



# Chapter 7

## **Group Policy**

Tran Thanh Dien, PhD

August, 2024



CANTHO UNIVERSITY

# Content

- Group Policy Objects
- GPOs
- GPO processing order
- Configuring Group Policy Settings
- Default Domain Policy



CANTHO UNIVERSITY

# Group Policy

- Policy: some kind of ruleset, structure, or standard to which you need something to adhere
- Group Policy: applying policies to a group of computers
- Group Policy: a centralized way to issue policies to groups of computers inside your domain network.



CANTHO UNIVERSITY

# Group Policy

- Contain settings and configurations applied to either computers or users in AD





# Group Policy

- A collection of configuration settings applied to objects in the AD DS, including:
  - Software Settings
  - Scripts
  - Security Settings
  - Administrative Templates
  - Folder Redirection
- Policies targeted to users, computers, group, sites, domains, and OUs; and then rely on the system to enforce those policies
- Policies can execute scripts during logon or logoff and computer startup and shutdown.

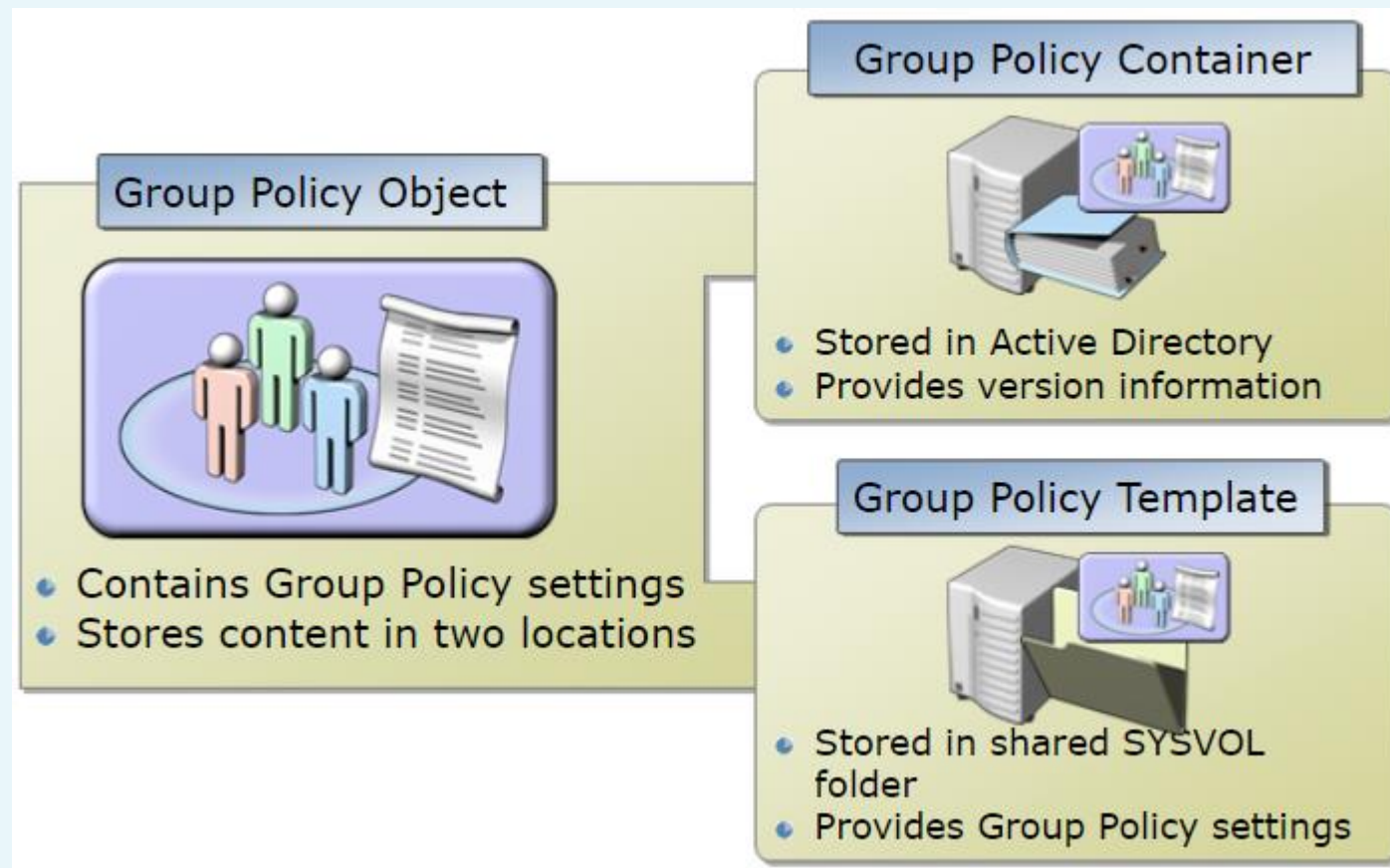


CANTHO UNIVERSITY

# Group Policy

## Group Policy Objects (GPOs)

- An individual instance of a Group Policy known as a Group Policy Object (GPO)
- Contain one or many policy settings applying to the domain computers and users
- Control the behavior of workstations and the end-user experience across the entire organization
- Settings in GPO applied automatically to computers joining to domain





# Group Policy

## Group Policy Objects (GPOs)

- Every time a domain user logs into a domain-joined computer, computer reaches out to AD and asks, “Hey, got any GPO settings for me?”
- A DC hands over all of the GPO settings that apply to the computer and/or user logging in
- GPOs define to whom each policy applied
- Group Policy reprocesses itself every 90 minutes or at the time users to log in or restart their computers
- To force computers to grab updated GPO settings: `gpupdate /force`



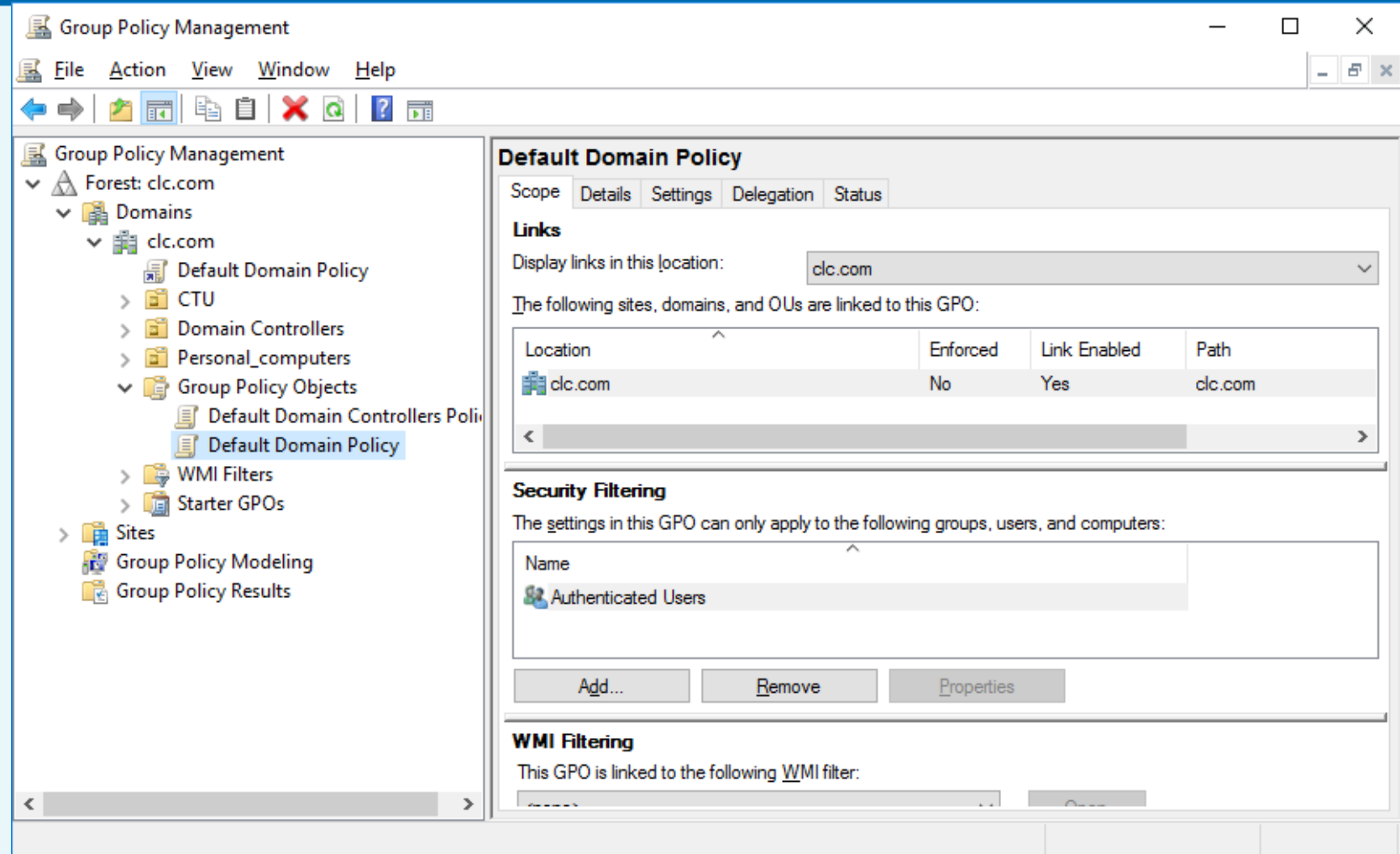


CANTHO UNIVERSITY

# Group Policy

## Creating GPOs

- **Group Policy Management console (GPMC):** The utility used to create, manage, delegate, and link GPOs.
- **Group Policy Management Editor (GPME):** The utility used to edit a GPO.







# Group Policy

## Creating GPOs

Group Policy Management

File Action View Window Help

Group Policy Management

Forest: clc.com

Domains

clc.com

- Default Domain Policy
- CTU
- Domain Controllers
- Personal\_computers
- Group Policy Objects
- Default Domain C
- Default Domain P
- WMI Filters
- Starter GPOs

Sites

Group Policy Modeling

Group Policy Results

Group Policy Objects in clc.com

Contents Delegation

Name	GPO Status	WMI Filter	Modified	Owner
Default Domain Controller...	Enabled	None	7/28/2020 8:45:...	Domain
Default Domain Policy	Enabled	None	7/28/2020 8:45:...	Domain

New

- Back Up All...
- Manage Backups...
- Open Migration Table Editor
- View
- New Window from Here
- Refresh
- Help

New GPO

Name:

TestPolicy

Source Starter GPO:

(none)

OK Cancel

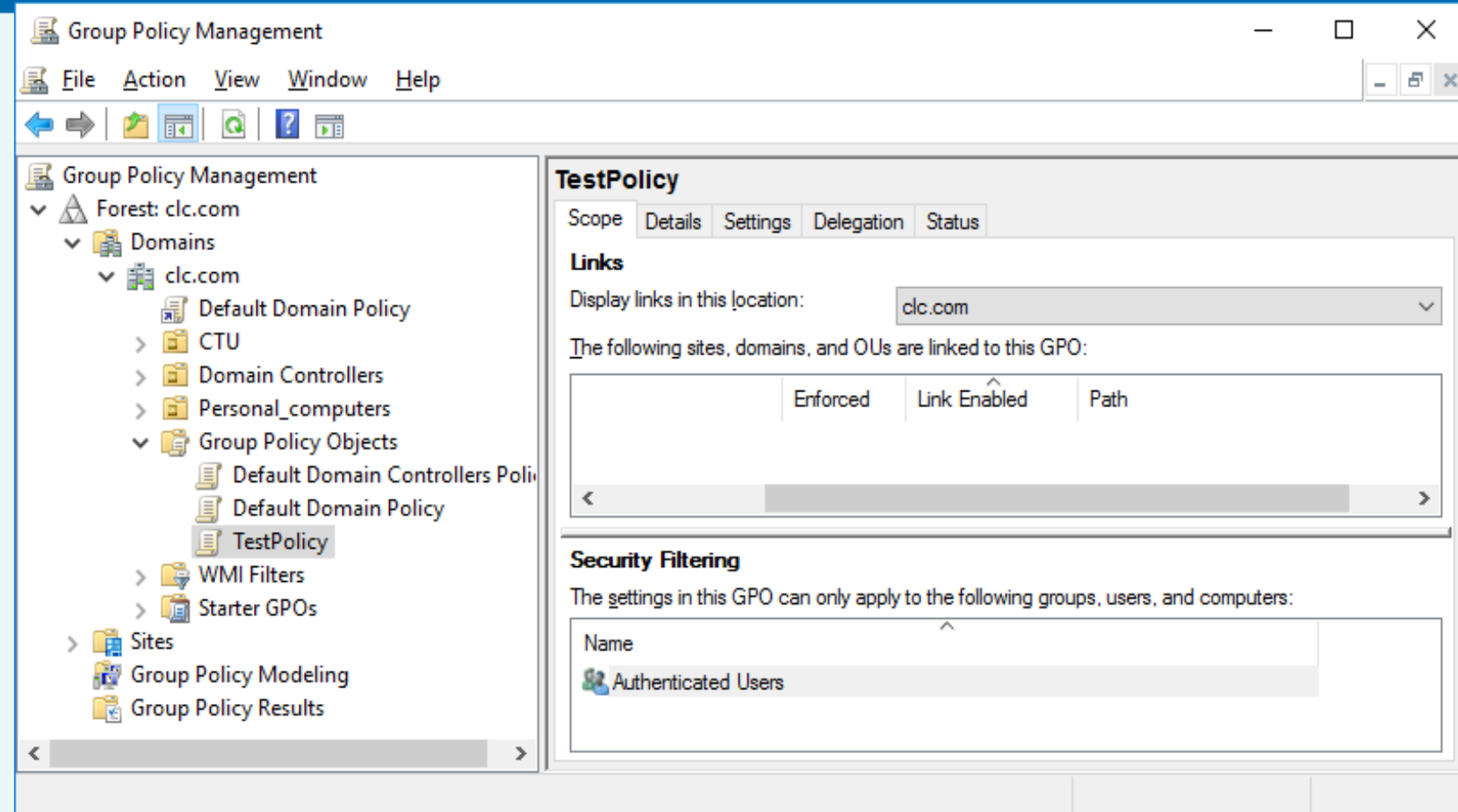


CANTHO UNIVERSITY

# Group Policy

## Creating GPOs

- New GPO now shows up in the list of available GPOs, but not yet applying to anyone or any computers
- The policy settings in the GPO not applied until it is linked.



New GPO is void of any settings or configurations

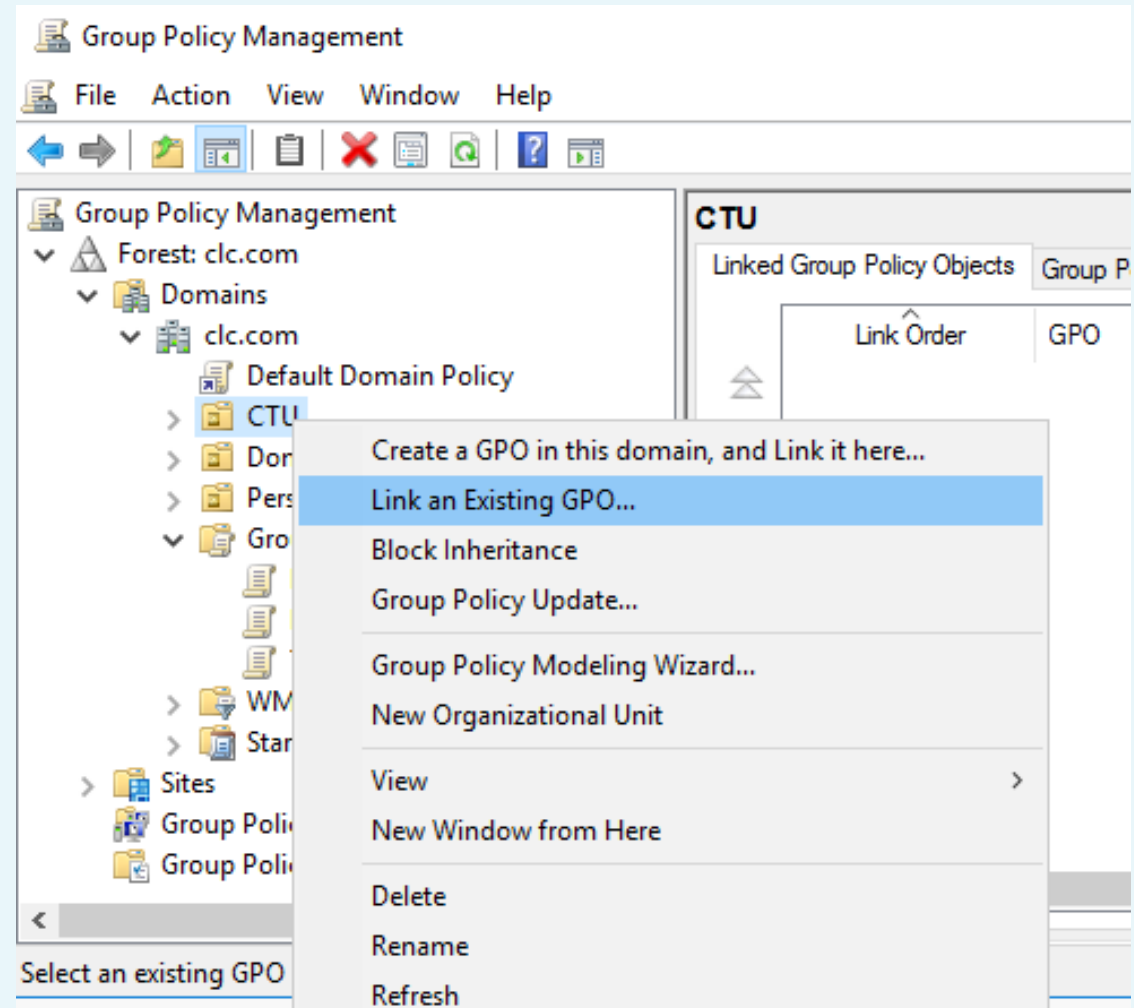


CANTHO UNIVERSITY

# Group Policy

## Configuring GPO Links

- Link GPO to a location in Active Directory (a site, domain, or OU) to apply its contained settings to users and devices that are within that location
- Inside the GPMC, find the location (OU) to which you want to link the GPO, e.g., assign this GPO to my CTU OU
- Right-click on the OU, and then choose **Link an Existing GPO...**





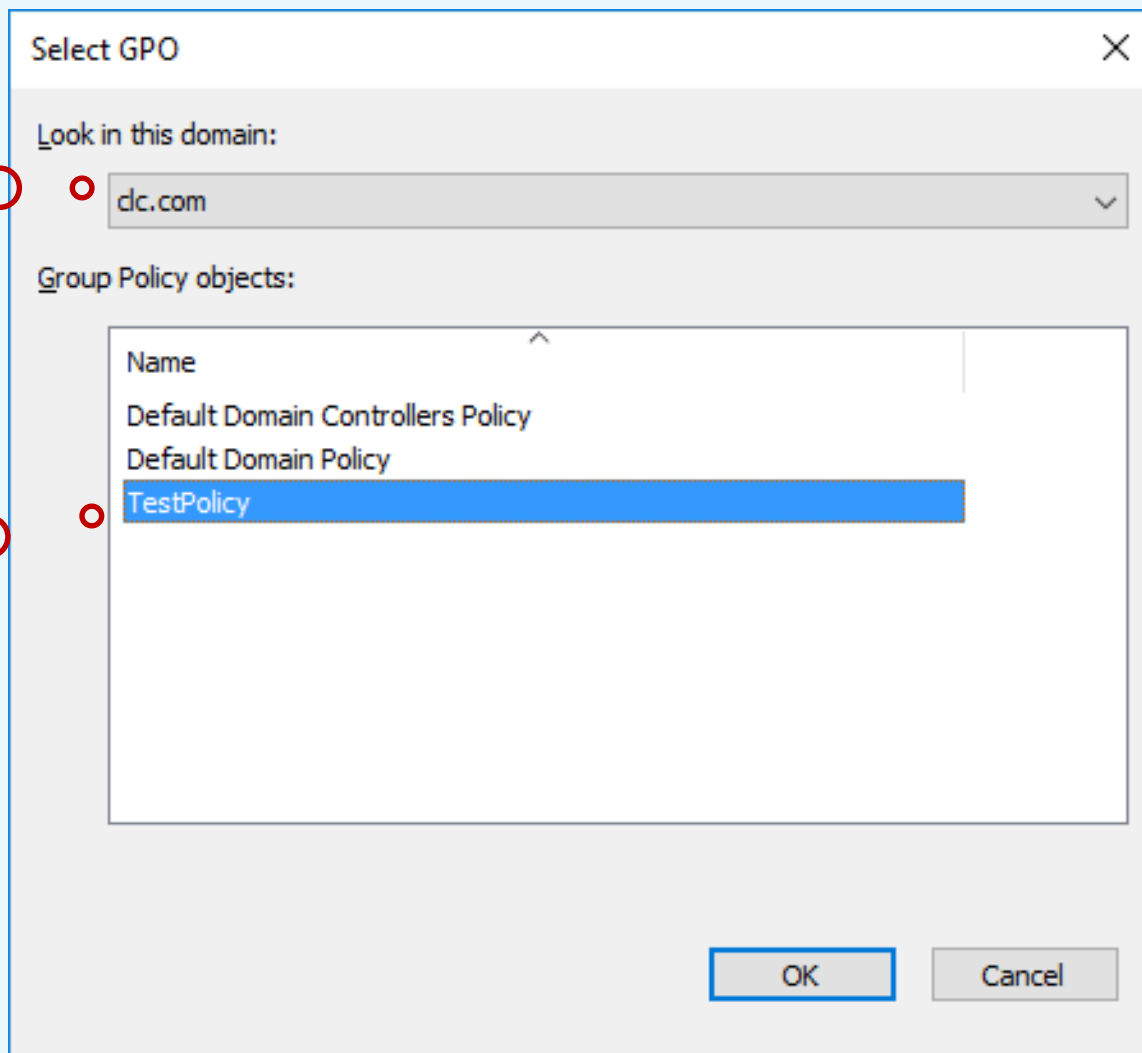
CANTHO UNIVERSITY

# Group Policy

## Configuring GPO Links

Choose the domain  
to search for  
policies

select a policy

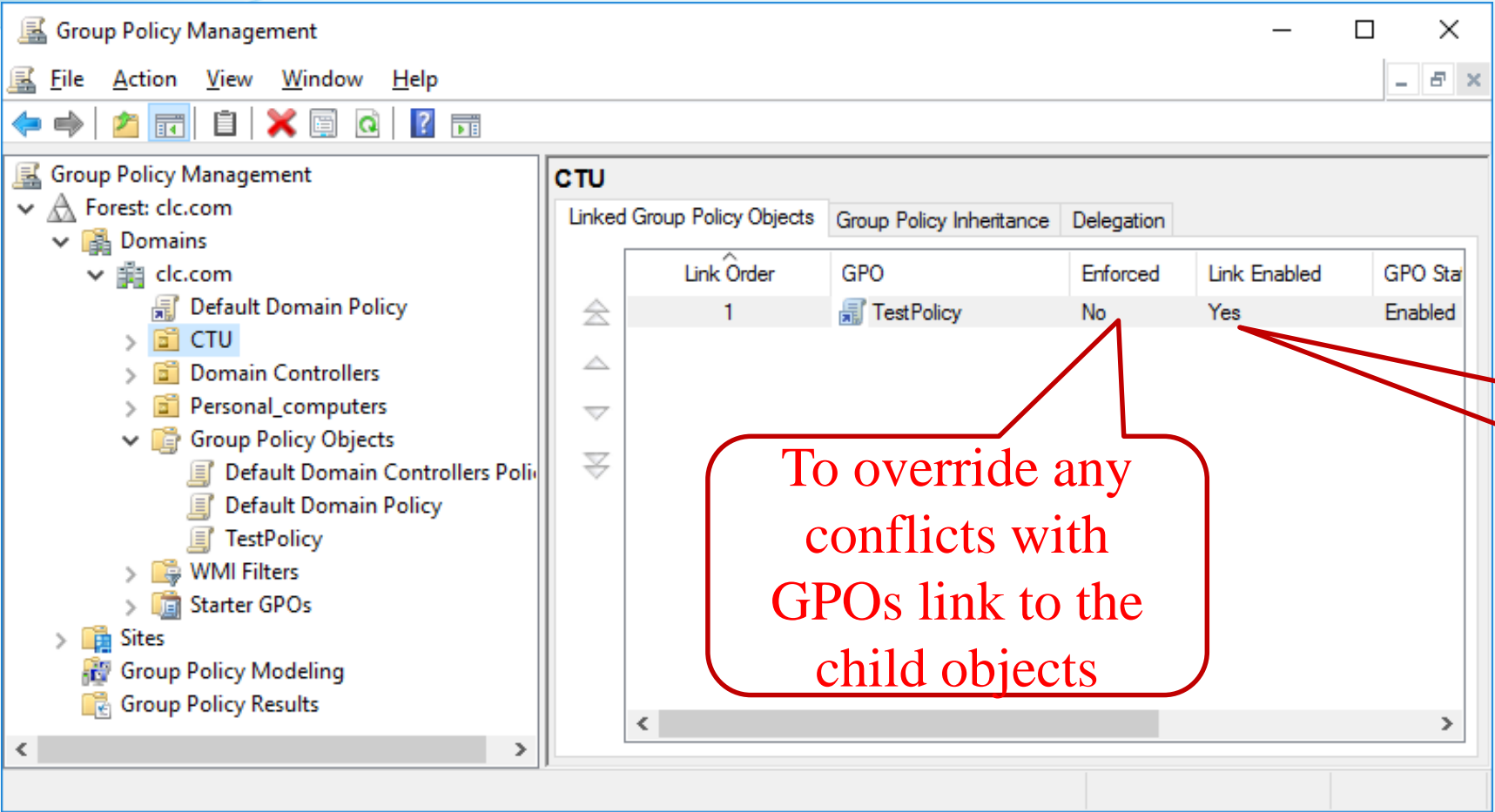




CANTHO UNIVERSITY

# Group Policy

## Configuring GPO Links



All GPOs linked to the currently selected node

To override any conflicts with GPOs link to the child objects

Disabled links: Not apply settings to objects in the directory



CANTHO UNIVERSITY

# Group Policy

## Managing Starter GPOs

- GPOs have the potential to be large, complex configurations (thousands of potential settings)
- A template of preconfigured policy settings to reduce the time and burden when creating new policies
- Starter GPO serves as templates
- New GPOs created from a starter GPO will include all the settings, values, comments, and delegations defined in the starter GPO
- Starter GPOs can also be easily exported and imported for use across domains, forests, or even entirely separate AD DS deployments

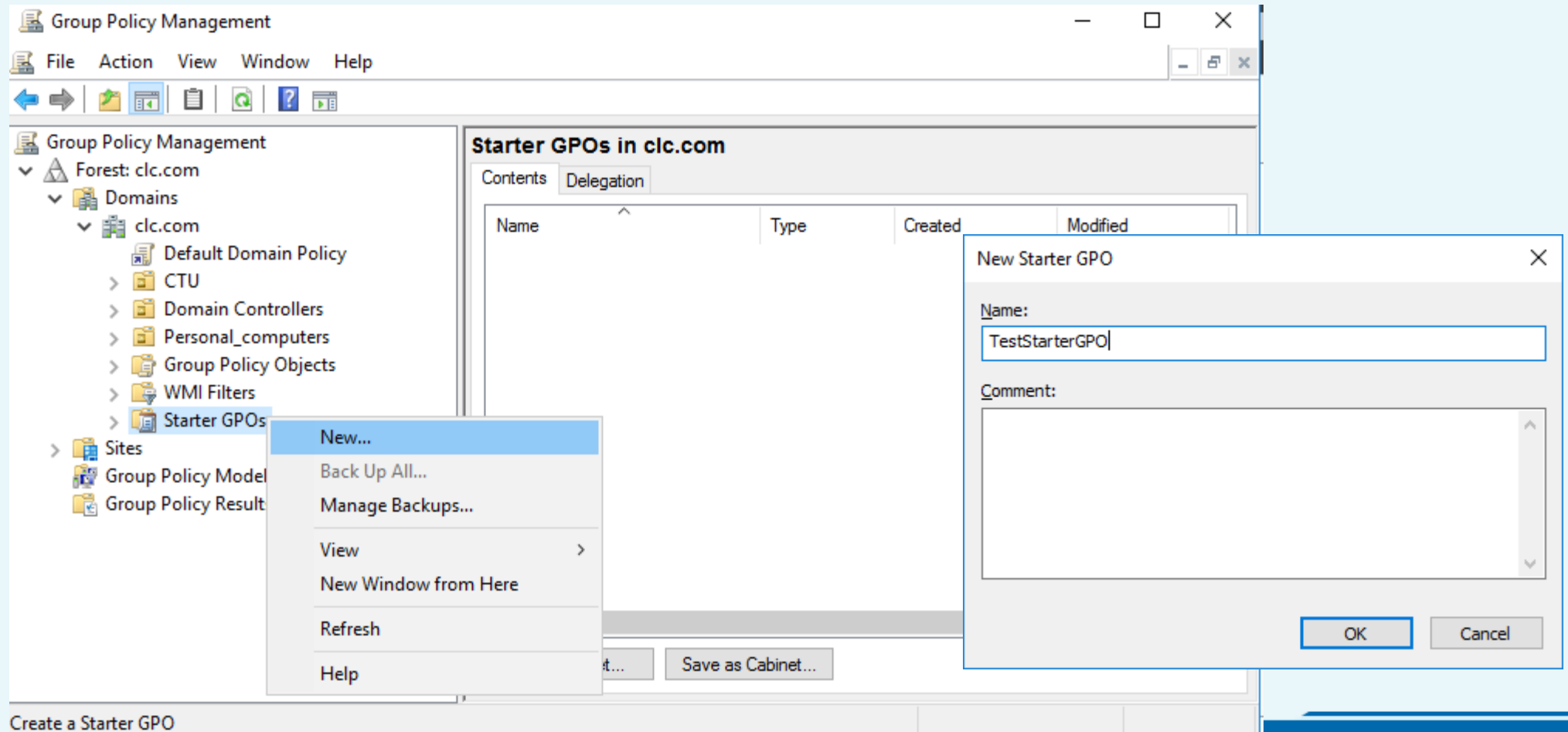


CANTHO UNIVERSITY

# Group Policy

## Managing Starter GPOs

### Creating a Starter GPO





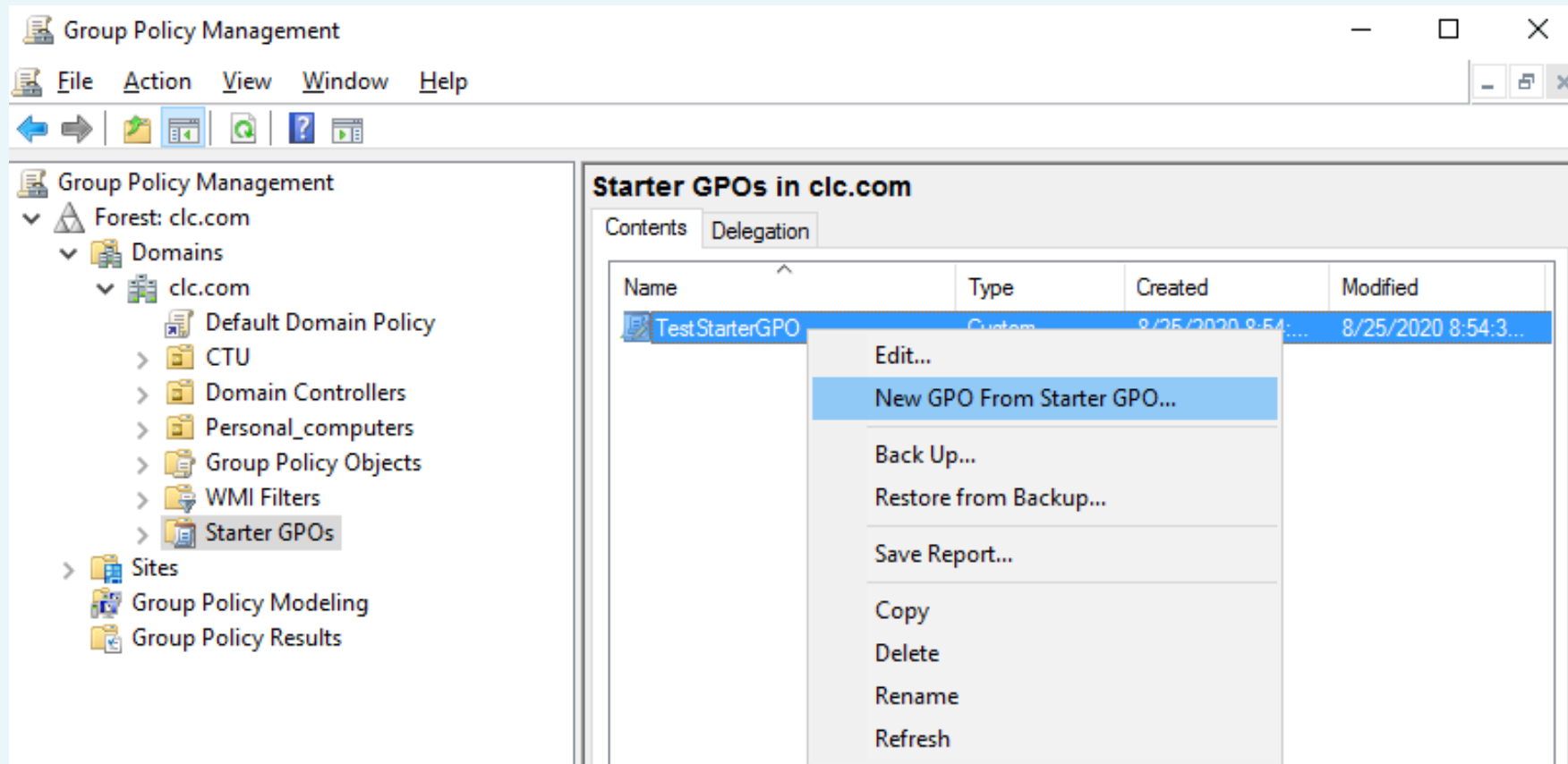


CANTHO UNIVERSITY

# Group Policy

## Managing Starter GPOs

### Creating new GPO from Starter GPO



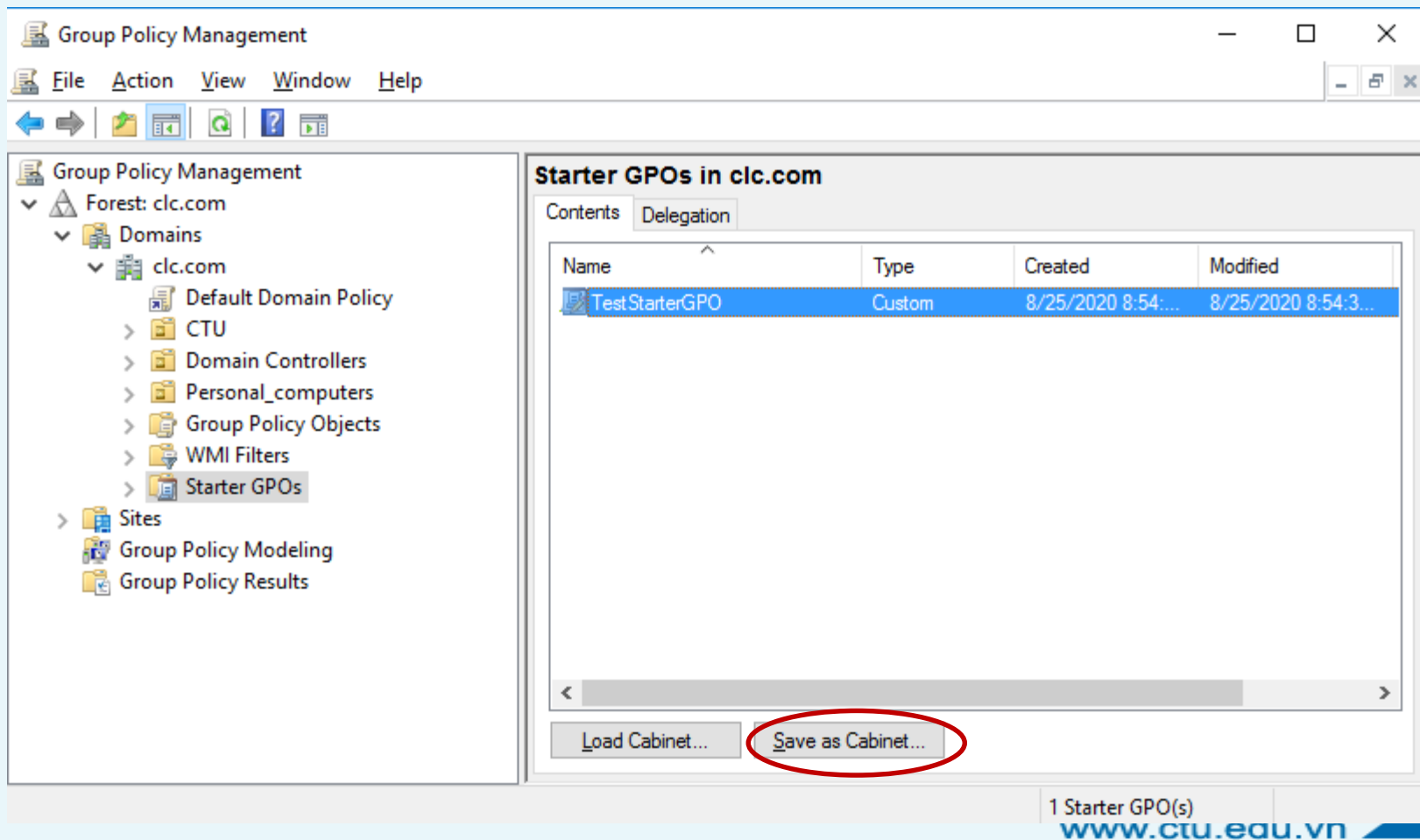


CANTHO UNIVERSITY

# Group Policy

## Managing Starter GPOs

Export starter GPOs to use in another forest



The screenshot shows the Group Policy Management console for the forest clc.com. The left pane shows the tree structure: Forest: clc.com > Domains > clc.com > Starter GPOs. The right pane shows the 'Starter GPOs in clc.com' list with one entry: TestStarterGPO, Custom type, created and modified on 8/25/2020 8:54:30. The 'Save as Cabinet...' button at the bottom is circled in red.

Name	Type	Created	Modified
TestStarterGPO	Custom	8/25/2020 8:54:30	8/25/2020 8:54:30

1 Starter GPO(s)  
www.ctu.edu.vn



CANTHO UNIVERSITY

# Group Policy

## GPO Processing order

- Ways that a GPO can be applied to a security principal:
  - linked to a domain, site, or OU
  - inherited from a parent OU
  - and assigned by local Group Policy
- More than one GPO applied to AD objects
- How does Group Policy resolve conflicts when two or more GPOs apply the same policy setting?
  - Group Policy walks through a specific order when processing GPO
  - As GPOs processed, Group Policy retains the most recent value for a policy setting
  - Any policy setting that is not configured on subsequent GPOs still applied



CANTHO UNIVERSITY

# Group Policy

## GPO Processing order

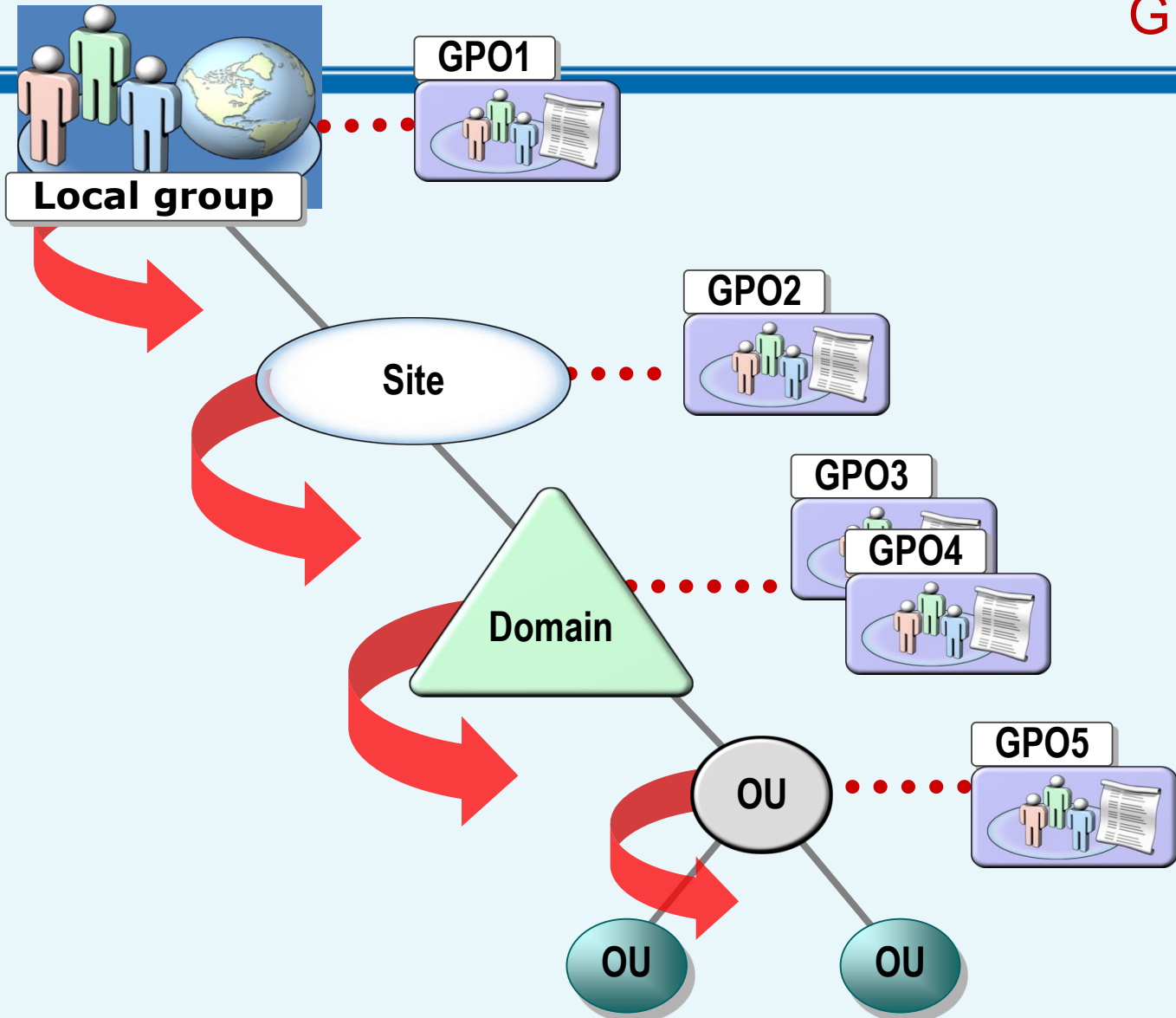
- GPOs are processed on a client computer in the following order:
  1. Local GPOs
  2. Site-level GPOs
  3. Domain-level GPOs
  4. OU GPOs, including any nested OUs
- Last GPO applied takes precedent



CANTHO UNIVERSITY

# Group Policy

GPO Processing order





CANTHO UNIVERSITY

# Group Policy

## GPO Processing order

- Within each processing step there are additional rules as well
  - When multiple GPOs linked to a node, GPMC indicates a Link Order value.
  - GPOs processed descending order, from highest to lowest. i.e., a policy with a Link Order of 1 takes precedence over policies with a higher link order

The screenshot shows the Group Policy Management console for the forest clc.com. The left pane displays the hierarchy: Forest: clc.com > Domains > clc.com > CTU. The right pane shows the 'Linked Group Policy Objects' tab for the CTU node. It contains a table with the following data:

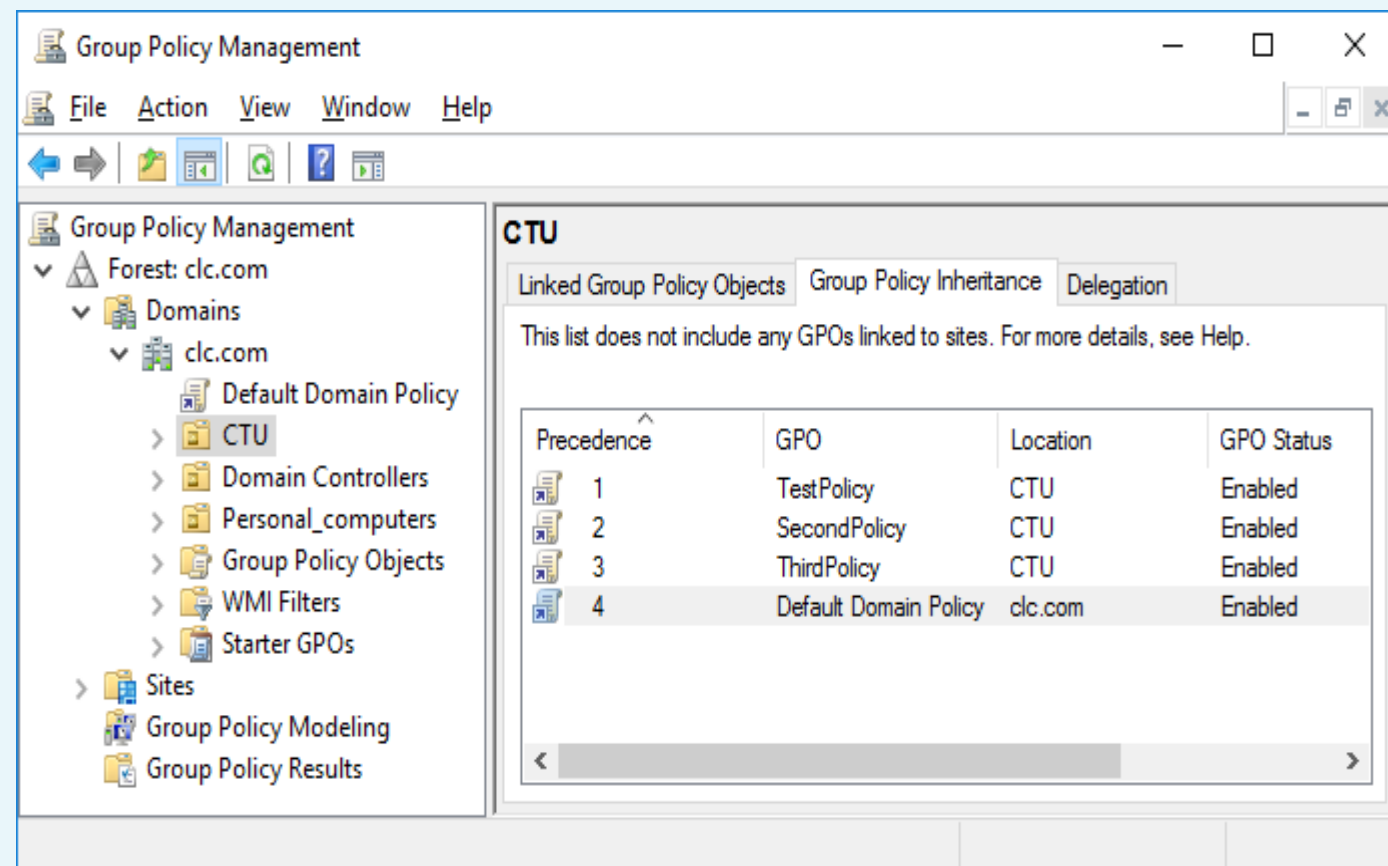
Link Order	GPO	Enforced	Link Enabled	GPO Status
1	TestPolicy	No	Yes	Enabled
2	SecondPolicy	No	Yes	Enabled
3	ThirdPolicy	No	Yes	Enabled

Administrators can adjust the Link Order for GPOs at a node

# Group Policy

## GPO inheritance and preference

- The application of GPOs linked to each container results in a cumulative effect called policy inheritance:
  - Default precedence: Local → Site → Domain → OU → Child OU...
  - Visible on the **Group Policy Inheritance** tab
- The lower the number the higher the precedence of the GPO







# Group Policy

## GPO inheritance and precedence

- Block Inheritance (attribute of OU):
  - Inheritance can be blocked both for an entire domain or for individual OUs.
  - When inheritance blocked, the node not inherit any of the policies from GPOs linked to its parent node unless the parent GPO link flagged as Enforced
- Enforced (attribute of GPO link):
  - Enforced GPOs override Block Inheritance
  - Enforced GPO settings win over conflicting settings in lower GPOs



# Group Policy

## Security Filtering

- Link GPO to particular OUs to apply settings to machines
- Having a new GPO linked to an OU contained all of your desktop computers, but then decided that some of those machines needed the policy and some did not
- Split those machines up into two separate OUs just for the purpose of this policy
- This is where GPO Security Filtering comes into play



# Group Policy

## Security Filtering

- **Security Filtering:** the ability to filter a GPO down to particular AD objects
- Set Filters the GPO to only apply to particular users, particular computers, or even particular groups of users or computers
  - Create a new Security Group inside Active Directory and add only those computers into the group
- Once the GPO configured with that group listed in the filtering section, that policy would only apply to machines that are part of that group.



**Security Filtering:** set security filter so that only machines belong to the specific security group actually receive the settings from the GPO

The screenshot shows the Group Policy Management console. On the left, the tree view is expanded to 'Group Policy Objects' > 'Adding Trusted Sites'. The right pane shows the 'Adding Trusted Sites' task with the 'Details' tab selected. Under 'Links', a table lists linked sites. Below this, the 'Security Filtering' section is visible, showing a list of groups, users, and computers that can receive the GPO settings. One entry, 'Accounting Computers (CONTOSO\Accounting Computers)', is circled in red.

**Adding Trusted Sites**

Scope Details Settings Delegation Status

**Links**

Display links in this location: Contoso.local

The following sites, domains, and OUs are linked to this GPO:

Location	Enforced	Link Enabled	Path
Desktop Computers	No	Yes	Contoso.local/Cor

**Security Filtering**

The settings in this GPO can only apply to the following groups, users, and computers:

Name
Accounting Computers (CONTOSO\Accounting Computers)

Buttons: Add... Remove Properties

- The primary goal of Group Policy is to apply configuration settings on the client machines. The settings used to:
  - create a consistent and seamless experience for users across the domain.
  - ensure that users not have access to features and functions that could compromise enterprise security efforts.
  - control what software is installed, where folders are located on the network, access and rights to various Windows features,...

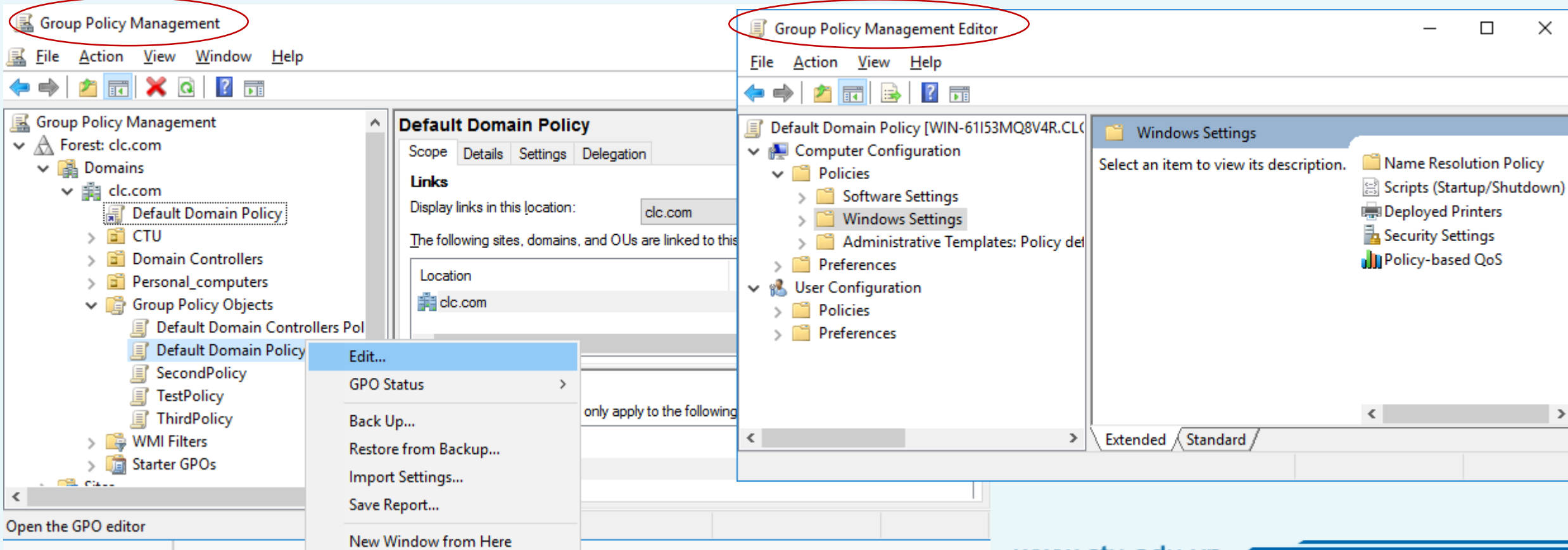


CANTHO UNIVERSITY

# Group Policy

## Configuring Group Policy Settings

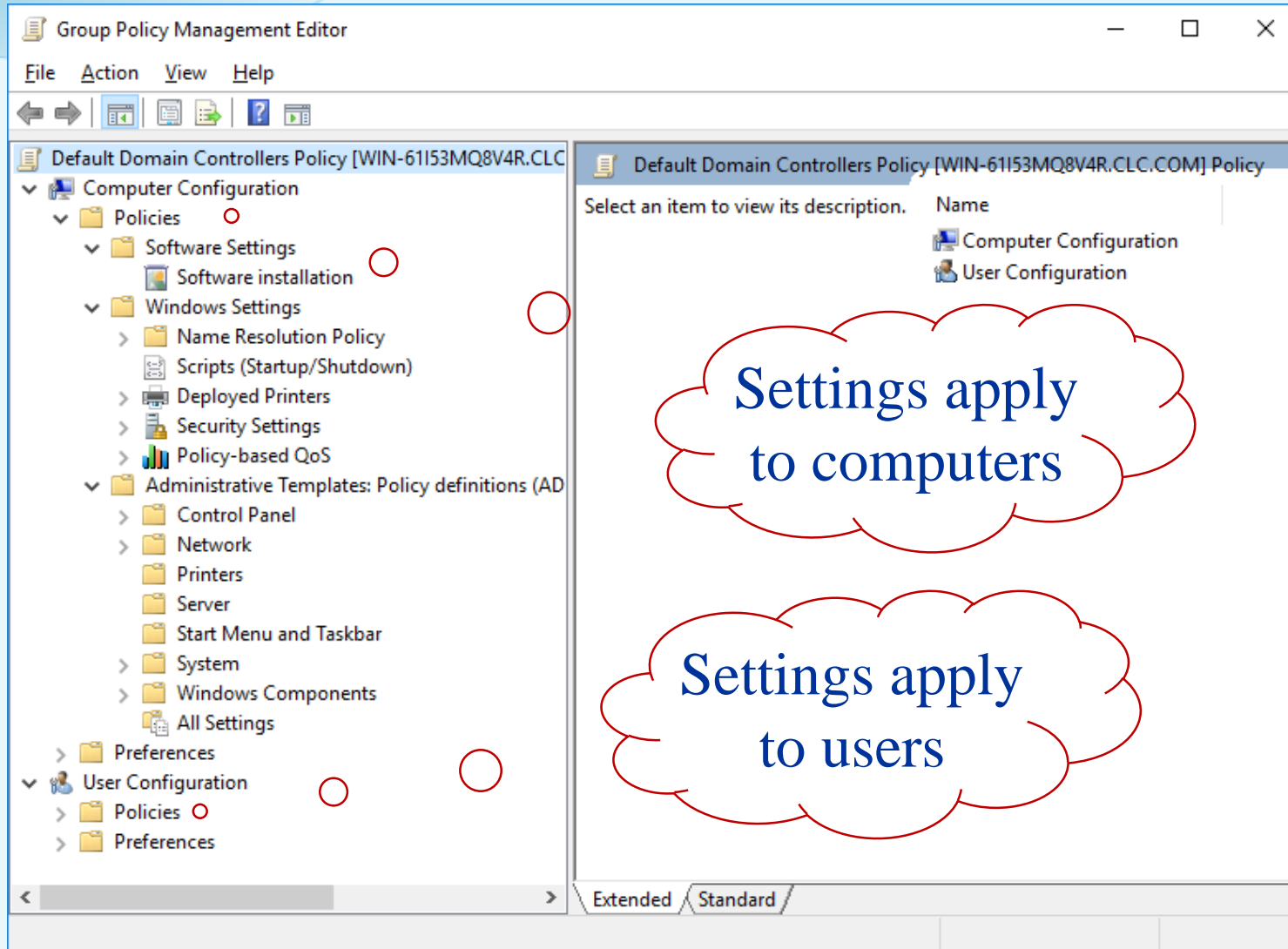
To manage GPOs, in Server Manager, Click Tools, and choose Group Policy Management.





# Group Policy

## Configuring Group Policy Settings



Two distinct sets of policies:

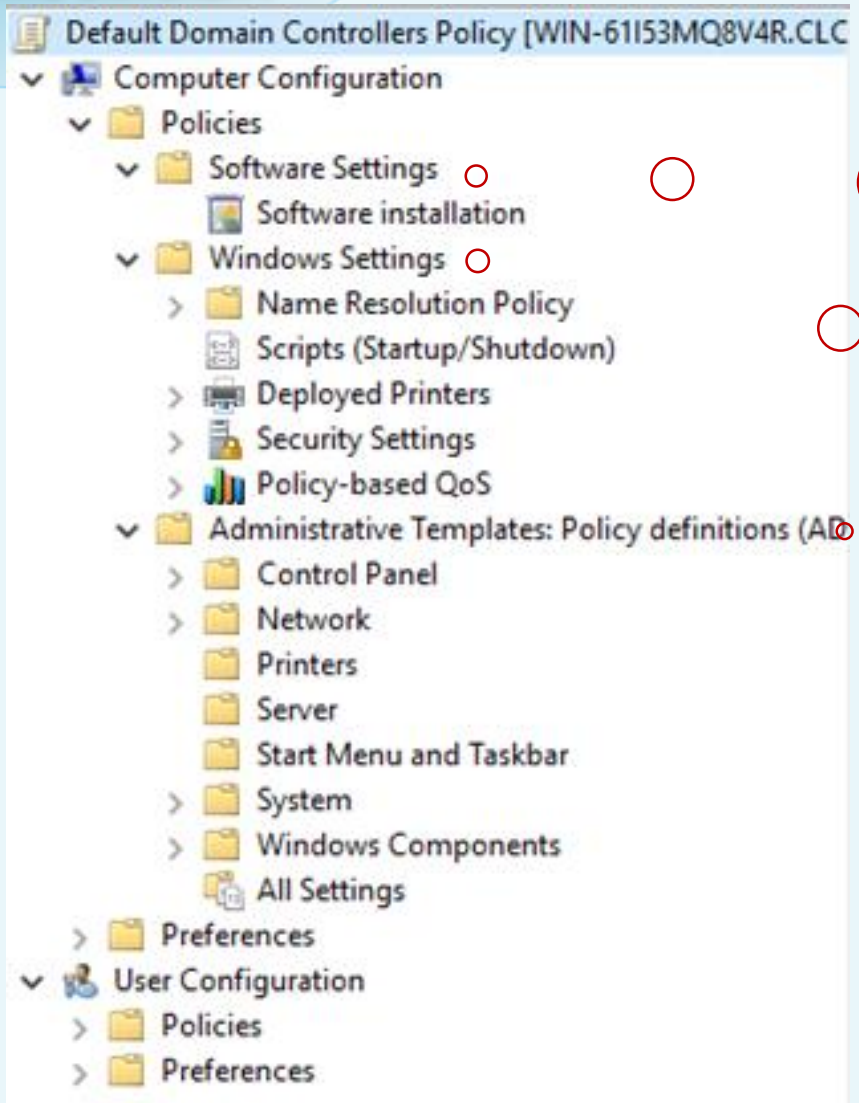
- **Computer policies:** Settings apply to computers and triggered when a computer is started
- **User policies:** Settings apply to users and triggered when a user logs on to a computer





# Group Policy

## Configuring Group Policy Settings



For automated  
deployment of new  
software and  
software upgrades

For managing key  
Windows settings:  
scripts, security,  
Remote Installation,...

For managing  
registry settings

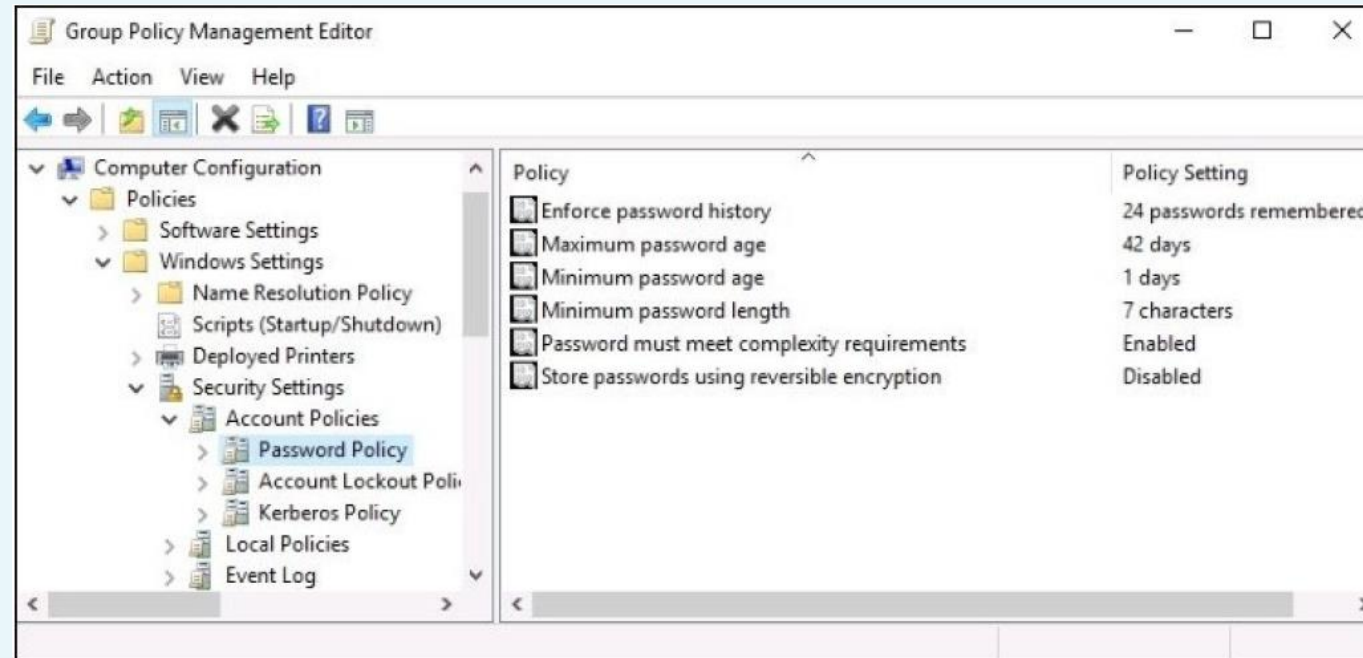


CANTHO UNIVERSITY

# Group Policy

## Default Domain Policy

- Created during installation, and applies to every computer and user who is part of the domain
- A common place to enforce global password policies or security rules that need to apply to everyone





CANTHO UNIVERSITY

# Group Policy

## Default Domain Policy

- Default Domain Policy: a very quick and easy way to get settings configured and pushed out to everyone
- Settings change to this policy affect everyone in your domain, including yourself
- It is highly recommended that you stay away from the **Default Domain Policy**
- And instead set up a brand new GPO when need applied some settings



CANTHO UNIVERSITY

# Software Deployment



CANTHO UNIVERSITY

# Software Deployment

## Assigning Software

- Automatically distribute programs to client computers or users
- Distribute computer programs by using the following methods:
  - 1) *Assigning Software*: assign a program to users or computers
    - If assign the program to a user, it is installed when the user logs on to the computer.
    - If assign the program to a computer, it is installed when the computer starts, and it is available to all users who log on to the computer.

### 2) *Publishing Software:*

- Publish a program distribution to users.
- When the user logs on to the computer, the published program is displayed in the Add or Remove Programs dialog box, and it can be installed from there.

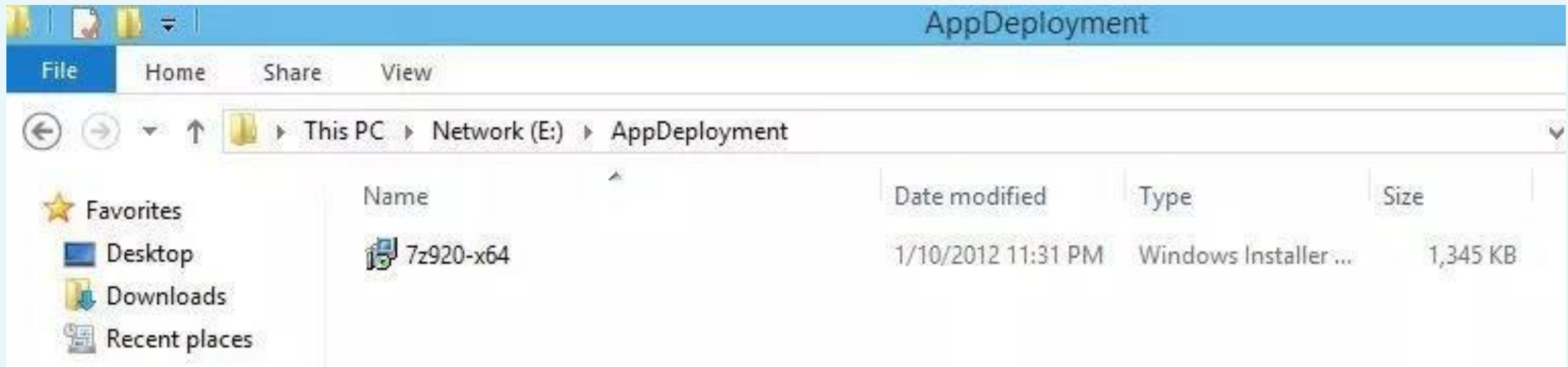


CANTHO UNIVERSITY

# Software Deployment

## Using Group Policy

1. **Create a folder** in Server and share it with appropriate permission for domain users to execute MSI files







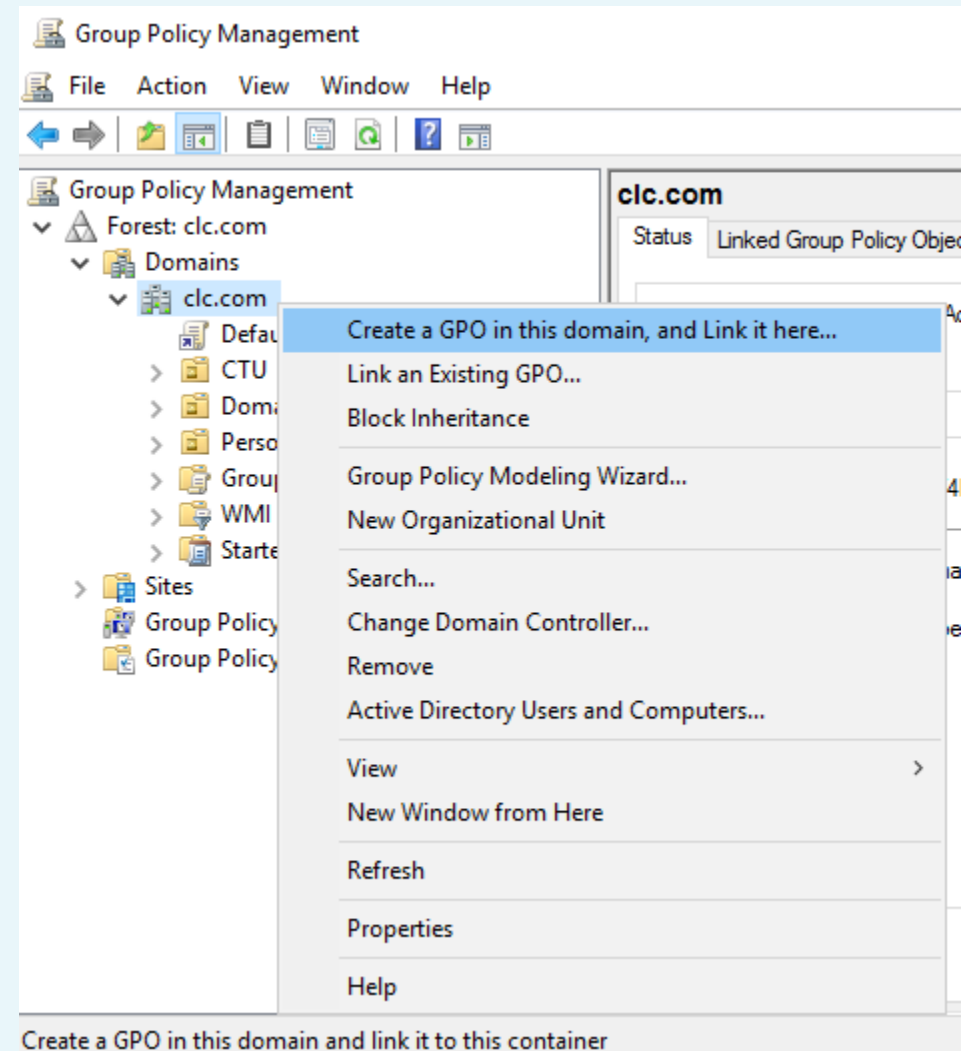
CANTHO UNIVERSITY

# Software Deployment

## Using Group Policy

### 2. Create a new Group Policy

- In Server Manager, click **Tools** and open **Group Policy Management**
- In the Group Policy Management console, right click domain name, and click **Create a GPO in this domain, and link it here.**



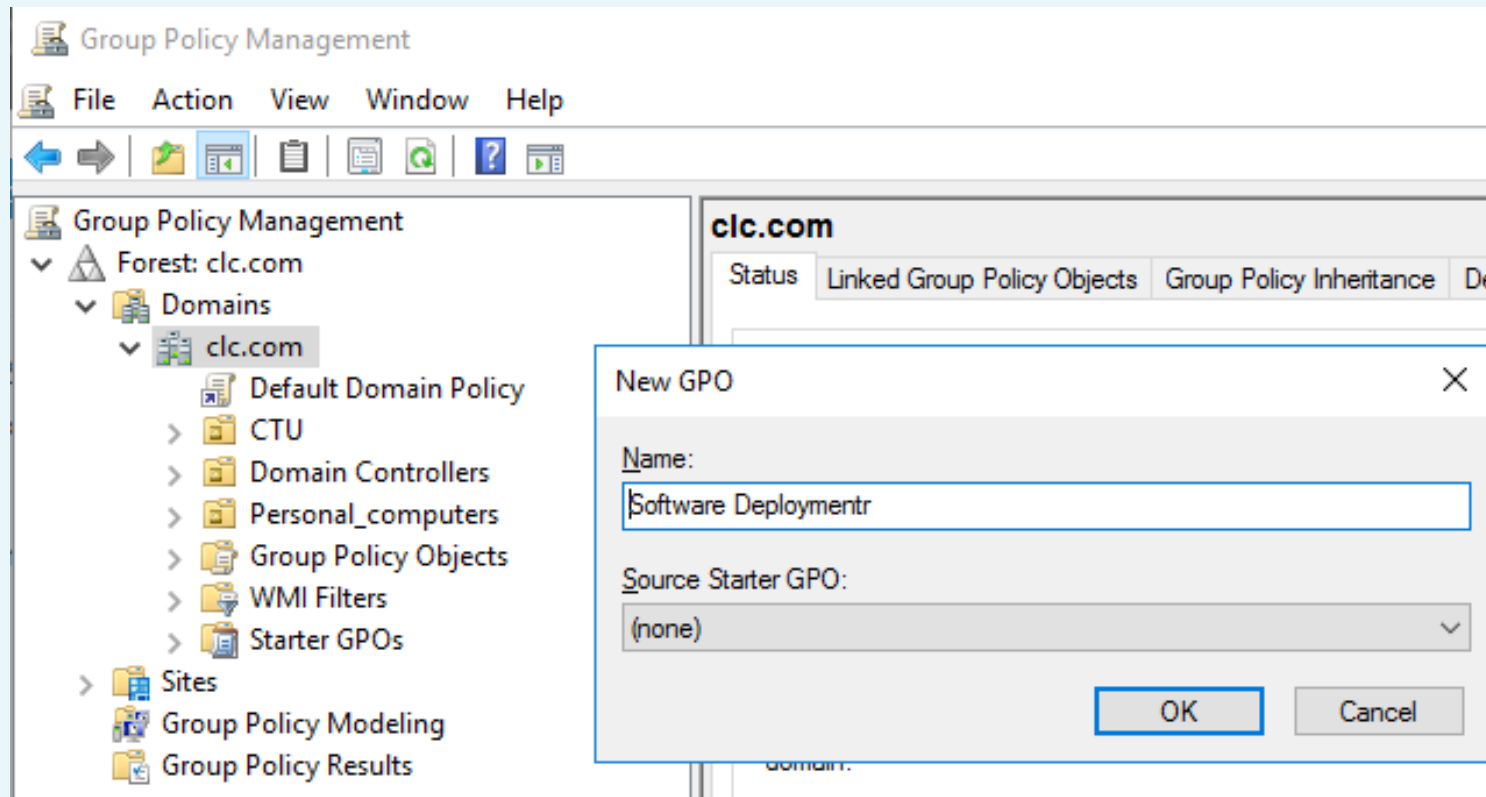


CANTHO UNIVERSITY

# Software Deployment

Using Group Policy

- In the New GPO box, in the Name box, type **Deploy Software**, and then click OK..





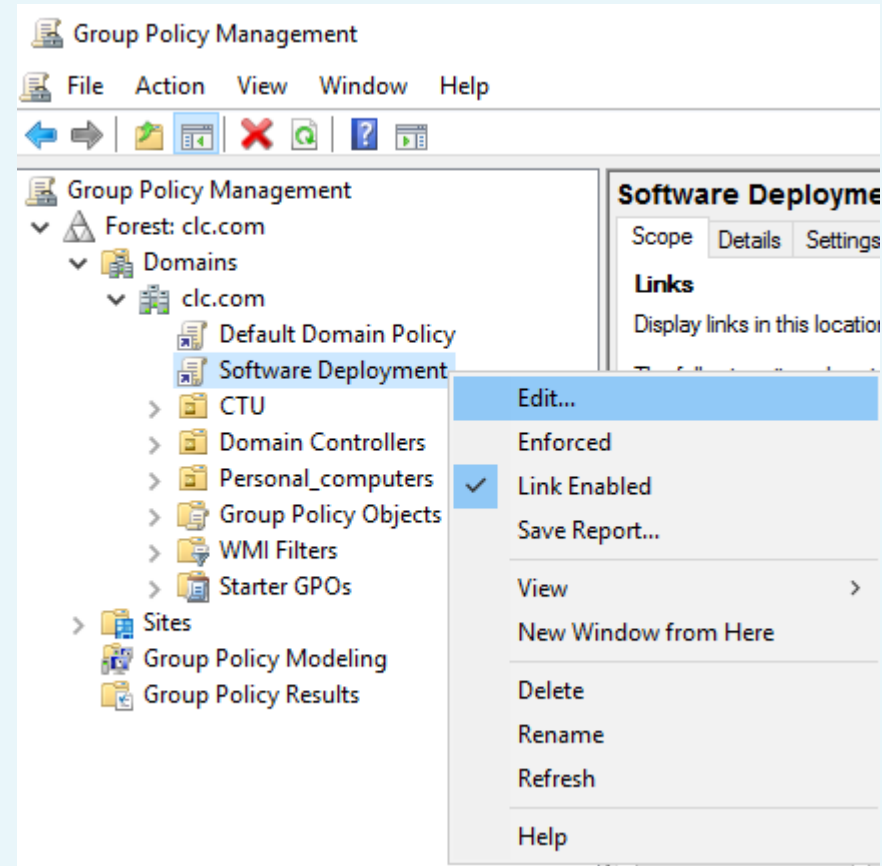
CANTHO UNIVERSITY

# Software Deployment

## Using Group Policy

### 3. Edit New GPO

In the **Group Policy Management** console, right click **Deploy Software GPO** and click **Edit**.



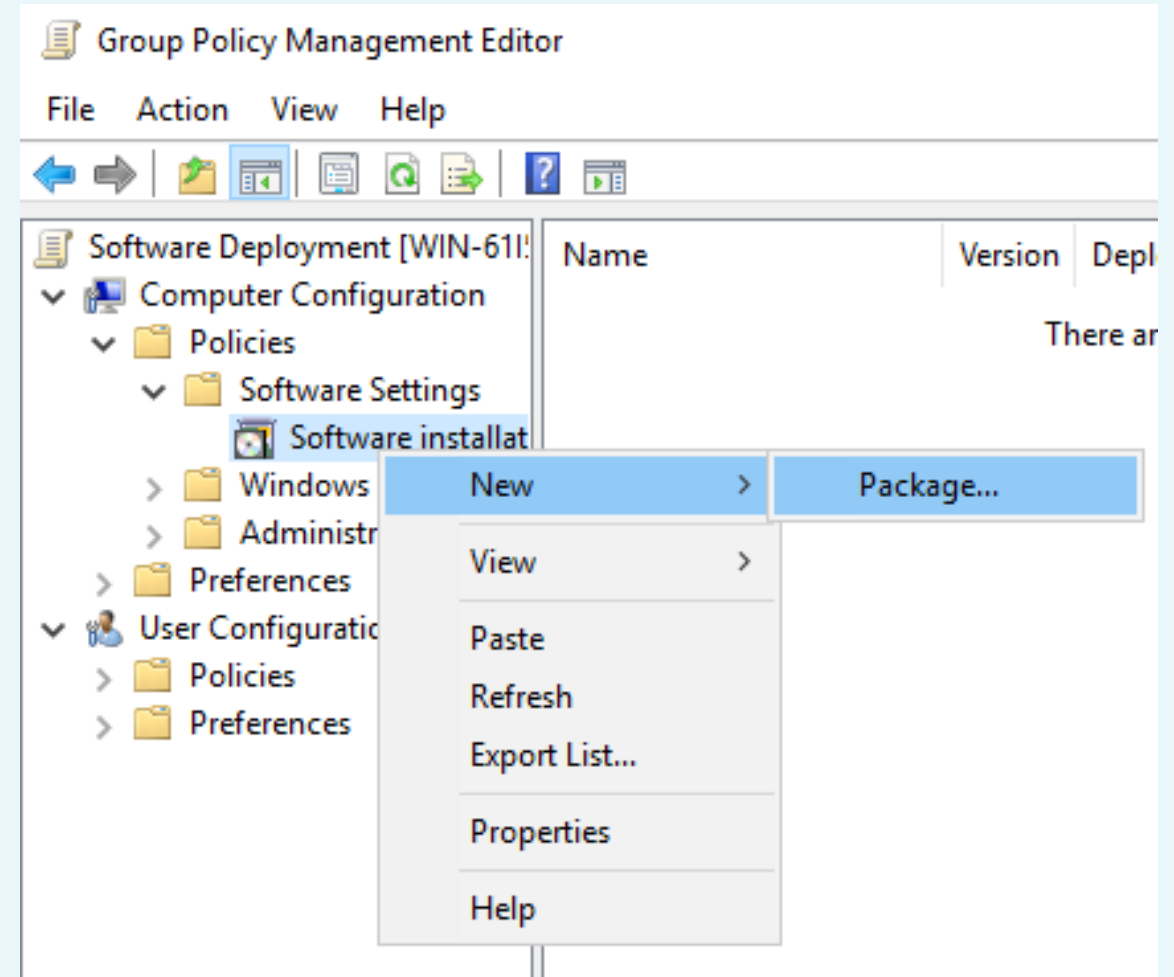


CANTHO UNIVERSITY

# Software Deployment

## Using Group Policy

- In the **Group Policy Management Editor**, under **Computer Configuration**, expand **Policies**, and then expand **Software Settings**
- Right-click **Software installation**. From the context menu, click **New**, and then click **Package**.



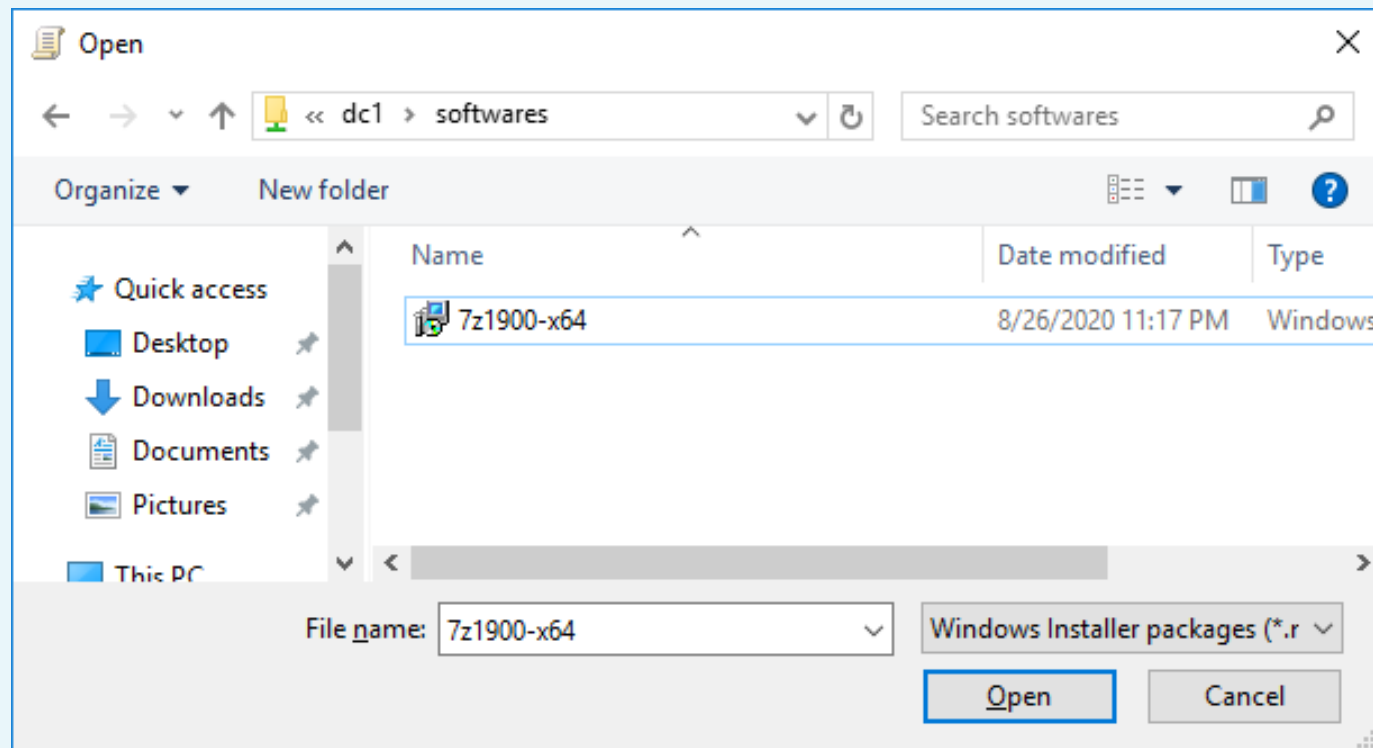


CANTHO UNIVERSITY

# Software Deployment

## Using Group Policy

- In the opened window, using the UNC path of the software select the software MSI file you want to deploy (e.g., 7zip software) to clients.



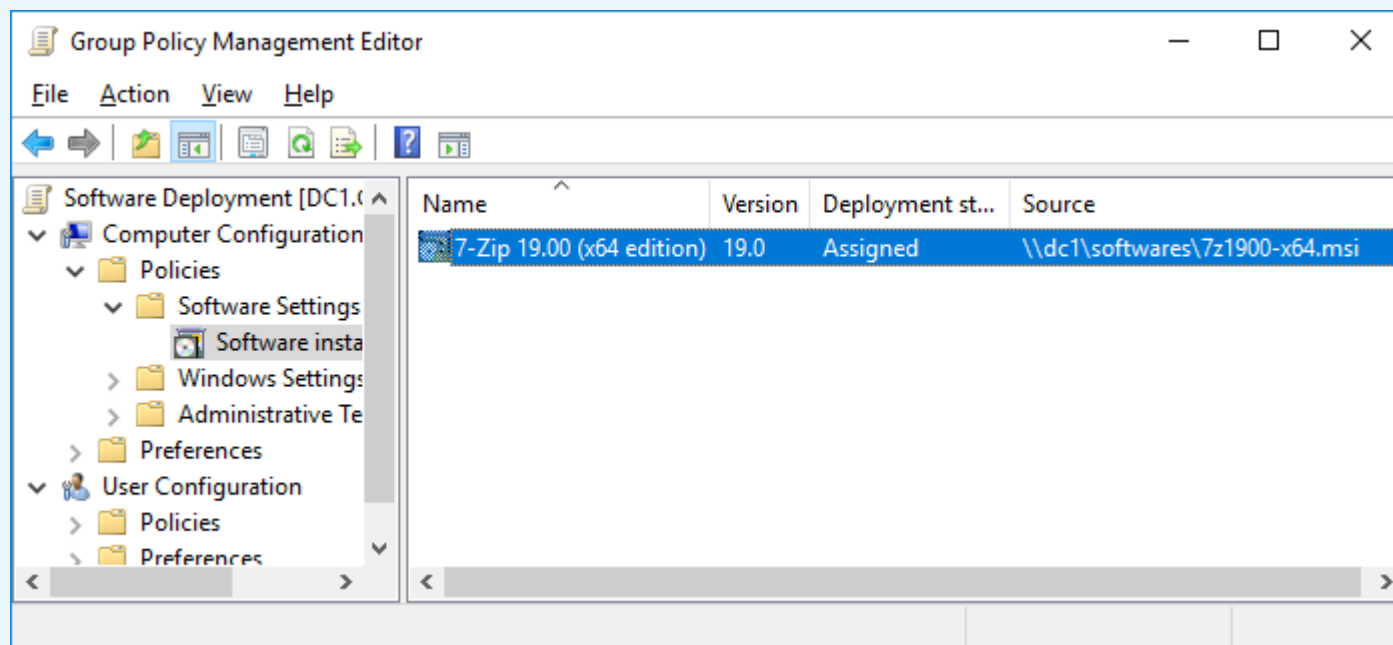
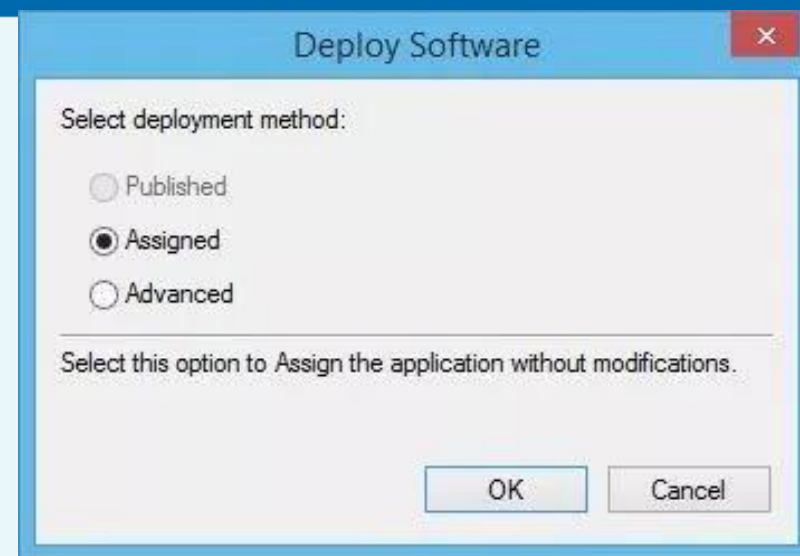


CANTHO UNIVERSITY

# Software Deployment

Using Group Policy

- In the Deploy Software window, ensure that the Assigned option is selected, and then click OK.



- Wait for few second and verify that the 7-zip is listed in the GPME

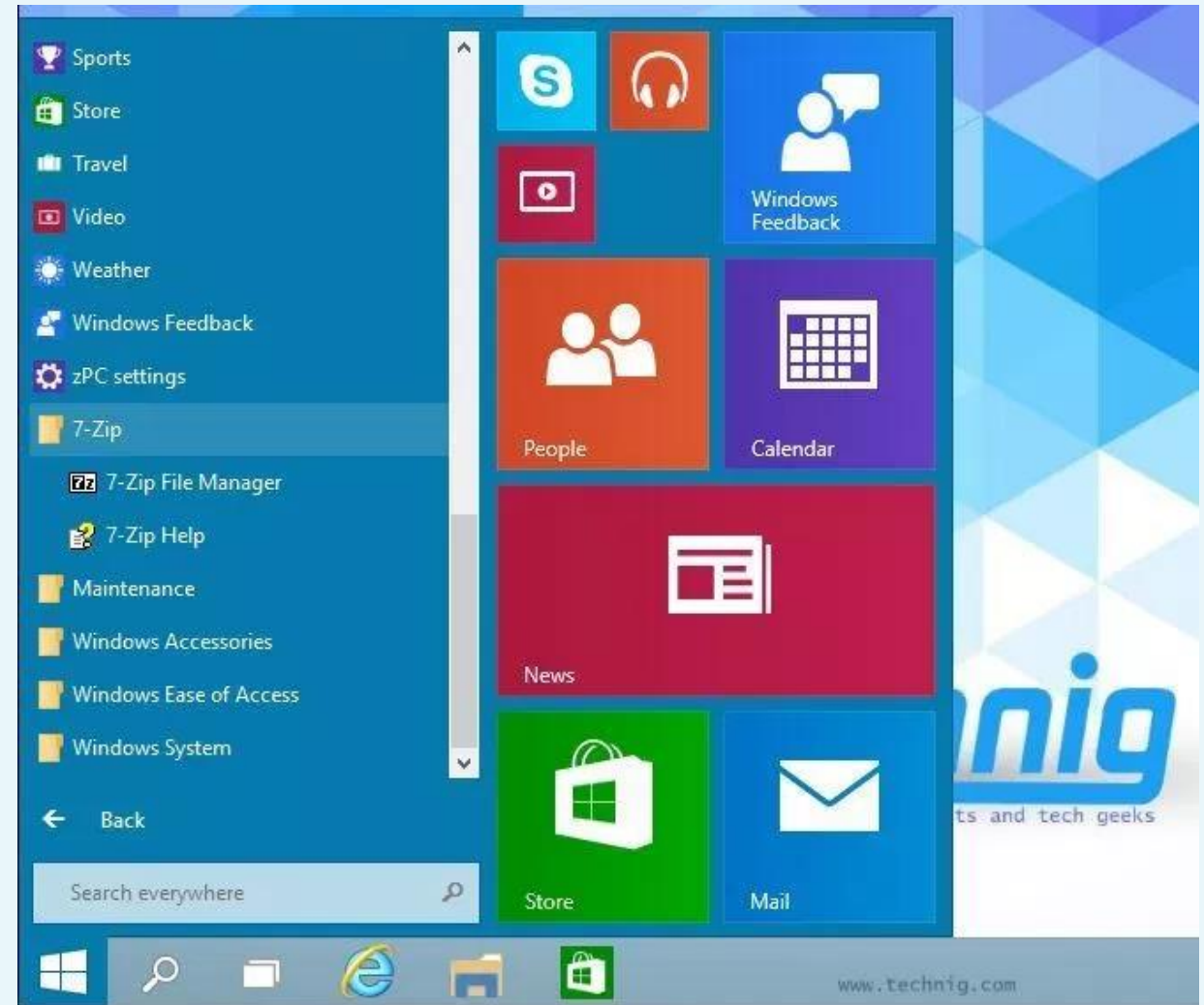




# Software Deployment

## Testing Software Deployment

- Now let's switch to our Windows 10 client PC, and run **gpupdate /force** in the client PC and then restart the client PC.
- After restarting your client PC and log in as domain user, you can verify that 7-zip is installed.







CANTHO UNIVERSITY

# Summary

- Group Policy Objects and GPOs
- GPO processing order
- Configuring Group Policy Settings
- Default Domain Policy
- Software deployment