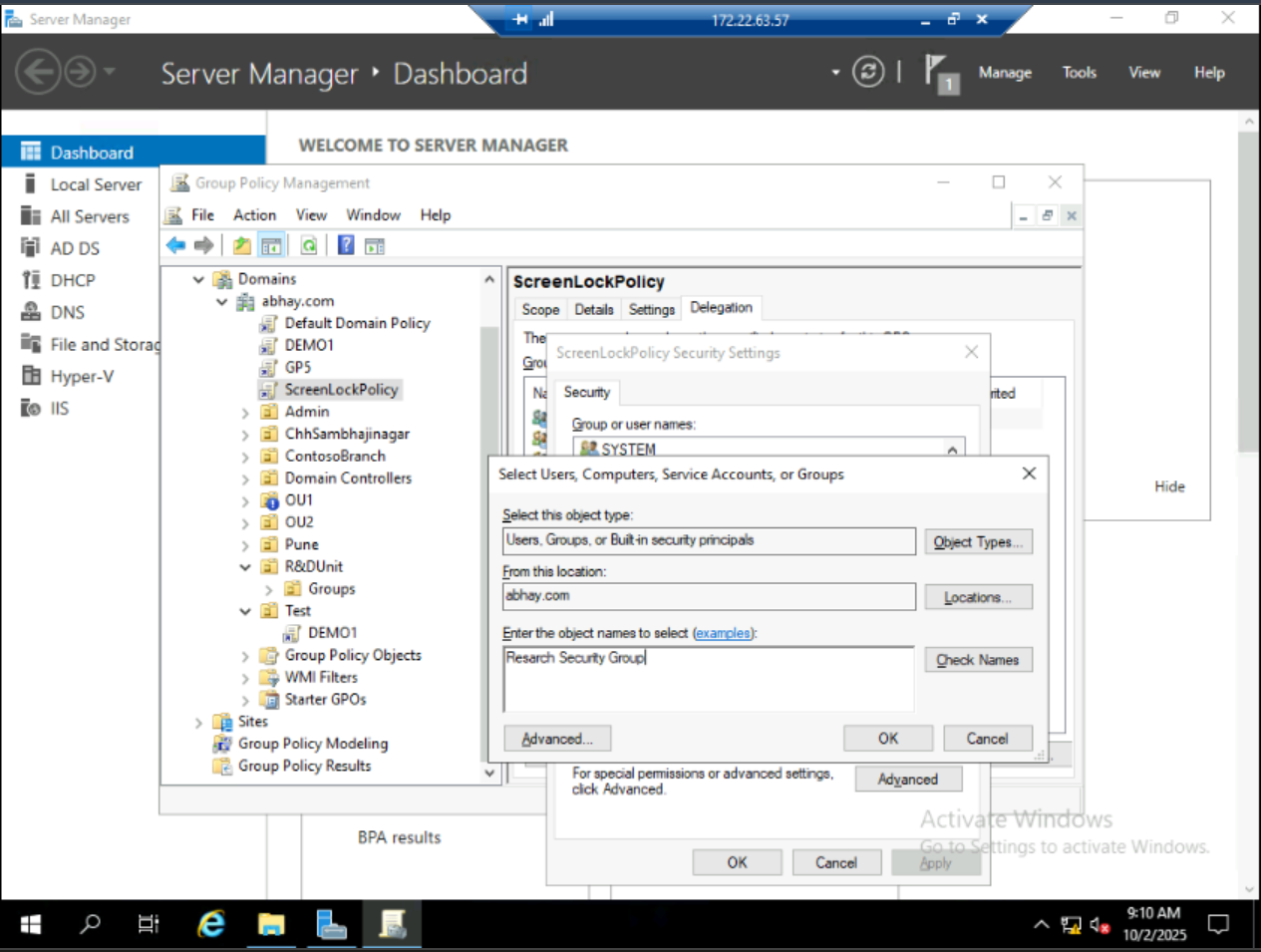
**Day 7 Assignment**

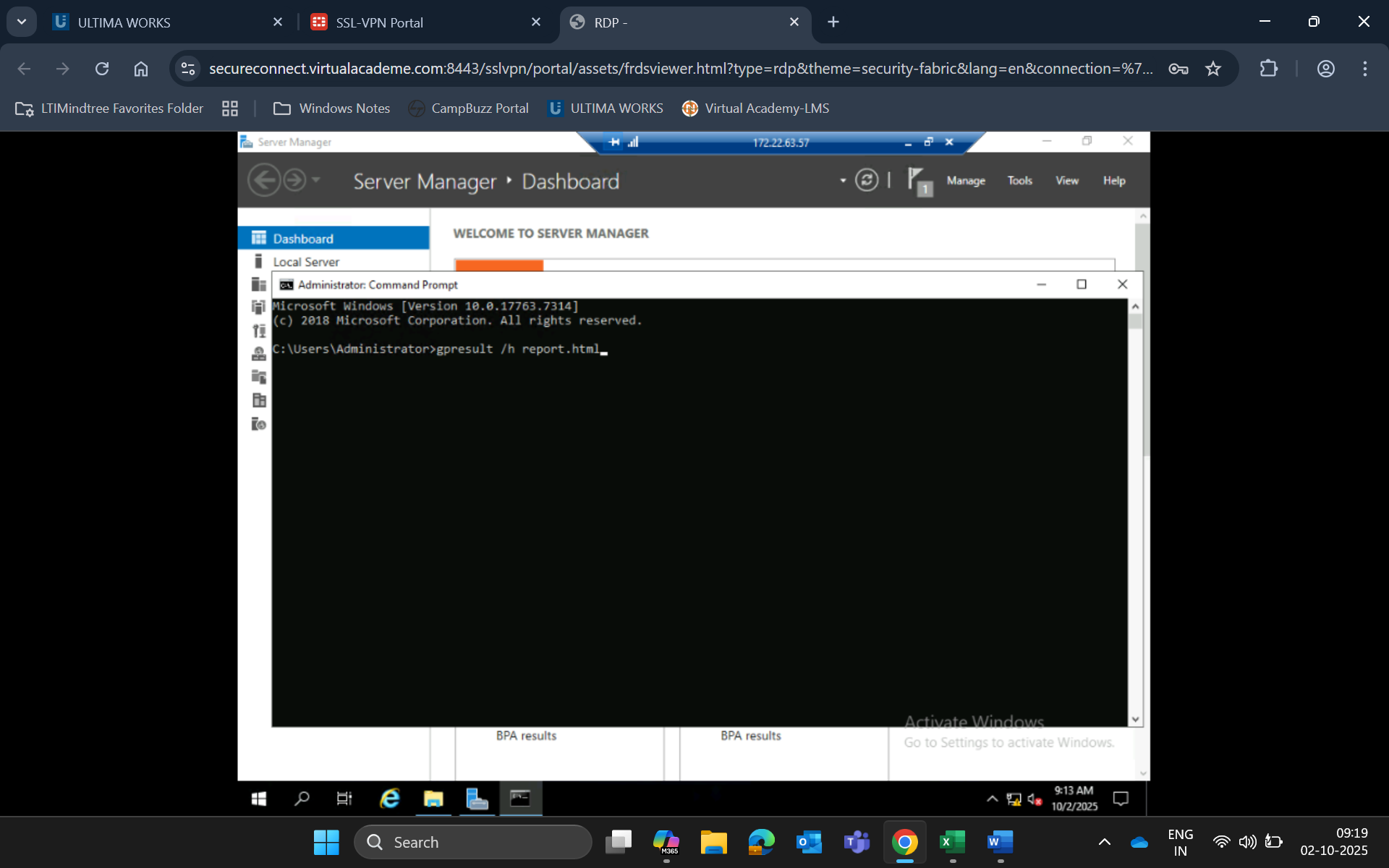
Your manager asked you to use Group Policy to implement standardized security settings to lock computer screens when users leave computers unattended for 10 minutes or more. You also have to configure a policy setting that will prevent access to certain programs on local computers. You configured Group Policy to lock computer screens when users leave computers unattended for 10 minutes or more. However, after some time, you were made aware that a critical application used by the Research engineering team fails when the screen saver starts. An engineer asked you to prevent the GPO setting from applying to any member of the Research security group. He also asked you to configure conference room computers to be exempt from corporate policy. However, you must ensure that the conference room computers use a 2-hour time out. Create the policies that you need to evaluate the RSoPs for users in your environment. Make sure to optimize the Group Policy infrastructure and verify that all policies are applied as they were intended. Objectives After completing this lab, you will be able to:

• Create and configure GPOs.







  
• Manage GPO scope.

* **Optimize Group Policy Infrastructure**
* **Avoid GPO duplication: Reuse settings where possible.**
* **Use WMI filters for targeting specific machines.**
* **Minimize GPO links: Link GPOs to OUs instead of the domain when possible.**
* **Document GPOs: Add descriptions for clarity.**

1. **Simulate AD Corruption and Perform Authoritative & Non-Authoritative Restore**
2. **Simulate AD Corruption:**

* Delete a critical AD object (e.g., an Organizational Unit or user) using Active Directory Users and Computers (ADUC) to simulate corruption.

1. **Non-Authoritative Restore:**
2. Boot the Domain Controller into **Directory Services Restore Mode (DSRM)**.
3. Use **Windows Server Backup** to restore the system state:
4. wbadmin start systemstaterecovery -version:<backup-version>
5. Reboot normally. The DC will replicate changes from other healthy DCs.
6. **Authoritative Restore:**
7. Boot into DSRM and restore the system state as above.
8. Open Command Prompt and run:
9. ntdsutil
10. activate instance ntds
11. authoritative restore
12. restore object "CN=DeletedUser,CN=Users,DC=domain,DC=com"

Or to restore an entire OU:

restore subtree "OU=Engineering,DC=domain,DC=com"

1. Exit and reboot normally. The restored object will replicate to other DCs.
2. **7. Document the Recovery Process and Verify Restored Objects**
3. **Recovery Documentation Template:**

|  |  |  |  |
| --- | --- | --- | --- |
| Step | Action | Tool Used | Outcome |
| 1 | Deleted OU 'Engineering' | ADUC | Simulated corruption |
| 2 | Booted into DSRM | OS Boot | Accessed recovery mode |
| 3 | Restored system state | wbadmin | Successful |
| 4 | Performed authoritative restore | ntdsutil | OU restored |
| 5 | Verified replication | ADUC / repadmin | Verified restored objects |

1. **Verification:**

* Use **Active Directory Users and Computers (ADUC)** to confirm restored objects.
* Run the following command to verify replication:
* repadmin /showrepl

1. **8. Configure and Apply Fine-Grained Password Policies (FGPP)**
2. **Steps to Configure FGPP:**
3. Open **Active Directory Administrative Center (ADAC)**.
4. Navigate to:  
   System → Password Settings Container
5. Click **New → Password Settings** and configure:
   * **Name**: EngineeringPolicy
   * **Precedence**: (Lower number = higher priority)
   * **Password length**, **complexity**, **history**, **lockout settings**, etc.
   * **Apply to**: Add specific users or groups (e.g., EngineeringGroup)