Project Title: Windows Defender Policy Deployment via Group Policy (GPO)

Name: Chandrakant Singh

Date: January 22, 2026

1. Executive Summary

The objective of this project was to establish a centralized Active Directory environment to enforce security baselines across network endpoints. Using Windows Server 2022 and Windows 10 Enterprise, I successfully deployed a Group Policy Object (GPO) that prevents users from disabling Windows Defender Real-time Protection and enables cloud-delivered protection.

2. Environment Configuration

I set up a virtualized lab environment with the following specifications:

- **Network:** Isolated Private Network (LAN Segment: "ADLAB") with Static IP addressing.
- **Domain Controller (Server):**
    - **OS:** Windows Server 2022 Standard (Desktop Experience)
    - **Hostname:** DC01
    - **IP Address:** 192.168.10.2
    - **Role:** AD DS, DNS
- **Client Workstation:**
    - **OS:** Windows 10 Enterprise
    - **Hostname:** Client01
    - **IP Address:** 192.168.10.10
    - **DNS:** Pointing to 192.168.10.2 (DC01)

3. Implementation Steps

Step 1: Domain Configuration

- Promoted DC01 to a Domain Controller for the new forest corp.local.
- Configured the Windows 10 client network adapter to communicate with the server.
- Joined Client01 to the corp.local domain and verified the computer account in Active Directory Users and Computers (ADUC).

Step 2: Policy Creation

- Launched **Group Policy Management Console (GPMC)** on DC01.
- Created a new GPO named **"Defender_Policy"** and linked it to the domain root (corp.local).
- Navigated to the following path: Computer Configuration > Policies > Administrative Templates > Windows Components > Microsoft Defender Antivirus

Step 3: Security Settings Configured I configured the following specific registry values via the GPO:

1. **Real-time Protection:** Set "Turn off real-time protection" to **Disabled**. (This enforces protection to be **ON**).
2. **MAPS (Cloud Protection):** Set "Join Microsoft MAPS" to **Enabled** (Advanced MAPS).
3. **Sample Submission:** Set "Send file samples" to **Enabled** (Safe samples only).

4. Verification & Testing

To validate the deployment, I performed the following tests on the client machine:

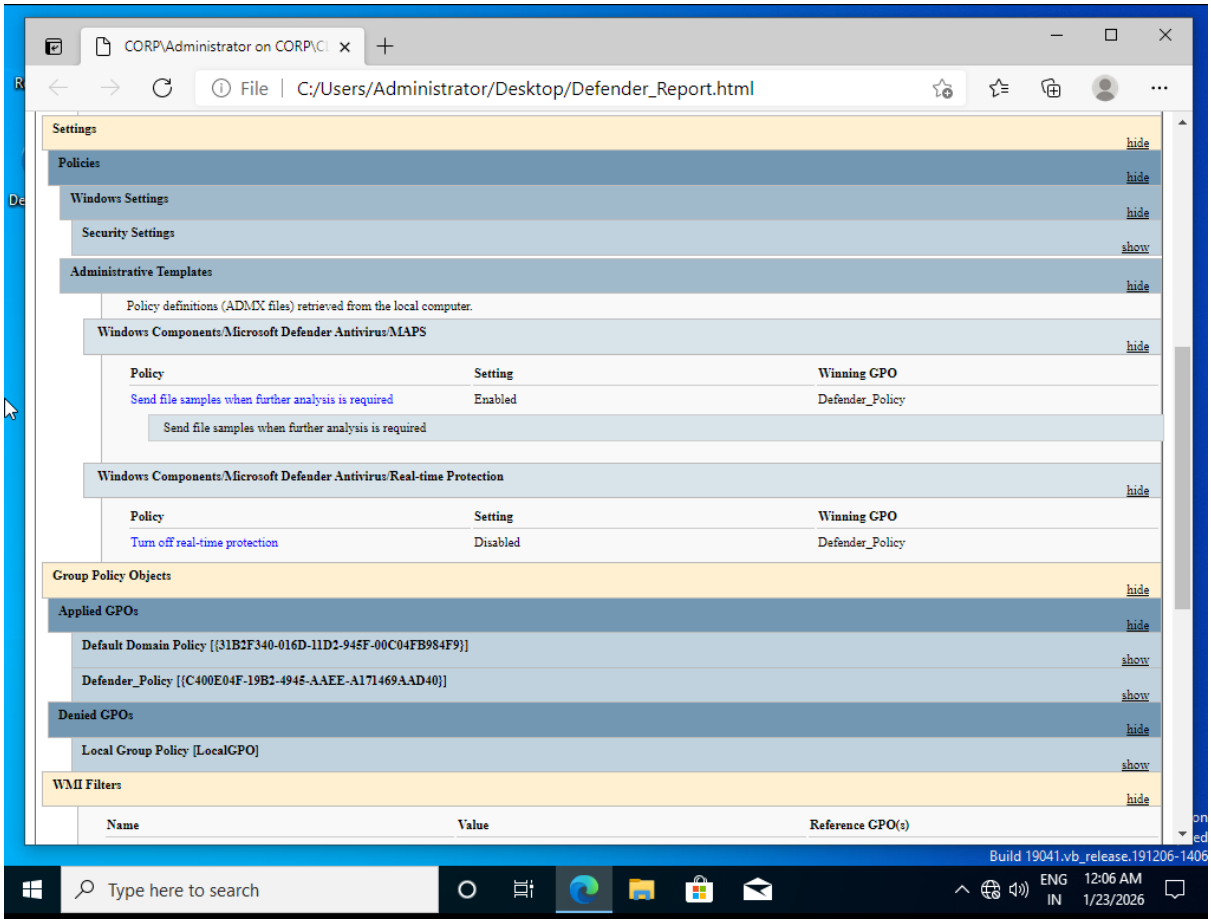
1. Logged in as CORP\Administrator.
2. Executed gpupdate /force in Command Prompt to pull the latest policies.
3. Generated a policy report using gpresult /h report.html.
4. **Result:** The report confirmed that "Defender_Policy" was the "Winning GPO."
5. **Visual Check:** Opened Windows Security settings and verified that the "Real-time protection" toggle was greyed out and displayed the message: "This setting is managed by your administrator."

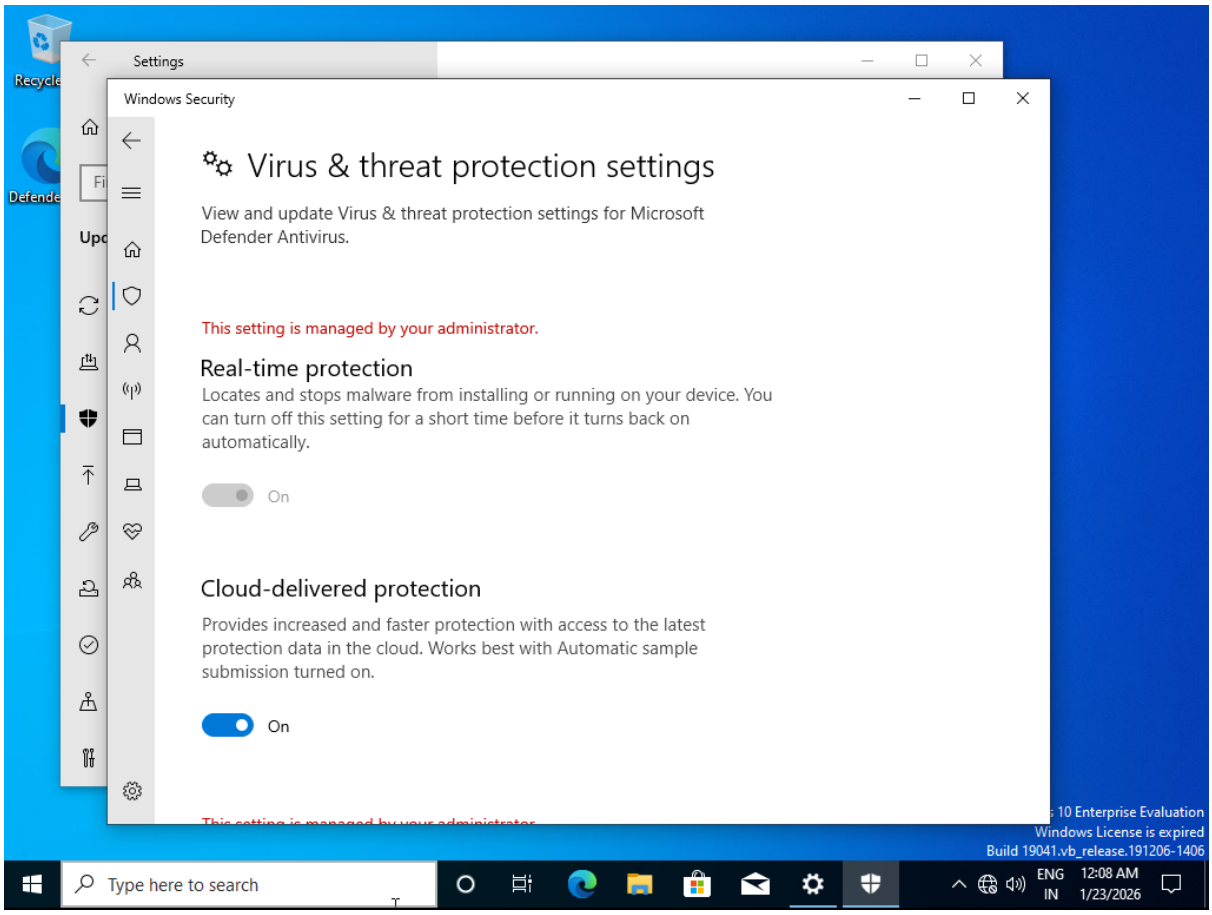
5. Challenges & Troubleshooting

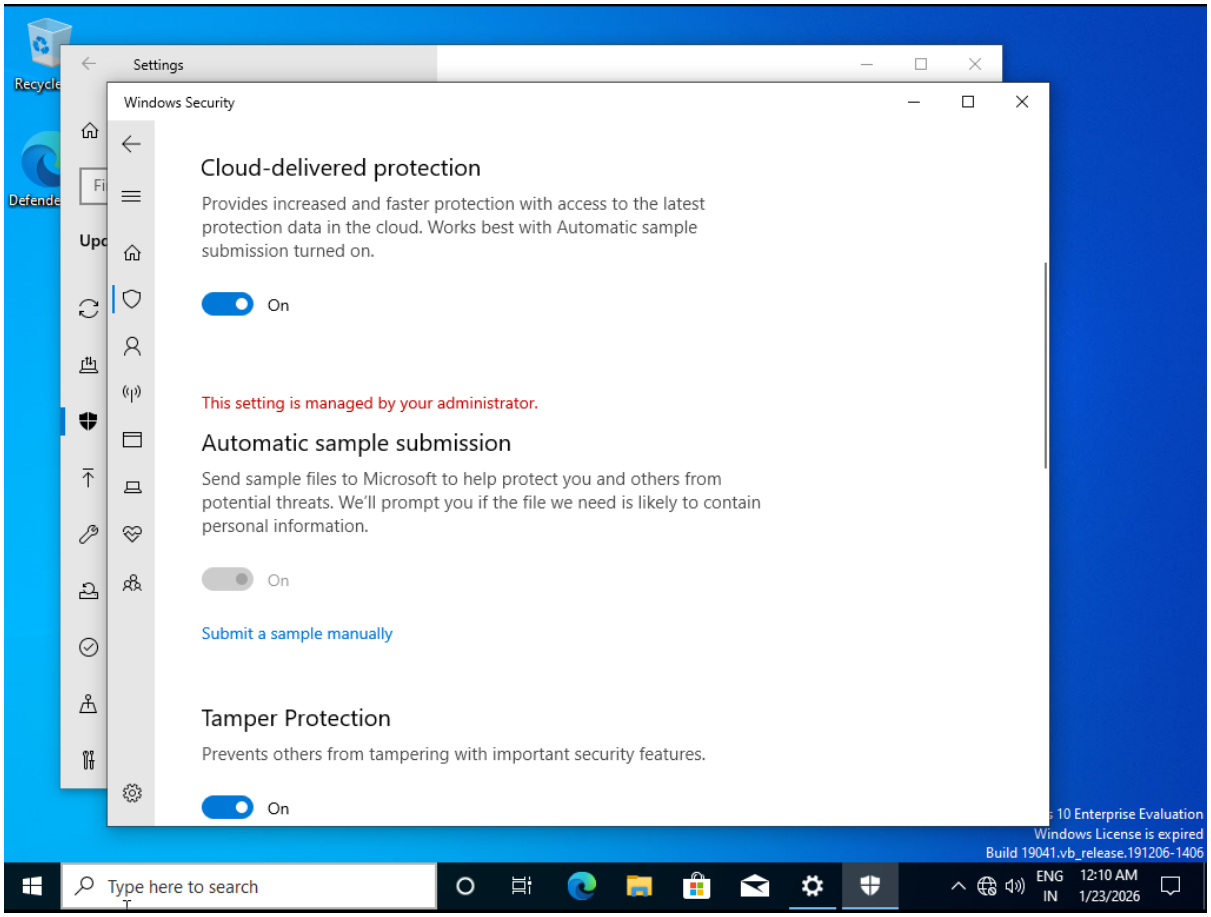
- **Issue:** Initially, the client could not ping the Domain Controller.
- **Resolution:** I verified that both VMs were on the same "LAN Segment" in VMware settings and confirmed the Client's DNS server was pointing to the Server's IP (192.168.10.2).
- **Issue:** VMware automated installation caused a "Floppy Drive" error.
- **Resolution:** I removed the autoinst.flp floppy drive from the VM hardware settings to allow the manual installation to proceed.

6. Evidence

See attached screenshots below showing the Group Policy Management Editor and the Client GPResult HTML report.


CORP\Administrator on CORP\C
File | C:/Users/Administrator/Desktop/Defender_Report.html
Settings
hide
Policies
hide
Windows Settings
hide
Security Settings
show
Administrative Templates
hide
Policy definitions (ADMX files) retrieved from the local computer.
Windows Components/Microsoft Defender Antivirus/MAPS
hide
Policy
Setting
Winning GPO
Send file samples when further analysis is required
Enabled
Defender_Policy
Send file samples when further analysis is required
Windows Components/Microsoft Defender Antivirus/Real-time Protection
hide
Policy
Setting
Winning GPO
Turn off real-time protection
Disabled
Defender_Policy
Group Policy Objects
hide
Applied GPOs
hide
Default Domain Policy [{31B2F340-016D-11D2-945F-00C04FB984F9}]
show
Defender_Policy [{C400E04F-19B2-4945-AAEE-A171469AAD40}]
show
Denied GPOs
hide
Local Group Policy [LocalGPO]
show
WMI Filters
hide
Name
Value
Reference GPO(s)
Build 19041.vb_release.191206-1406
Type here to search
ENG
IN
12:06 AM
1/23/2026


Settings
Windows Security
Virus & threat protection settings
View and update Virus & threat protection settings for Microsoft Defender Antivirus.
This setting is managed by your administrator.
Real-time protection
Locates and stops malware from installing or running on your device. You can turn off this setting for a short time before it turns back on automatically.
On
Cloud-delivered protection
Provides increased and faster protection with access to the latest protection data in the cloud. Works best with Automatic sample submission turned on.
On
10 Enterprise Evaluation
Windows License is expired
Build 19041.vb_release.191206-1406
Type here to search
ENG
IN
12:08 AM
1/23/2026


Settings
Windows Security
Cloud-delivered protection
Provides increased and faster protection with access to the latest protection data in the cloud. Works best with Automatic sample submission turned on.
On
This setting is managed by your administrator.
Automatic sample submission
Send sample files to Microsoft to help protect you and others from potential threats. We'll prompt you if the file we need is likely to contain personal information.
On
Submit a sample manually
Tamper Protection
Prevents others from tampering with important security features.
On
Type here to search
ENG
IN
12:10 AM
1/23/2026