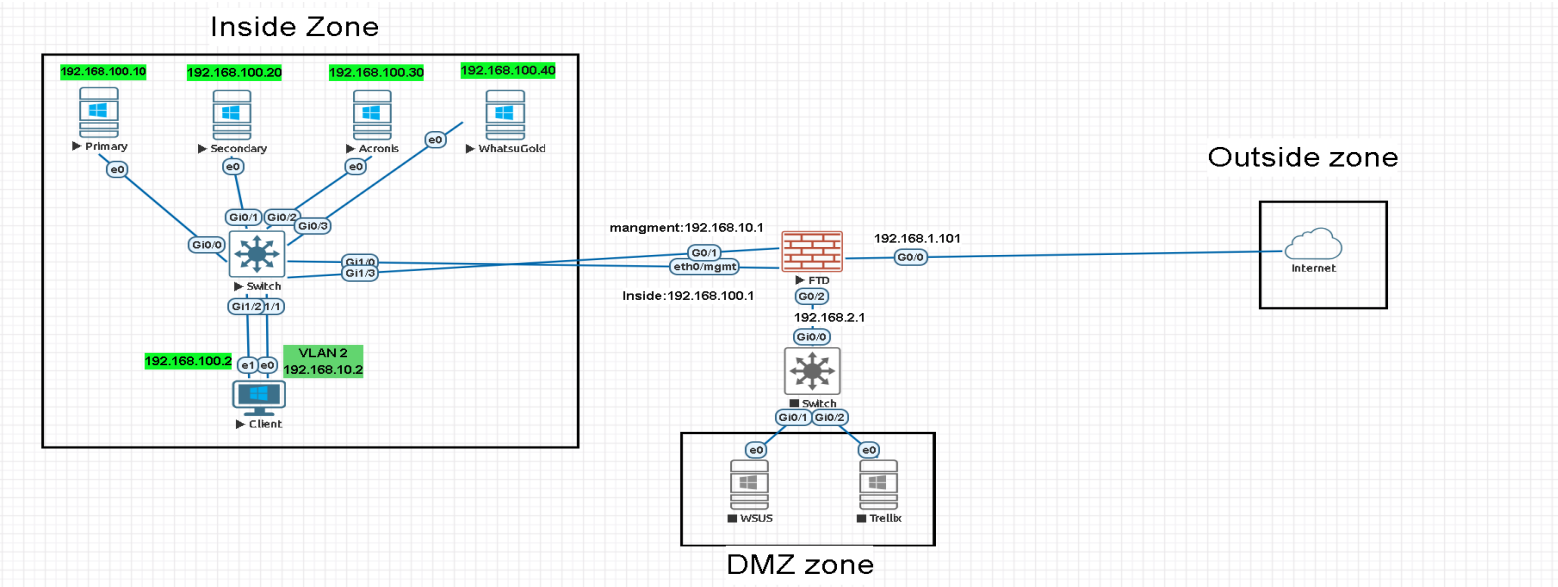
Abdelrhman nabil
OT cybersecurity engineer



There are some changes happened while I'm configuring so take only the concept and enhance it

Zone	Purpose	Example IP Range	Internet Access
Inside Zone	Internal network for AD, File, and Acronis servers; business and OT management systems	192.168.100.0/24	No direct Internet access
DMZ Zone	Intermediate zone for update, backup, and endpoint management servers	192.168.2.0/24	Limited Internet access (for updates)
Outside Zone	Internet	192.168.1.0/24 (via FTD outside)	Internet uplink
Management Zone	Out-of-band management of the FTD and FMC	192.168.10.0/24	Only for admins

FTD sits **between Inside, DMZ, and Outside zones**, enforcing security policies and NAT rules.

Inside Zone (192.168.100.0/24)

Purpose

This zone hosts your **critical internal services**, including Active Directory, backups, and local management tools.
It represents **Purdue Level 4** in an OT context (business and site-level IT).

Abdelrhman nabil
OT cybersecurity engineer

Hosts

Host	Role	IP	Notes
Primary DC	Main Domain Controller	192.168.100.10	Handles AD DS, DNS, GPOs
Secondary DC	Additional Domain Controller	192.168.100.20	Replicates with Primary
Acronis	Backup Server	192.168.100.30	For backup and recovery process
Client PC	Domain-joined workstation	VLAN 2 — 192.168.10.2	Used by users/admins

Traffic Rules (to define in FMC)

- Inside → DMZ: **Allow only required ports**
- Inside → Internet: **DENY ALL**
- Inside → FTD management (192.168.10.1): **Allow only admins**

DMZ Zone (192.168.2.0/24)

Purpose

DMZ hosts servers that **act as intermediaries** between your internal environment and the Internet.
They allow patching, updates, and backup synchronization **without exposing the inside directly to the Internet.**

Hosts

Host	Role	IP	Notes
WSUS Server	Windows updates	192.168.2.x	Syncs with Microsoft update servers via Internet
Trellix Server	Endpoint protection console	192.168.2.x	Agents from Inside connect to this server

Traffic Rules

- DMZ → Internet: **Allow** only required traffic
    - WSUS → Microsoft Update

    - Trellix → Vendor update servers
- Inside → DMZ: **Allow**
    - Clients/DCs → WSUS
    - Agents → Trellix (agent communication port)
- DMZ → Inside: **Deny all unless specifically required**

Outside Zone (192.168.1.0/24)

Purpose

Represents the **Internet or external WAN**.
Only the **FTD outside interface (192.168.1.101)** connects here.

Traffic Rules

- FTD NATs DMZ outbound traffic to Internet.
- Inside zone has **no Internet route**; all traffic must go via approved DMZ services.

Management Network (192.168.10.0/24)

Purpose

Dedicated network for **FTD/FMC and admin access**.
Separates management from production data and prevents attackers from pivoting into management interfaces.

Host	Role	IP	Notes
FTD Management Interface	eth0 / mgmt.	192.168.10.1/30	For FMC connection and SSH/HTTPS admin
Admin Workstation / FMC	Management access point	192.168.10.2/30	-----

Abdelrhman nabil
OT cybersecurity engineer

Security Summary (Defense in Depth)

Control	Implementation
Segmentation	Clear separation between Inside, DMZ, and Outside
Least privilege	ACLs permit only specific service ports
No direct Inside–Internet flow	Inside depends on DMZ for updates and AV
Inspection	FTD inspects DMZ↔Internet flows
AD hardening	AD confined to Inside zone
Backup resilience	Acronis & Trellix

The design follows Purdue segmentation principles by keeping **Level 3 (Inside)** separated from Internet via a **3.5 DMZ**.

Condfigure Vlan for management:

#enable

#conf t

#interface range gi0/0-1

#switchport mode access

#switchport access vlan 10

Configuring the Primary and Secondary (Addtional) DCs

Domain Controllers Setup

Server	Role	IP	DNS
Primary	**Domain Controller (DC)**	192.168.100.10	127.0.0.1
Secondary	**Additional Domain Controller (ADC)**	192.168.100.20	192.168.100.10

Abdelrhman nabil
OT cybersecurity engineer

Both servers are in the **Inside Zone**, isolated from the Internet.

Set static IP for Primary:

- IP: 192.168.100.10
- Subnet mask: 255.255.255.0
- Default gateway: 192.168.100.1
- DNS: 127.0.0.1

Set static IP for Additional:

- IP: 192.168.100.20
- Subnet mask: 255.255.255.0
- Default gateway: 192.168.100.1
- DNS: 192.168.100.10

Install the Active Domain Services role in the primary and promote it as New forest and proceed till it promoted and restarted then in the secondary first make it join the domain then promote it as additional server

Open **Server Manager**

Add **Active Directory Domain Services** role

Click **Promote this server to a domain controller**

Select:

- “Add a domain controller to an existing domain”
- Domain: Shadow.Project
- Supply: Shadow\Administrator credentials

Check:

- DNS Server
- Global Catalog

Leave “Read-Only Domain Controller” unchecked

Complete wizard → Reboot

Abdelrhman nabil
OT cybersecurity engineer

Verify Replication

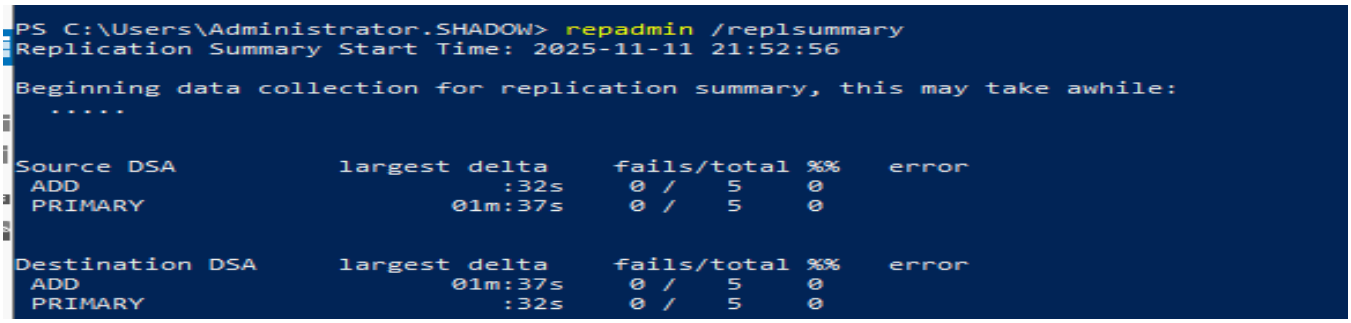
On **DC1**:

repadmin /showrepl

On **DC2**:

repadmin /replsummary

You should see:



Also, open **ADUC** on either DC → both should show each other under *Domain Controllers OU.*

Verify DNS Replication

1. Open **DNS Manager** on both DC1 and DC2.
2. Under **Forward Lookup Zones**, ensure shadow.project is identical.
3. Test from any client:
4. nslookup primary.shadow.project
5. nslookup add.shadow.project

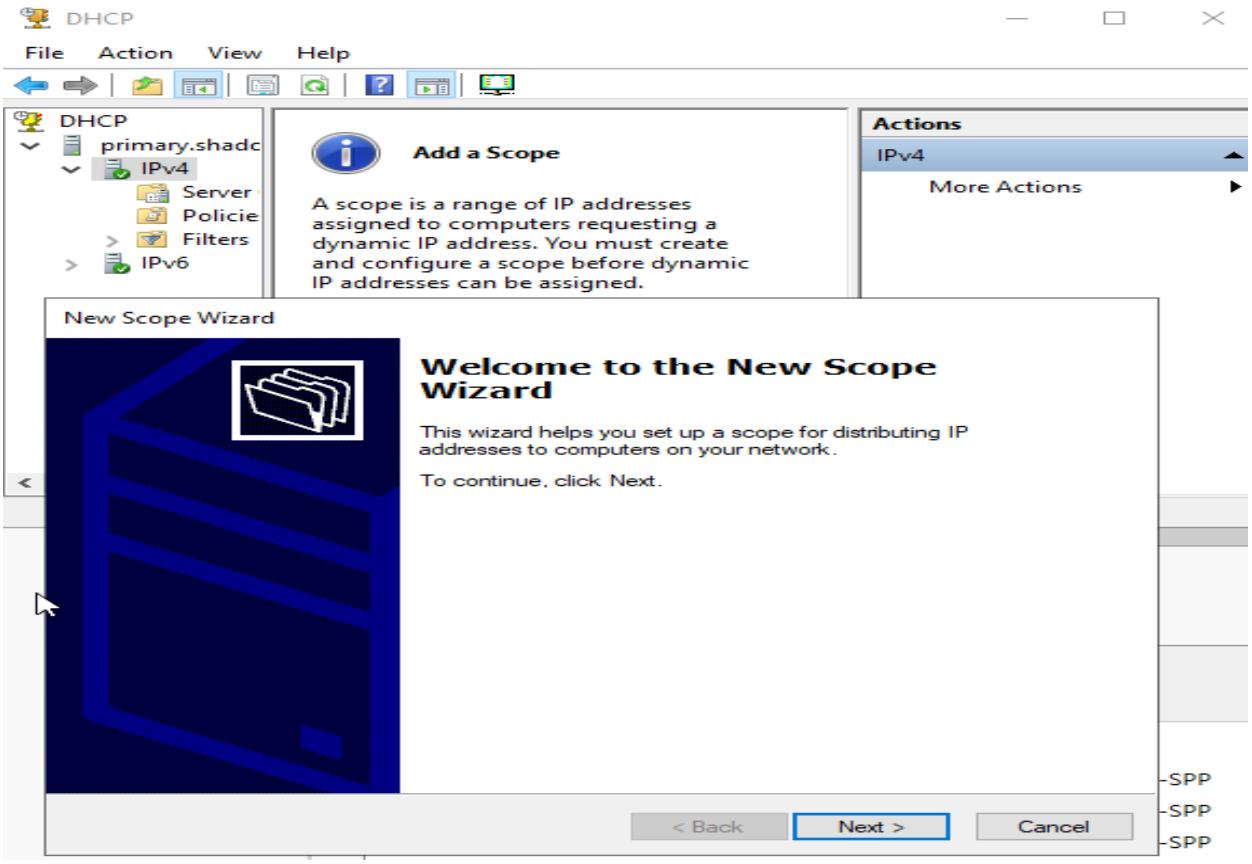
Both should resolve correctly.

Abdelrhman nabil
OT cybersecurity engineer

Configuring the DHCP

It's not recommended in the real enviroments give each A static IP but we just practice

first add the DHCP role and install it , then go to The DHCP service from Tools and create a scoop



DHCP Configuration — Inside Zone

(Primary DC: 192.168.100.10 | Secondary DC: 192.168.100.20)

Goal

- **Primary DC (DC1) = main DHCP server for 192.168.100.0/24**
- **Secondary DC (DC2) = DHCP failover partner**
- **DHCP will automatically provide IPs to:**
  - **Inside clients (e.g. your Windows 7 workstation)**
  - **Possibly future OT engineering stations**
- **Both servers will have synchronized lease and reservation info**

Abdelrhman nabil
OT cybersecurity engineer

Step 1 — Install DHCP Role on Both DCs

Step 2 — Authorize DHCP in Active Directory

You must authorize DHCP servers so they can lease IPs in the domain.

On DC1:

1. **Open Server Manager → Tools → DHCP**
2. **Right-click on your server → Authorize**
3. **Wait a few seconds → refresh → status changes to "Authorized"**

On DC2:

Repeat the same step.

Step 3 — Create DHCP Scope on Primary DC (DC1)

1. **In DHCP Console → expand your server → right-click IPv4 → New Scope**
2. **Configure as follows:**

Parameter	Value
Scope Name	Inside_Clients
Start IP Address	192.168.100.50
End IP Address	192.168.100.200
Subnet Mask	255.255.255.0
Default Gateway	192.168.100.1 *(FTD inside interface)*
DNS Server	192.168.100.10, 192.168.100.20
Lease Duration	8 days (default)
Activate Scope	Yes

This will serve any new inside client (like your VLAN 2 workstation).

Abdelrhman nabil
OT cybersecurity engineer

Step 4 — Configure DHCP Failover with Secondary (DC2)

On DC1:

1. **In DHCP console → IPv4 → Right-click "Inside_Clients" → Configure Failover**
2. **Select the scope → Next**
3. **In the Partner Server field → Enter:**
4. **Add.Shadow.Project**

(or IP 192.168.100.20)

5. **Select:**
   - **Mode: Load balance or Hot standby**
     - **Recommended: Hot Standby**
6. **Set:**
   - **Primary server: DC1**
   - **Secondary server: DC2**
   - **Shared Secret: (e.g. OTlab123!)**
7. **Finish wizard.**

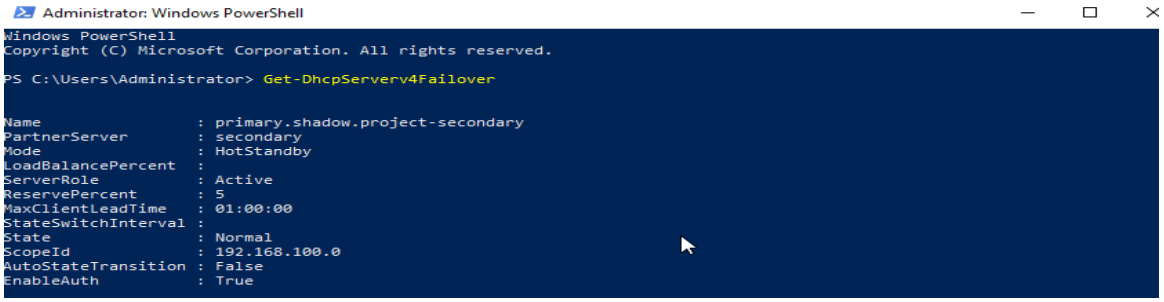
This replicates DHCP leases and config between both servers.

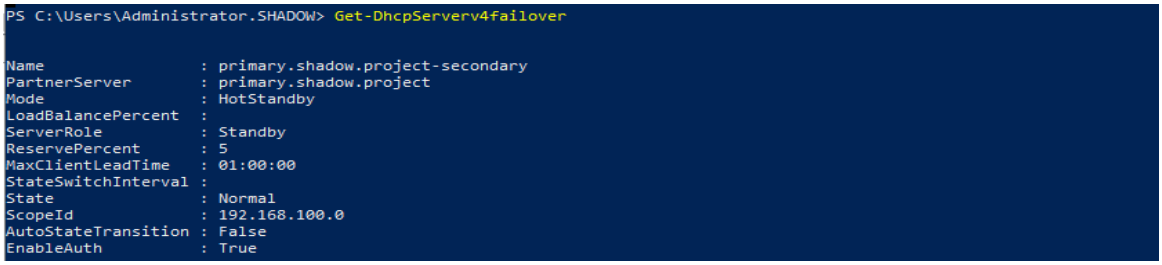
Step 5 — Verify Replication

On both servers:

PowerShell:

Check that the Inside_Clients scope appears on DC2 as well (automatically replicated).





Abdelrhman nabil
OT cybersecurity engineer

Active Directory Organizational Units (OU) and Groups Design

Design Principles (Professional Best Practice)

Goal	Description
Separation of assets	Servers and clients are placed in separate OUs for targeted GPOs
Delegation-ready	Admins can manage clients without touching servers
Role-based groups	Admin and non-admin users organized in security groups
Scalable	Easy to expand (e.g., add DMZ servers or OT operator workstations later)

Target Structure

Shadow.Project

```
├── Clients
|   ├── Admins
|   |   ├── OT_Admins
|   |   └── IT_Admins
|   └── Non-Admins
|       ├── Operators
|       └── Engineers
```

let's Configure the Hardening GPOs

1- disable CMD and Powershell on the non-Admins:

Create the gpo and link it to the non-admin OU and edit it as follows

Go to:

User Configuration → Administrative Templates → System

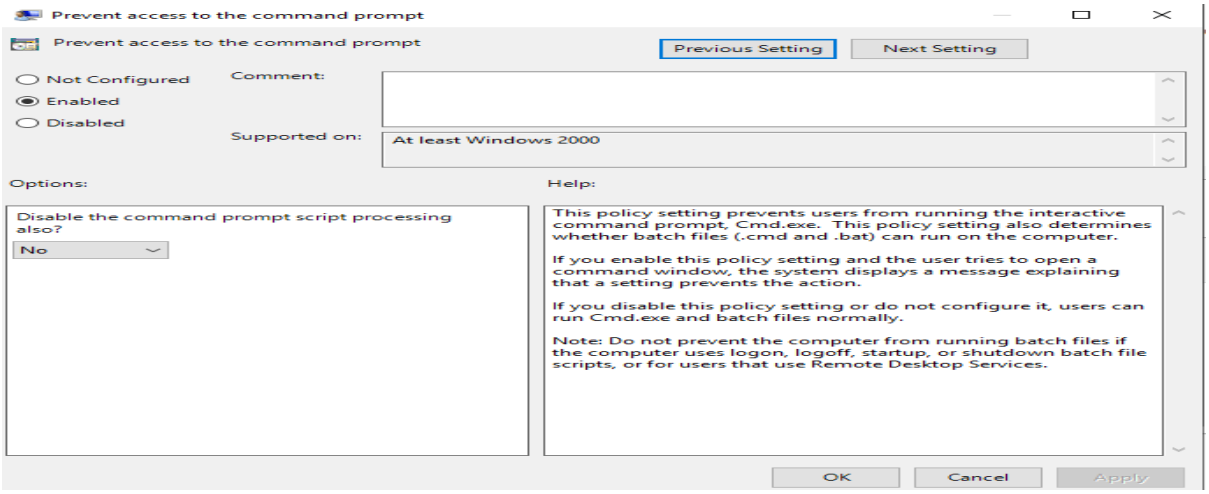
Find the policy:

Prevent access to the command prompt

Abdelrhman nabil
OT cybersecurity engineer

Set it to:

- **Enabled**
- **And select: no for “running script at logon” (if we want to open application like calc)**

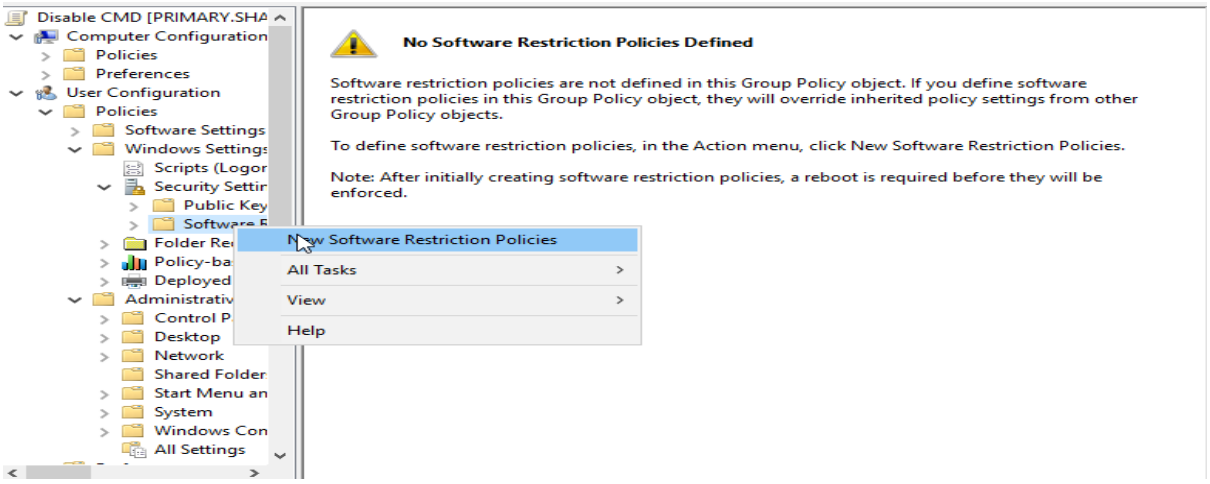


THEN let's disable powershell

Use Software Restriction Policies (SRP)

User Configuration → Windows Settings → Security Settings → Software Restriction Policies

if no SRP exists, right-click “Software Restriction Policies” → New Software Restriction Policies



Then under Additional Rules, right-click → New Path Rule

1. **Path:**
2. **%SystemRoot%\System32\WindowsPowerShell**

Security level: Disallowed

3. **Add another rule:**
4. **%SystemRoot%\SysWOW64\WindowsPowerShell**

Security level: Disallowed

Effect: Blocks PowerShell from being executed for affected users.

Or you can use another way by using AppLocker:

If you have Windows 10/11 Pro or Enterprise, you can use AppLocker instead of SRP:

Computer Configuration → Windows Settings → Security Settings → Application Control Policies → AppLocker → Executable Rules

Create a rule that denies PowerShell.exe and pwsh.exe for Non-Admin users.

2-Password and Account policies

Computer Config → Windows Settings → Security Settings → Account Policies → Password Policy

Computer Config → Windows Settings → Security Settings → Account Policies → Account Policy

Make them as follow and if you wanna add more do it but link it to domain as whole :

Enforce password history	1 passwords remembered
Maximum password age	Not Defined
Minimum password age	Not Defined
Minimum password length	12 characters
Minimum password length audit	Not Defined
Password must meet complexity requirements	Enabled
Store passwords using reversible encryption	Not Defined

Account lockout duration	30 minutes
Account lockout threshold	3 invalid logon attempts
Reset account lockout counter after	30 minutes

3-Prevent registery editing tools

User Config → Admin Templates → System → "Prevent access to registry editing tools"

4- Prevent access to Control Panel and PC settings

User Config → Admin Templates → Control Panel

Abdelrhman nabil
OT cybersecurity engineer

5-Disable USBs

Computer Configuration → Administrative Templates → System → Removable Storage Access

Configure the following policies:

Policy	Setting	Description
All Removable Storage classes: Deny all access	Enabled	Blocks all read/write/execute to removable storage
Removable Disks: Deny execute access	Enabled	Blocks running programs from USB
Removable Disks: Deny read access	Enabled	Prevents reading files from USB
Removable Disks: Deny write access	Enabled	Prevents writing files to USB

You can choose whether to "Deny all" or just "Deny write" depending on how strict you want to be.

6-Disable Wi-Fi Adapters via GPO

Option A — Disable driver installation for Wi-Fi devices

1. **On your Primary DC, open:**
2. **gpmc.msc**
3. **Edit or create a GPO for Non-Admin clients (for example, Network_Hardening_NonAdmins)**
4. **Navigate to:**
5. **Computer Configuration → Administrative Templates → System → Device Installation → Device Installation Restrictions**
6. **Enable:**
    - **Prevent installation of devices that match any of these device IDs**
    - **Add the hardware IDs of Wi-Fi adapters.**

Abdelrhman nabil
OT cybersecurity engineer

To find IDs:

1. **On a client, open Device Manager → Network Adapters**
2. **Right-click your Wi-Fi adapter → Properties → Details → Hardware IDs**
3. **Copy something like:**
4. **PCI\VEN_8086&DEV_24FD&SUBSYS_00348086**
5. **Add it to the policy.**
6. **Then enable:**
   - **Prevent installation of removable devices**
   - **Prevent installation of devices not described by other policy settings**
7. **Apply and run:**
8. **gpupdate /force**

Result: Windows will prevent new Wi-Fi drivers from being installed or re-enabled.

Option B — Disable WLAN AutoConfig service (stronger)

1. **Go to:**
2. **Computer Configuration → Windows Settings → Security Settings → System Services**
3. **Find WLAN AutoConfig**
4. **Set it to:**
   - **Startup mode: Disabled**
   - **Define this policy setting: Checked**

Effect: Wi-Fi management service is disabled, so even if the adapter exists, it won't connect.

Disable Bluetooth Adapters via GPO

Option A — Disable driver installation

Repeat the same steps:

Computer Configuration → Administrative Templates → System → Device Installation → Device Installation Restrictions

Add hardware IDs of Bluetooth adapters from:

Abdelrhman nabil
OT cybersecurity engineer

Device Manager → Bluetooth → <Adapter> → Details → Hardware IDs

Option B — Disable Bluetooth Support Service

1. **Go to:**
2. **Computer Configuration → Windows Settings → Security Settings → System Services**
3. **Find Bluetooth Support Service**
4. **Set it to:**
    - **Startup mode: Disabled**

Option C — Disable via Administrative Templates

Navigate to:

Computer Configuration → Administrative Templates → Windows Components → Bluetooth

Set:

- **Turn off the Bluetooth advertising**
- **Turn off Bluetooth devices**
- **Turn off Bluetooth file transfer**

All → Enabled

7-desktop and start menu shows nothing

User Configuration → Administrative Templates → Desktop

Then set the following:

Setting	Path	Action
Hide and disable all items on the desktop	Desktop	Enabled
Do not add shares of recently opened documents to Network Locations	Desktop	Enabled (optional)
Remove Recycle Bin icon from desktop	Desktop	Enabled

Abdelrhman nabil
OT cybersecurity engineer

Lock Down the Start Menu

Go to:

User Configuration → Administrative Templates → Start Menu and Taskbar

Setting	Path	Action
Setting	Path	Action
Remove access to the context menus for the taskbar	Start Menu and Taskbar	Enabled
Lock all taskbar settings	Start Menu and Taskbar	Enabled

8-Opens the calculator automatically or (Replace calc.exe with your HMI, SCADA client, or operator console app.)

Go to:

User Configuration → Windows Settings → Scripts (Logon/Logoff)

Double-click Logon, then click Add → Browse.

In the logon scripts folder, click Show Files, then create a new script file named:

open_calc.bat

Inside open_calc.bat, add this line:

start calc.exe

9- remove search bar

Policy location: User Configuration -> Preferences -> Windows Settings -> Registry

Policy settings:

Anction: Update
Hive: HKEY_CURRENT_USER
Key Path: Software\Microsoft\Windows\CurrentVersion\Search
Value Name: SearchboxTaskbarMode
Value Type: REG_DWORD
Value Data: 0

Abdelrhman nabil
OT cybersecurity engineer

You can assign more and more GPOs tell you reach the KIOSK mode but defiantly be

Careful while you assigning to not affect another process or function

FTD Configurations:

It's just an FTD so we going to manage it locally by FDM and defiantly in Routed mode to route between different zones

The interface gonna be configured as follows

Topology Overview

Interface	Zone	IP	Purpose
Mgmt (eth0)	Management	192.168.10.1/32	For FMC communication & FTD management only
g0/0	Outside	192.168.1.200/24	Internet access (via cloud or router)
g0/1	Inside	192.168.100.1/24	Internal AD, clients, Acronis,etc.
g0/2	DMZ	192.168.2.1/24	DMZ servers (WSUS, Trellix)

NAME	LOGICAL NAME	STATUS	MODE	IP ADDRESS	STANDBY ADDRESS	MONITOR FOR HA	ACTIONS
GigabitEthernet0/0	outside		Routed	192.168.1.200 Static		Enabled	
GigabitEthernet0/1	inside		Routed	192.168.100.1 Static		Enabled	
GigabitEthernet0/2	dmz		Routed	192.168.2.1 Static		Enabled	
GigabitEthernet0/3			Routed			Enabled	
Management0/0	diagnostic		Routed			Enabled	

Then configure the DMZ zone the inside and outside gonna be configured by default from Object→security zones

Security Zones

3 objects

Filter

#	NAME	MODE	INTERFACES	ACTIONS
1	inside_zone	Routed	inside	
2	outside_zone	Routed	outside	
3	dmz_zone	Routed	dmz	

Then deploy this changes , and let's configure the Static Routes between Zones

Abdelrhman nabil
OT cybersecurity engineer

1 route

Filter

#	NAME	INTERFACE	IP TYPE	NETWORKS	GATEWAY IP	SLA MONITOR	METRIC	ACTIONS
1	to_internet	outside	IPv4	0.0.0.0/0	192.168.1.1		1	

Then Let's Configure the Access Control Policies (ACP):

#	NAME	ACTION	SOURCE			DESTINATION			APPLICATIONS	URLS	USERS		ACTIONS
			ZONES	NETWORKS	PORTS	ZONES	NETWORKS	PORTS					
1	inside_to_dmz	Allow	inside_zone	ANY	ANY	dmz_zone	ANY	ANY	ANY	ANY	ANY		
2	Inside_Outside_Rule	Block	inside_zone	ANY	ANY	outside_zone	ANY	ANY	ANY	ANY	ANY		
3	dmz_to_outside	Allow	dmz_zone	ANY	ANY	outside_zone	ANY	ANY	ANY	ANY	ANY		

Order	Source Zone	Destination	Action	Notes
1	INSIDE	DMZ	Allow	Allow AD servers to reach DMZ servers (Acronis/WSUS/Trellix)
2	INSIDE	OUTSIDE	Block	Inside has no internet access (per your requirement)
3	DMZ	OUTSIDE	Allow	Allow DMZ servers (Acronis, WSUS) to fetch updates from Internet
4	Default	Any	Block	Default deny all

Abdelrhman nabil
OT cybersecurity engineer

Let's configure the DMZ area :

Defitnly the WSUS and the Trellix gonna be in the DMZ BUT WHY:

Understand the Role of WSUS in Your OT Lab

- **WSUS = Windows Server Update Services.**
- **It downloads updates from Microsoft and distributes them to clients (in your Inside zone).**
- **So, it needs:**
  - **Internet access (OUTSIDE) → to sync updates.**
  - **Access to Inside (INSIDE zone) → to deliver updates to domain clients.**

That's *exactly* why you placed it in the DMZ — a *buffer zone* between internal OT assets and the Internet.

Perfect network design choice.

BUT ARE THEY GONNA JOIN THE DOMAIN

Compare the Two Approaches

Design	Domain-Joined WSUS	Standalone WSUS
Security posture	Higher risk: domain credentials exposed in DMZ	Lower risk: no domain trust exposure
Ease of management	Centralized GPOs and authentication	Must manually configure clients via registry or local GPO
Patching inside domain	Seamless via GPO	Needs registry-based WSUS target configuration
Access to Internet	Still possible via FTD	Same
Attack surface	Bigger (domain join extends AD trust boundary to DMZ)	Smaller (isolated system)

DO NOT domain-join servers in the DMZ unless absolutely necessary.

- **The DMZ is a *buffer zone*; it's expected to be probed, scanned, or attacked.**
- **If a DMZ server is domain-joined, a compromise can pivot directly into your Active Directory, which is at Purdue Level 3.**
- **In OT, this breaks the "conduit segmentation" principle (ISA/IEC 62443-3-3 SR 1.1 & SR 3.1).**

Abdelrhman nabil
OT cybersecurity engineer

So:

Best practice: keep WSUS in the DMZ as a standalone server, not joined to the domain.

Recommended Deployment Model

DMZ Zone

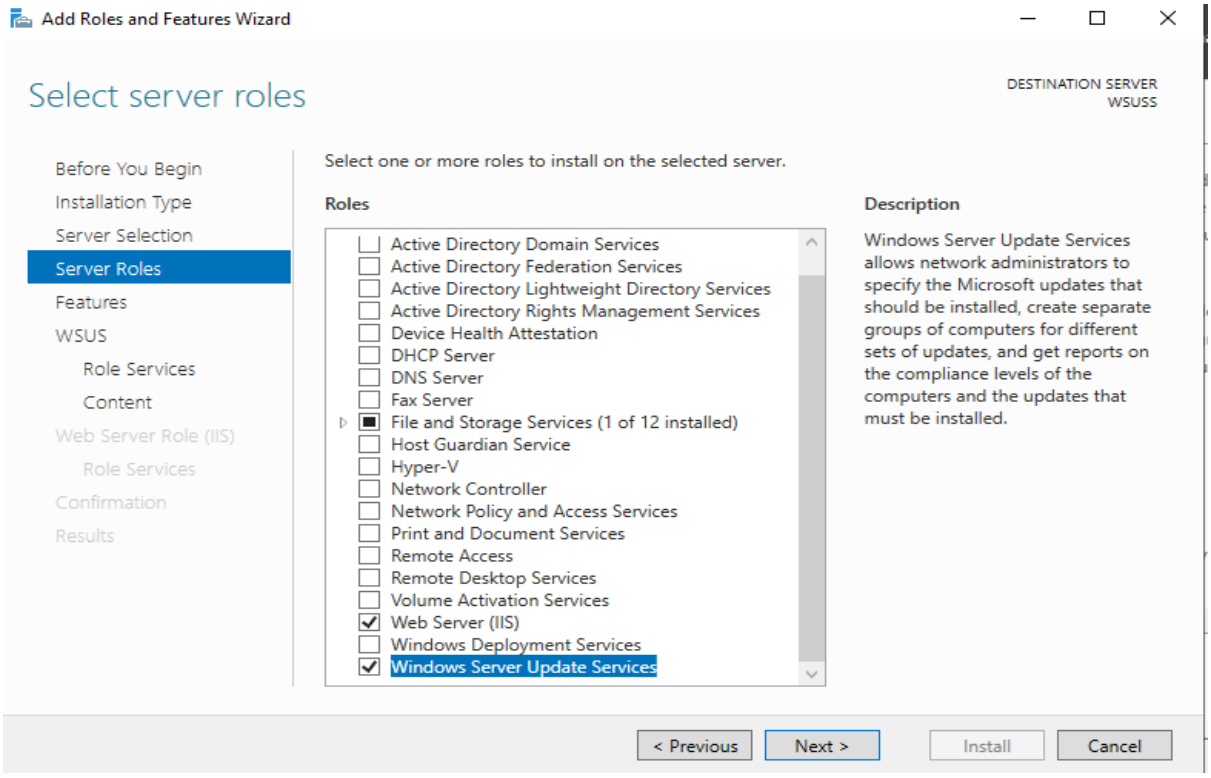
- **Server: WSUS01**
- **IP: 192.168.2.10**
- **Role: Standalone WSUS**
- **Internet Access: via FTD OUTSIDE (controlled)**
- **Inside Access: from clients/DCs**

Inside Zone

- **Domain: Shadow.Project**
- **AD/DC: 192.168.100.10 / 20**
- **Clients: Windows 7/10**
- **File Server: 192.168.100.x**
- **Policy: GPO directs clients to use http://192.168.2.10:8530 as WSUS.**

Configure WSUS for Standalone Mode

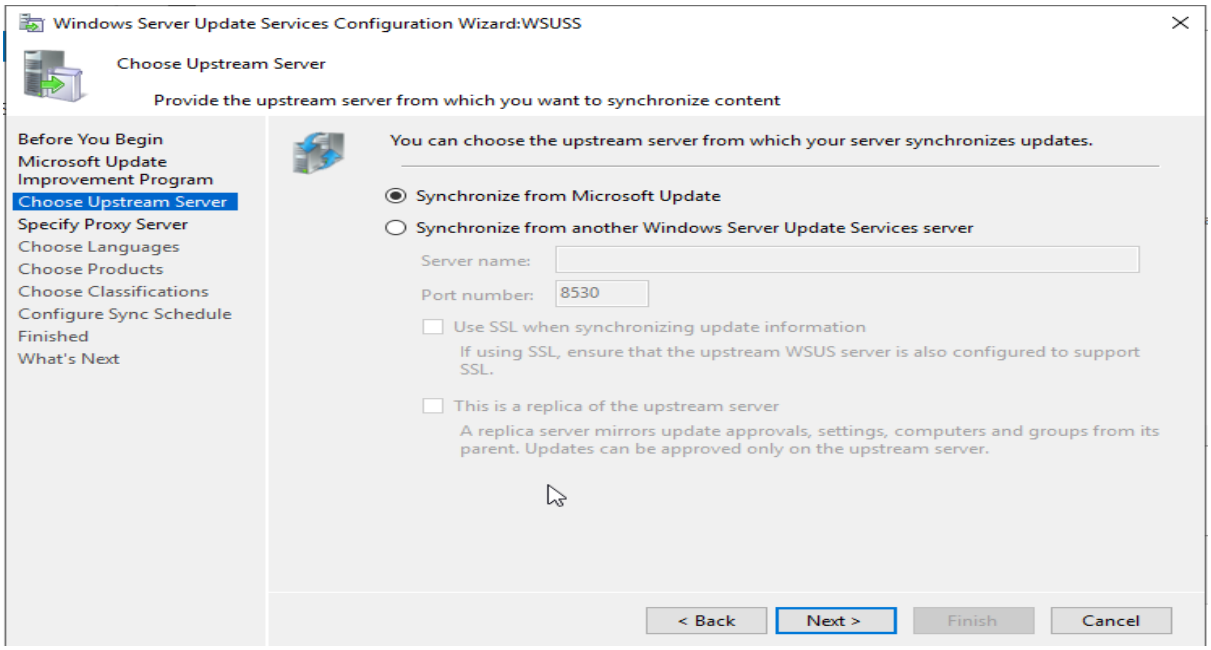
1. **Install WSUS on the DMZ server:**



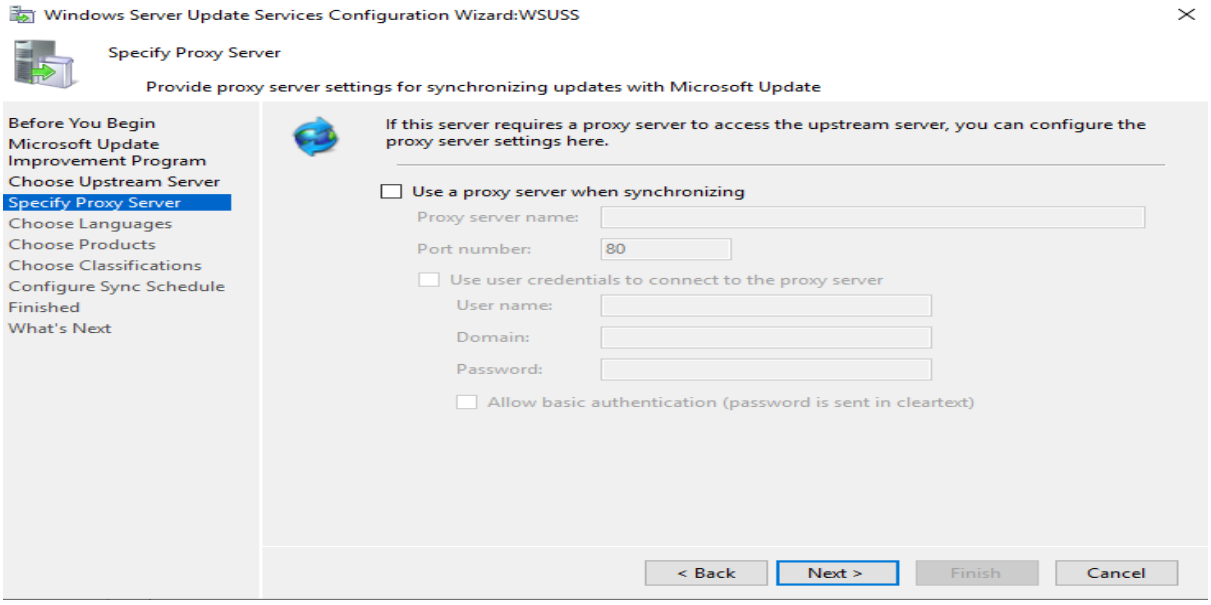
Abdelrhman nabil
OT cybersecurity engineer

During setup, choose:

- **“Synchronize from Microsoft Update”**
- **Storage path: D:\WSUS**
- **Port: 8530 (HTTP)**



This means if you want the updates form Microsoft or form another WSUS server located in different place



We will skip that cause the FTD is just Doing NAT and ACP not SSL INSPECTION OR CACHING so we gonna skip that , then you just need to specify the Updates you need and proceed and click finish .

Abdelrhman nabil
OT cybersecurity engineer

Just make sure you selected the right products and updates:

Options → Products and Classifications

Products Tab

Check only what you actually need (to avoid huge storage use):

- **Windows 10**
- **Windows 11 (if applicable)**
- **Windows Server 2019**
- **(Optional) Office, .NET Framework, etc.**

Then click OK.

b) Classifications Tab

Select at least:

- **Critical Updates**
- **Security Updates**
- **Definition Updates**
- **Updates**
  (You can add others like Feature Packs, Service Packs, Tools, etc.)

Click OK.

Force synchronization again

Now go to:

WSUS Console → Synchronizations → Synchronize Now

When it's done, check:

Updates → All Updates

You'll now see thousands of updates (initially "Not Approved").

Automatic Approval Rules

You can create auto-approval rules:

Options → Automatic Approvals

For example:

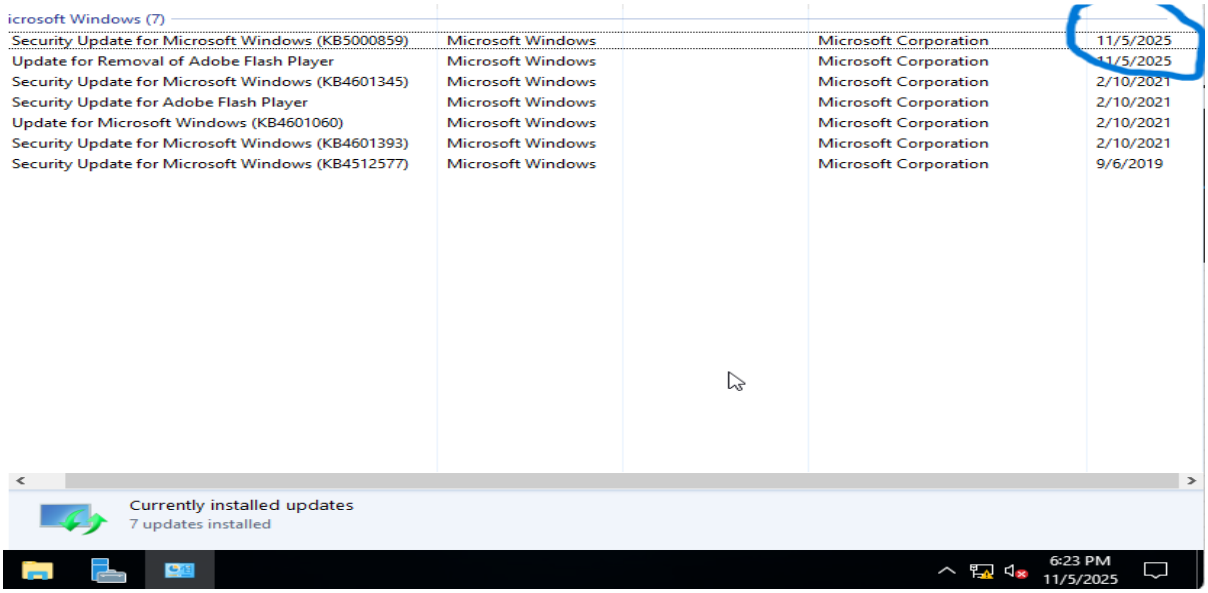
- **Automatically approve Critical and Security Updates for All Computers**

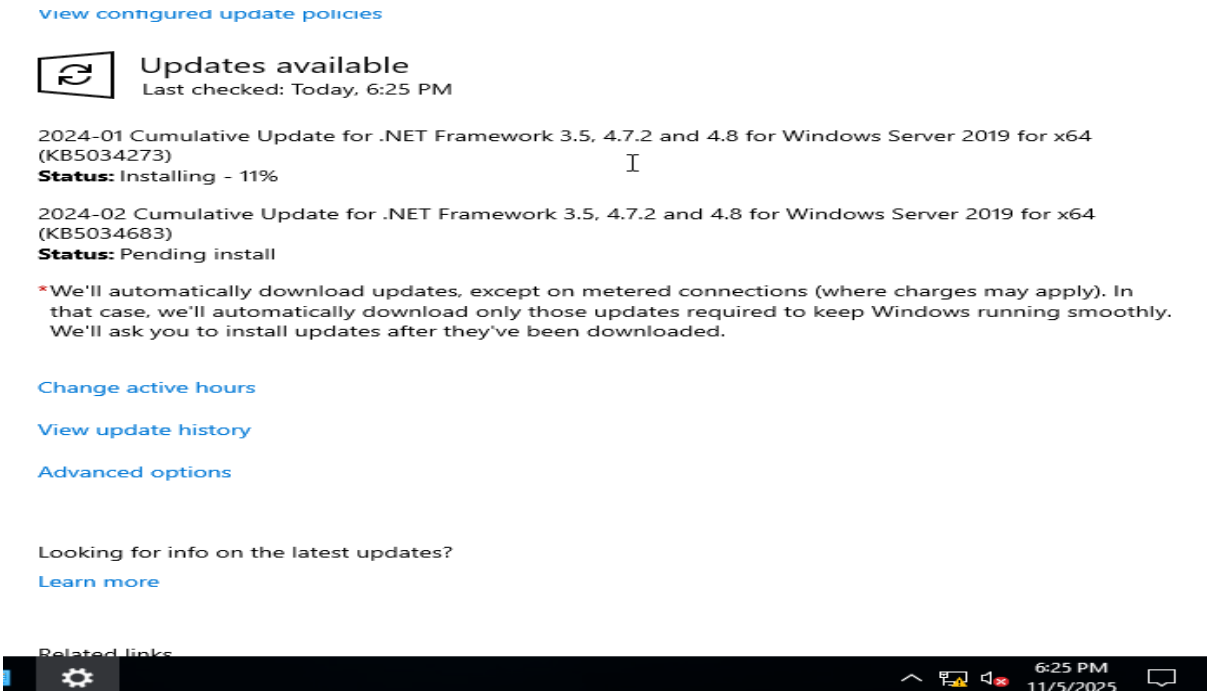
Abdelrhman nabil
OT cybersecurity engineer

Configure Clients (Inside Zone)
Using Group Policy (on DC):
GPO Name: GPO – WSUS Settings
Navigate to:
Computer Configuration → Policies → Administrative Templates → Windows Components → Windows Update
Set:

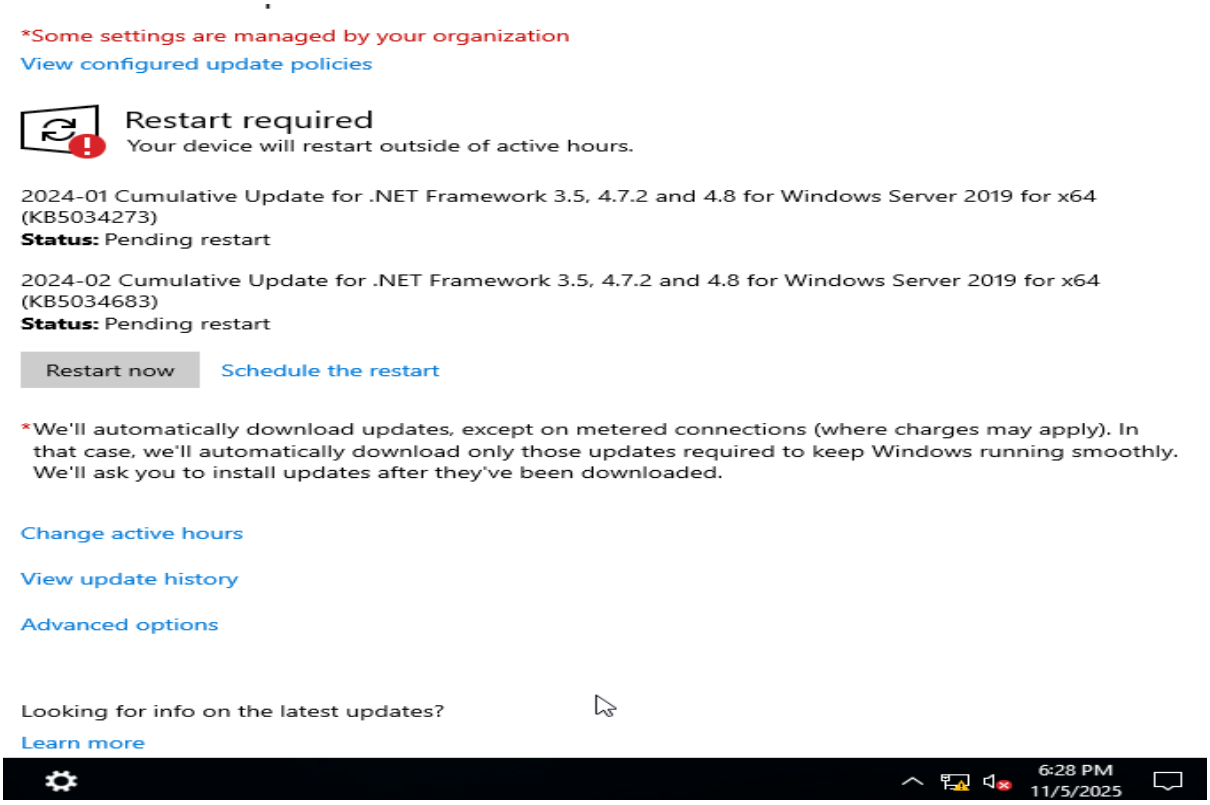
- **Specify intranet Microsoft update service location:**
- **http://192.168.2.10:8530**
- **Enable client-side targeting (optional)**
- **Automatic Updates → Enabled**

This tells Inside clients to fetch updates from the WSUS in the DMZ.





Abdelrhman nabil
OT cybersecurity engineer



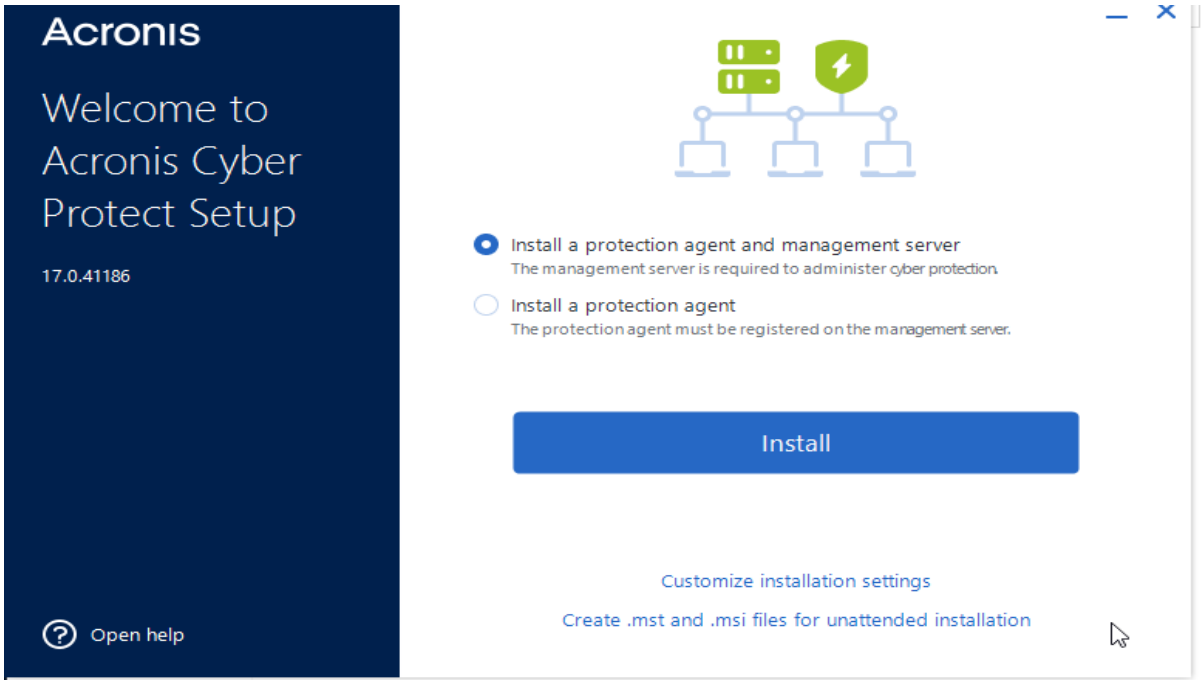
It fetched the updates successfully from the WSUS

Acronis Configuration:

When you access it by your business email download the enterprise offiline Acronis

Download the Management Server Acronis server 17 and install it gonna required approximetly 10GB

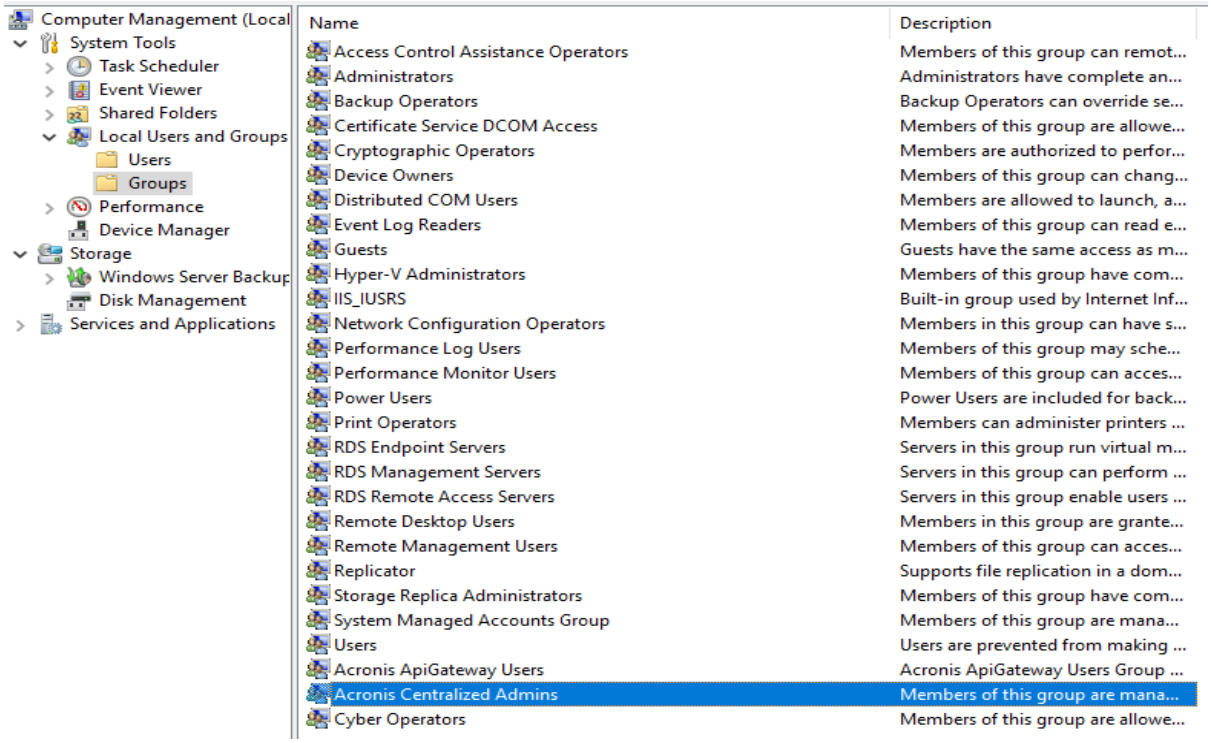
In c:\Program Files\Acronis gonna install management server and windows agent



Abdelrhman nabil
OT cybersecurity engineer

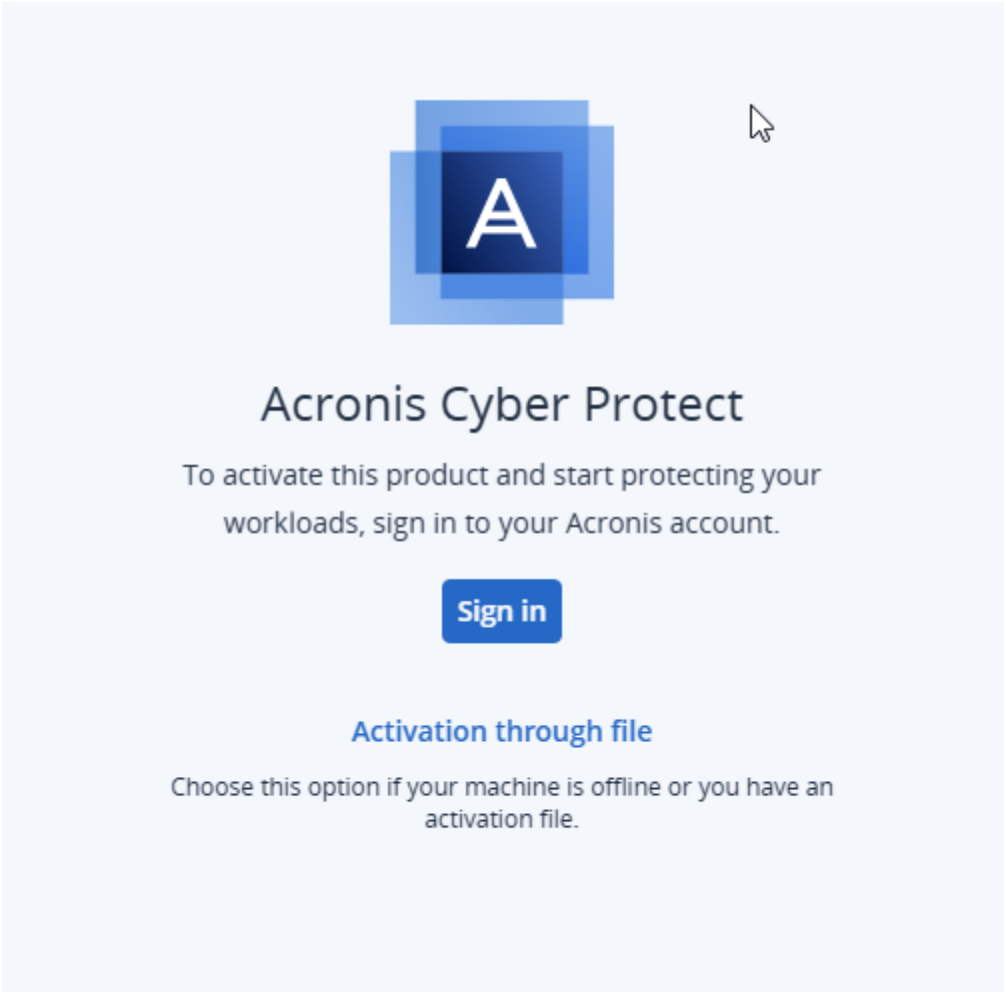
One of the problems I have face that one

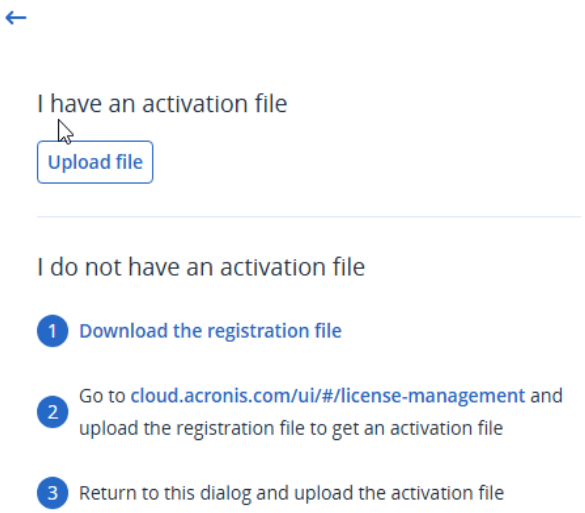
The problem has solved by adding my administrator account to Acronis Centralized admins group and add your account then you can Log In successfully

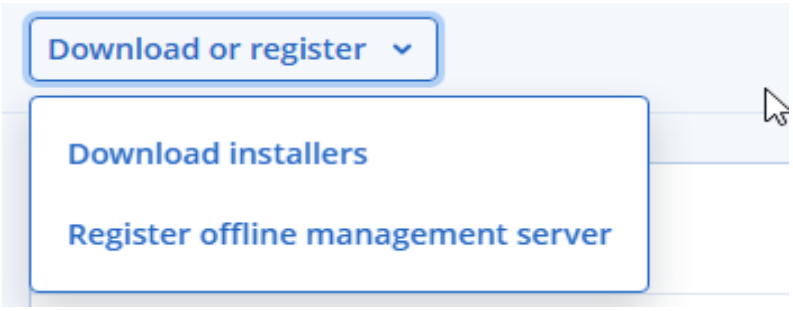


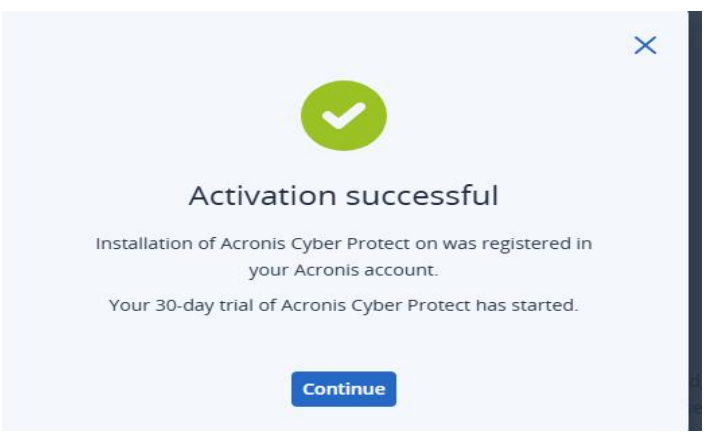
Then to activate the Acronis as you know it is offline in the inside zone so we gonna need activation file to upload it and we gonna get that through the registeration file as follows:

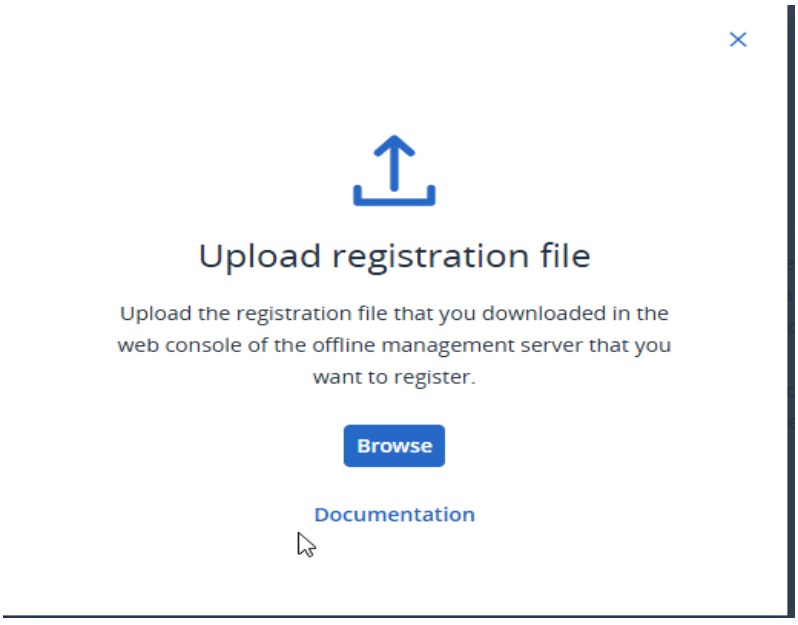
Abdelrhman nabil
OT cybersecurity engineer





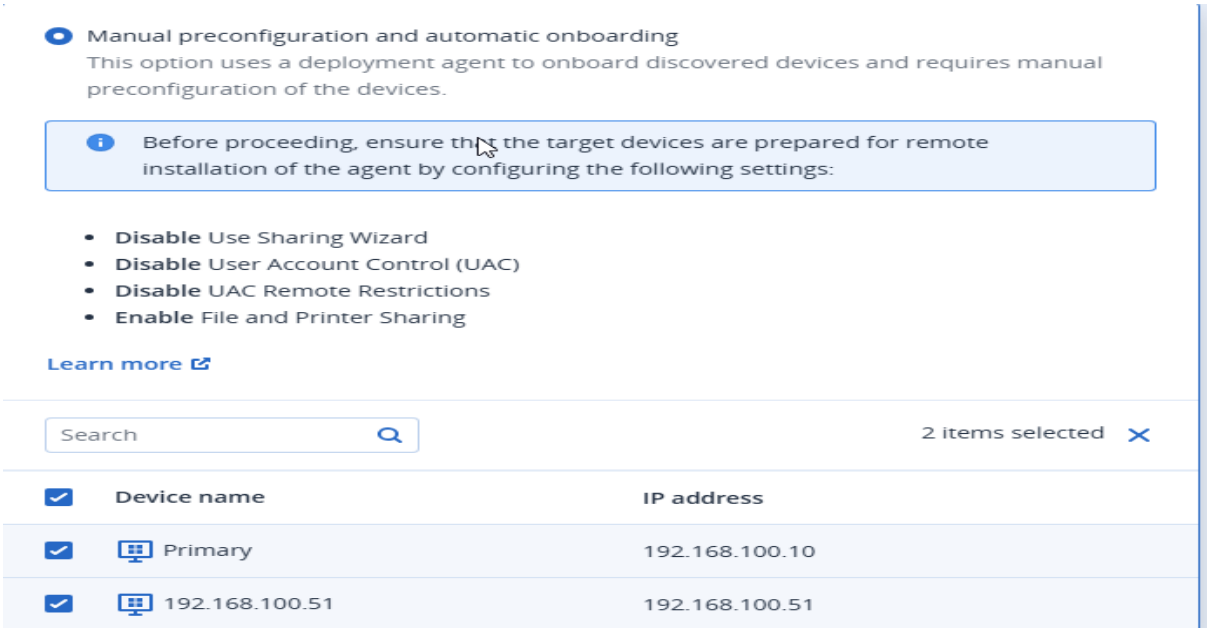






Abdelrhman nabil
OT cybersecurity engineer

After that we we gonna make a device discovery to get all devices and connect them:

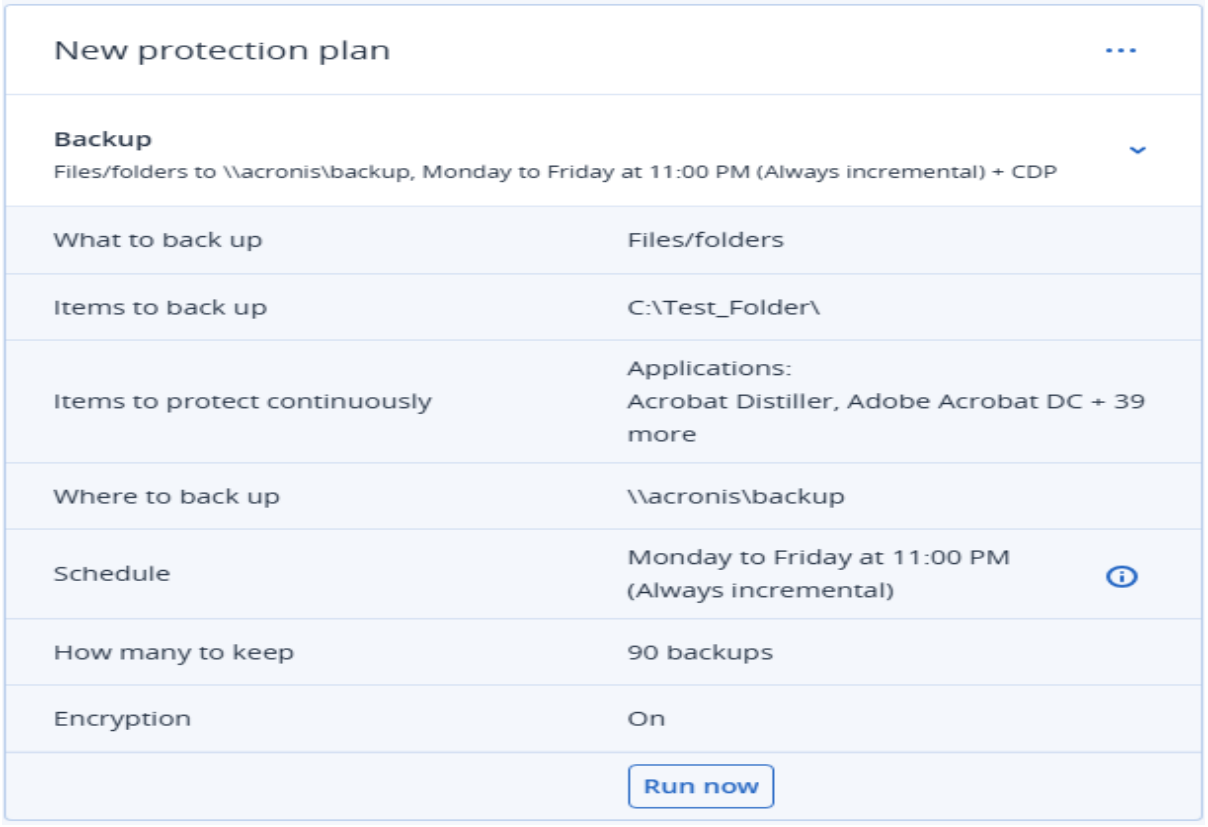


-We have to pre-Configure requirements before the agents installed remotely

-you can download the software to the client and install just the agent and connect it server

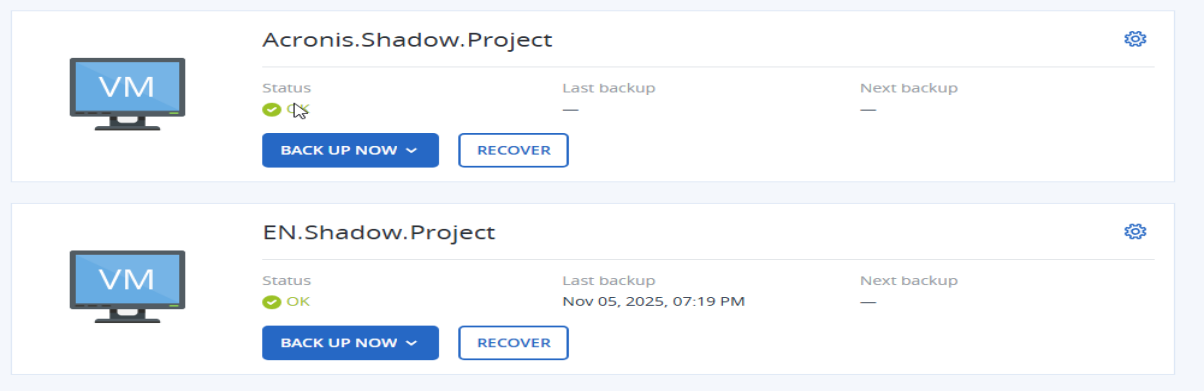
First go to Management → plans and create a protection plan that fits your need I created a simple one for me :

You just connect the agent and start doing the backup and protection plan

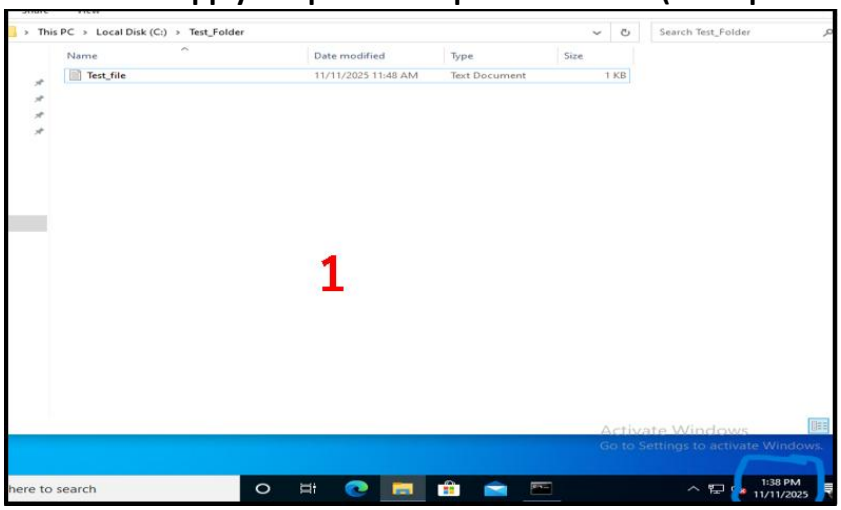


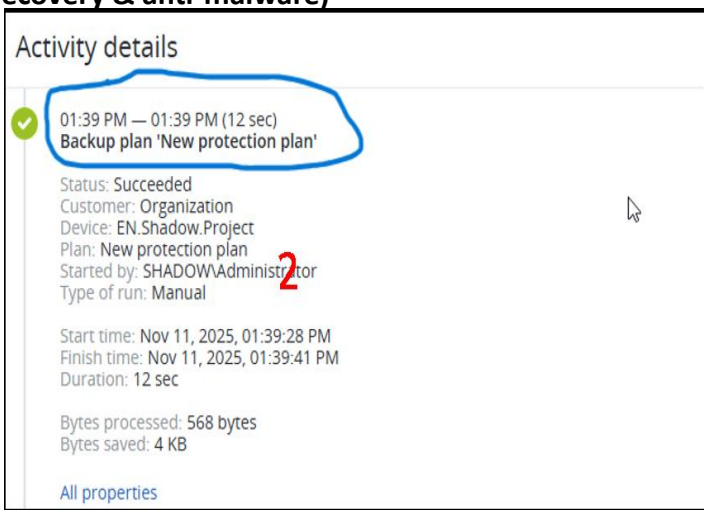
Abdelrhman nabil
OT cybersecurity engineer

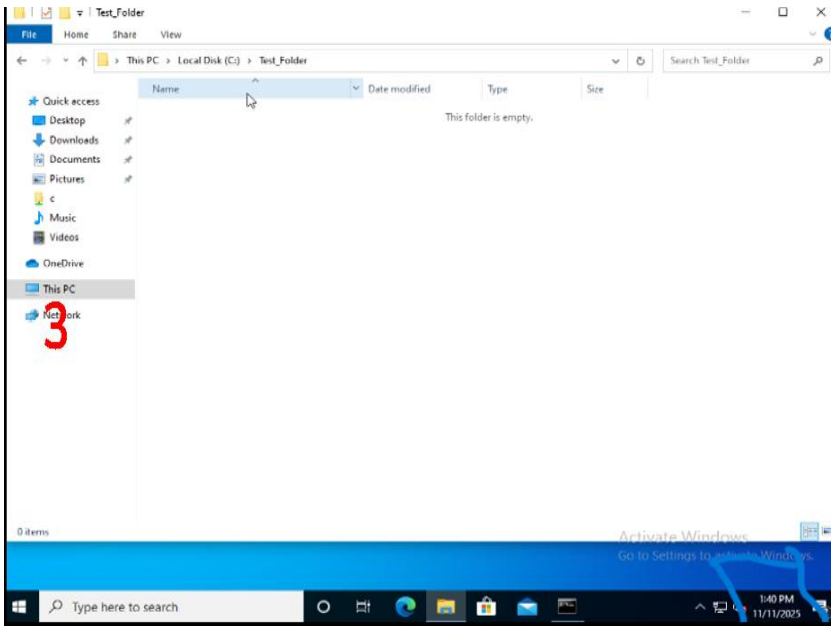
After you install the agent it gonna sound in your management console:

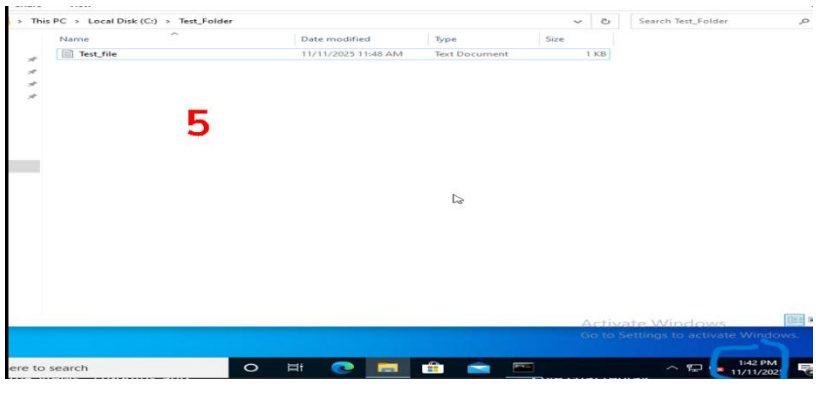


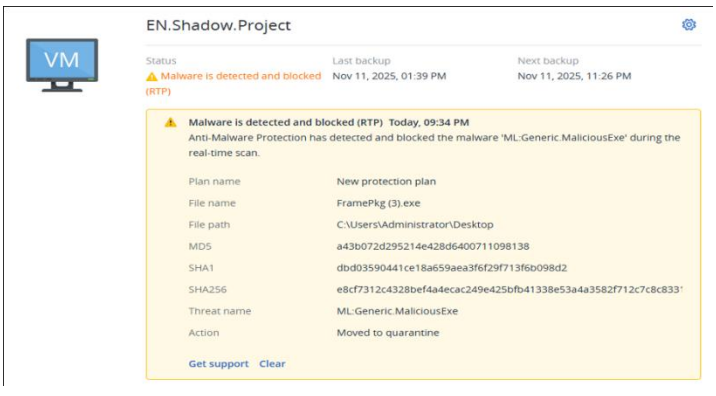
Apply the protection plan and test it (backup and recovery & anti-malware)











Abdelrhman nabil
OT cybersecurity engineer

Start configuring Trellix: (Trellix ENS 10.6.1 and ePO 5.10)

The Trellix EPP products can be installed in one of two configurations:

Self-managed solution

-In self-managed mode, Endpoint Security (ENS) software is installed and managed on each individual system manually without a centralized management system.

-The Trellix self-managed solution requires that you install Trellix ENS on every endpoint manually

-You need to update the DAT files and Exploit Prevention content on every computer manually as well.

Managed solution (ePO-managed)

-The managed solution allows you to install and monitor the Trellix products on your endpoints from a single, centralized location using the ePO console.

-It also allows you to update the DAT files, Exploit Prevention content, and patches on the endpoints from the ePO console.

Endpoint Security (ENS)

ENS is the only supported Trellix product that can be installed without ePO in a Self-managed mode. The other applications such as Trellix Agent, RSD, Device Control, and Solidcore (Trellix Application and Change Control (MACC)) require ePO.

Endpoint Security consists of these modules:

- **Threat Prevention**
- **Web Control**
- **Threat Prevention**

Threat Prevention replaces the traditional antivirus protection and intrusion prevention. It improves performance and productivity by bypassing scanning of the trusted processes. It prioritizes suspicious processes and applications. It also provides adaptive behavioral scanning to monitor and report on suspicious activity. Keeping this solution patched and up to date with the latest qualified version is crucial to the security of a system.

You must regularly update the security products to address the new vulnerabilities as they are discovered. For example, you must regularly update the virus scanning software with virus definition files (DAT files) that are part of ENS Threat Prevention. Trellix frequently releases new DAT files to incorporate results of its ongoing research on the characteristics of new viruses.

NOTE it's recommended updating DAT files on a daily basis.

Abdelrhman nabil
OT cybersecurity engineer

Web Control

ENS Web Control works as a browser extension or add-on with Internet Explorer, Google Chrome™, and Mozilla Firefox™. Web Control can add a layer of protection in case any inadvertent connections are made. Before using Web Control, you need to activate the ENS Web Control extensions manually on these browsers. These are the features for the Managed and Self-managed Web Control that you can configure in the system and create policies for.

Trellix Agent

The Trellix Agent is the client-side component that helps provide secure communication between the ePO and managed products. It serves as an updater for the Trellix products. The Trellix Agent runs in the background, gathers information and events from the managed systems, and sends them to the ePO server. It installs products and their updates including DAT files and Exploit Prevention content. It enforces policies and tasks on the managed systems and sends events back to the ePO server.

Device Control (DLP)

Device Control is a portion of Trellix's Data Loss Prevention (DLP) software that helps organizations to reduce the risk of an unintentional disclosure of confidential information. It helps prevent unauthorized use of removable media devices (such as CD\DVD, USB, and Floppy disk) to guard against data leaks. Such devices are one of the common ways malware can transfer itself from relatively unsecured home or business networks to the control network.

Solidcore (Trellix Application and Change Control (MACC))

Trellix Solidcore consists of two components: Application Control and Change Control. It uses an application called Solidcore that helps block unauthorized applications and changes to the process control networks by combining whitelisting and change control technology.

Application Control functions by listing the processes that are allowed to run (whitelisting) on fixed function devices. It helps block vulnerable, unauthorized, or malicious applications that can compromise the integrity of systems. Whitelisting helps secure the system and only allows authorized updates or changes that are defined by the administrators or trusted sources.

Abdelrhman nabil
OT cybersecurity engineer

Solidcore (Trellix Application and Change Control) software also supports change-control technology that can block unwanted, out-of-policy changes before they occur. The Solidcore enabled systems block the changes attempted outside of policy. The change attempt is logged and sent as an alert to the administrators.

It's recommended that you run a full scan on a regular basis. However, this can affect the performance of the system. Schedule a full scan during off-peak hours when the system is not expected to perform other CPU intensive activities.

ENS provides on-demand scan and on-access scan. On-demand scanning allows you to run a full scan at a specified time. On-access scanning scans the files as they are accessed.

Disabling Internet Explorer Enhanced Security Configuration (IE ESC)

You need to turn off the IE ESC for both the administrator and the user in order to start the ePO console. These are the steps:

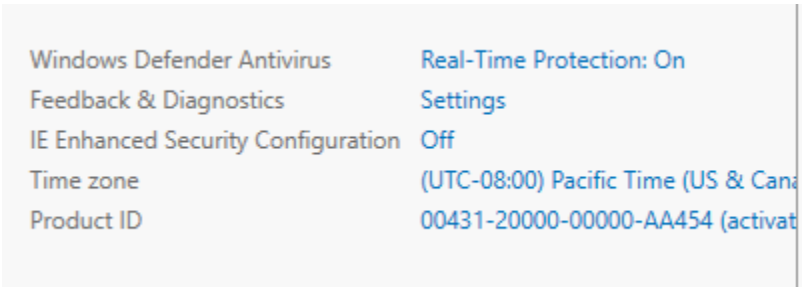
1.On the station on which you want to install the Trellix ePO software, log on using domain administrator with local administrative permissions.

2.Select Start > Control Panel > Administrative Tools > Server Manager.

3.In the left column, select Server Manager > Local Server.

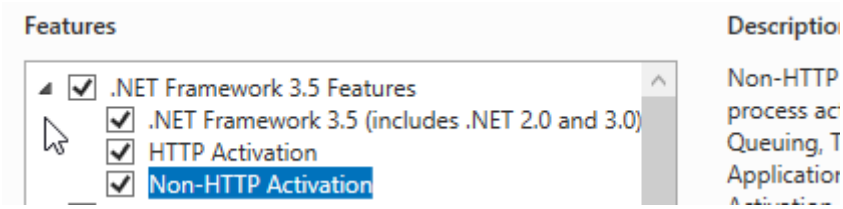
4.In the right column, verify that IE Enhanced Security Configuration is OFF.

5.Verify that IE ESC is turned off for both the administrator and the user. Select OK.



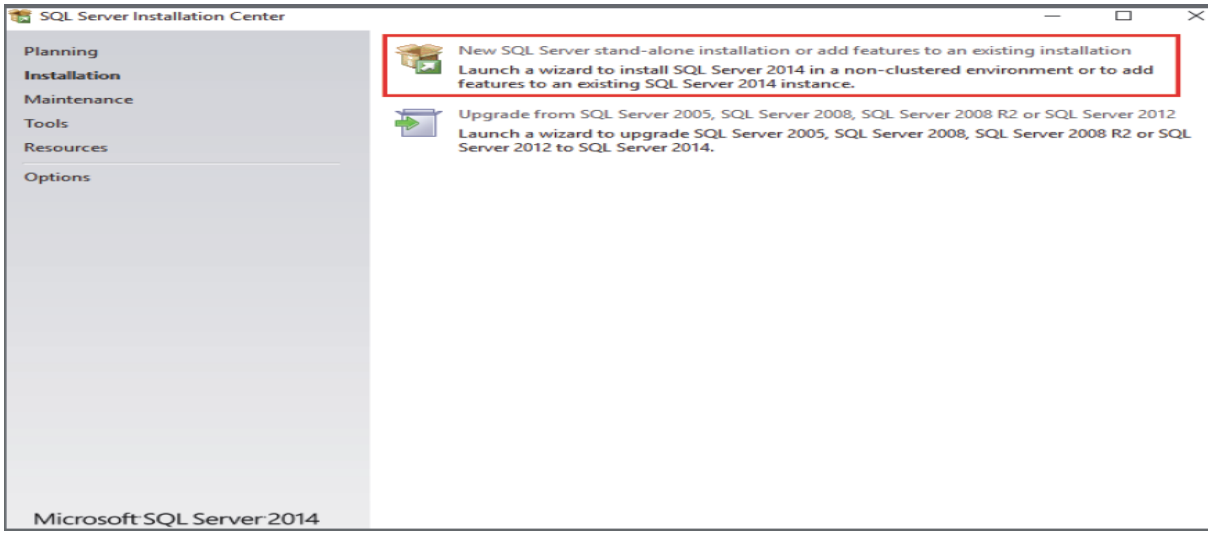
Abdelrhman nabil
OT cybersecurity engineer

And we need to install .net 3.5 SP1 from the features and SQL server:

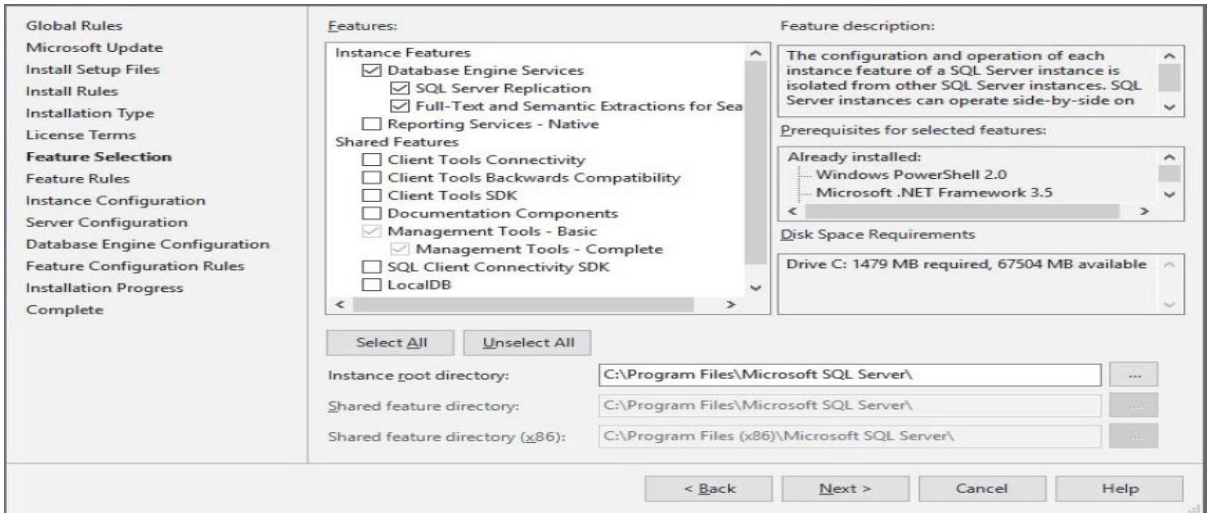


And install the sql server that supports TLS 1.2 or higher and that starts from sql server 2014 SP3

Initialize the DB server



In the Features Selection window, verify that the Database Engine Services and Management Tools-Basic checkboxes along with sub-checkboxes are selected and the others are cleared, and click Next



Abdelrhman nabil
OT cybersecurity engineer

-In the Instance Configuration window, change the Named instance: to EPOSERVER, and click Next.

-In the Server Configuration window, for SQL Server Browser change Startup Type to Automatic, and click Next.

-In the Database Engine Configuration window, verify that Windows Authentication Mode is selected and under Specify SQL Server Administrators, verify the user account with of domain administrator with local administrative permissions that you are currently using to install SQL Server, is listed. Click Next.

-In the Complete window, click Close.

-Close the SQL Server Installation Center window.

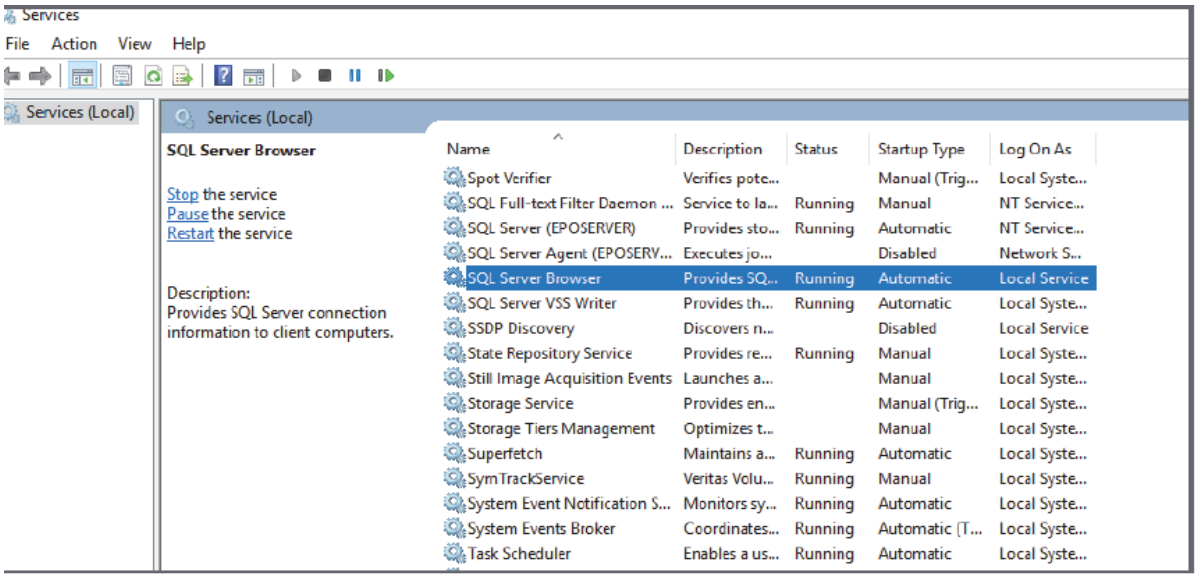
-Restart the server.

Verifying SQL Server Settings

To verify that the SQL Browser Service is running:

1.Click Start > Run. Enter services.msc and click OK.

2.Locate the SQL Server Browser service and verify that its Status is Running and Startup Type is Automatic.



Abdelrhman nabil
OT cybersecurity engineer

Changing the SQL Server Log On Account

You need to change the logon account to use the ePO services.

1.Click Start, search for Administrative Tools, and click Services.

2.If prompted for permissions, click Continue.

3.Right-click the SQL Server EPOSERVER service, and click Properties.

4.Click Log On, under Log on as, select the Local System account option, and click OK.

5.In the Services window, click OK.

6.Select the SQL Server EPOSERVER service, and click Start the service or Restart the service.

7.Close the Services snap-in.

Enabling Shared Memory, Named Pipes, and TCP/IP

Verify that the Shared Memory, Named Pipes, and TCP/IP are enabled in the SQL Server Configuration Manager:

1.Click Start > Microsoft SQL Server 2014 > SQL Server 2014 Configuration Manager.

2.In the User Access Control window, click Yes.

3.Expand the SQL Server Network Configuration and select Protocols for EPOSERVER.

4.Right-click to enable Shared Memory, Named Pipes, and TCP/IP. In the Warning window, click OK.

5.Right-click TCP/IP and select Properties.

6.Select the IP Address tab and scroll to the bottom.

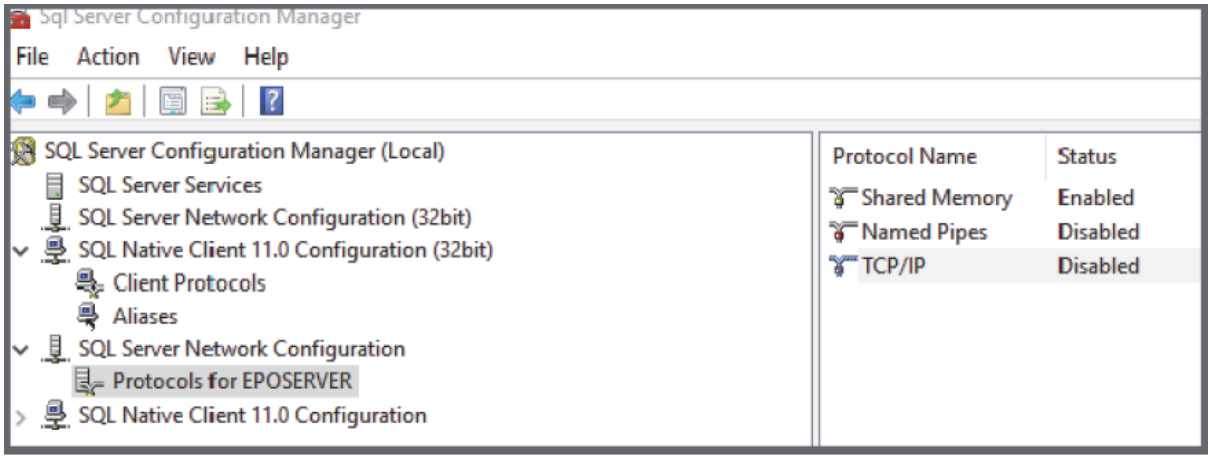
7.In the IPALL section, delete “0” from TCP Dynamic Ports and enter 1434 in TCP Port. Click Apply.

8.In the Warning window, click OK. In the TCP/IP Properties window, click OK.

9.Close the SQL Server Configuration Manager dialog box.

10.Restart the server.

Abdelrhman nabil
OT cybersecurity engineer

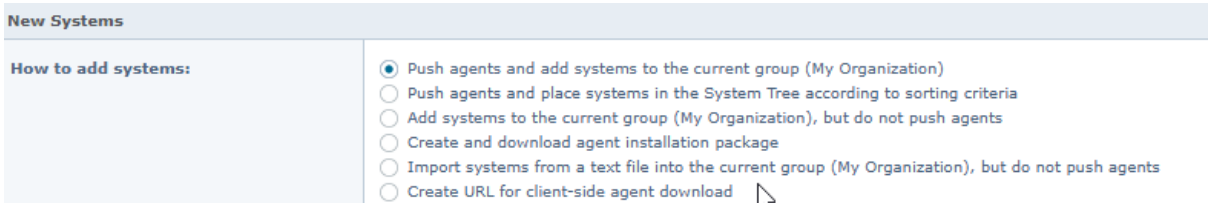


After that proceed with the EPO installation process .

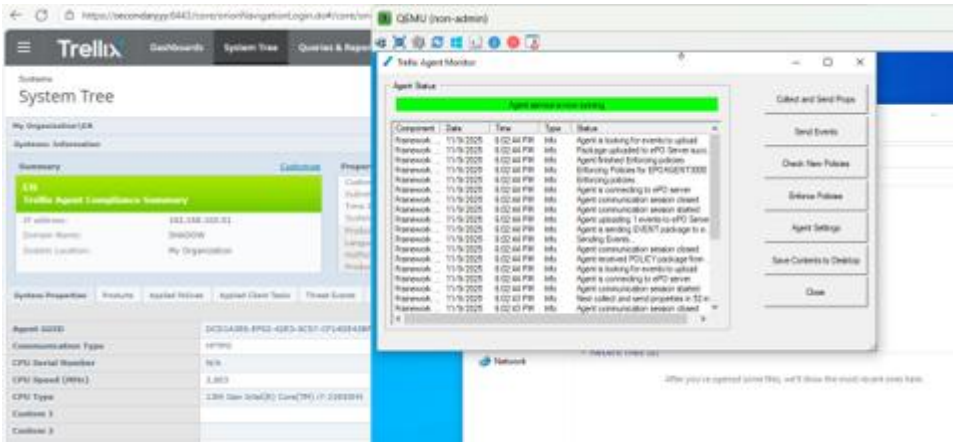
Then upload all the Extensions you have as follows:

Software → Extension

And you can add the agents by the system tree:



You got all these options to push an agent to the clients after it successfully connected you can assign the policies by the extensions you have:



And start in assigning the policies and see what you need and apply it but also be careful and test the policies before you apply them

Thanks for your time.