

COMODO
Creating Trust Online®



Comodo IT and Security Manager

Software Version 6.9

Bulk Enrollment via Active Directory

Guide Version 6.9.072717

Comodo Security Solutions
1255 Broad Street
Clifton, NJ 07013

ITSM – Bulk Enrollment via Active Directory

This tutorial briefly explains how you can install the ITSM agent on multiple Windows endpoints using Active Directory and group policy (GPO) and enroll them for management.

Software Requirements

- AD Server – Windows Server 2008 or higher
- Endpoints – Windows 7 or higher

Please note the method described below for creating a group policy (GPO) and deploying them is for Windows Server 2008 Standard. The steps may vary slightly for other Window server versions.

Step 1 – Configure the offline ITSM package

The ITSM agent is unique for each company and user. All endpoints that have an agent installed upon them will be listed under the logged in user name or as configured in the 'User' field on the form below.

- To configure the offline package, click 'Devices on the left then 'Bulk Installation Package'

Offline Package - Form Parameters	
Parameter	Description
User	Devices that are enrolled by installing the agent through

	<p>AD Group Policy are assigned to the currently logged-in administrator by default. If you want the devices to be assigned to a different user, specify the user in this field.</p> <ul style="list-style-type: none"> Start typing the first few characters of the name of the user in the text field and choose the user from the options that appear.
Company	<p>Choose the company to which the endpoints should be assigned. This field applies to C1 MSP customers only and is not available for C1 Enterprise / ITSM stand-alone customers.</p>
Device Group	<p>The drop-down displays the list of device groups added to ITSM</p> <ul style="list-style-type: none"> Choose the device group to which the enrolled devices should be added. <p>When enrollment is complete, the device group configuration profiles will be applied to the endpoints.</p>
Comodo Client	<p>Allows you to choose the components to be added to the installation package. The available options are:</p> <ul style="list-style-type: none"> Choose operating system – Select the operating system of the target endpoints. The options are: Windows x64, Windows x86, Windows x86 & 64 and MacOS. Communication - Adds Comodo One Client - Communication agent to the installation package. This is required for the endpoints to connect to ITSM. Security - Adds the endpoint security product, Comodo One Client - Security (CCS) to the installation package. <p>To create an installation package in MSI/MST format purely for bulk enrollment through AD, leave 'Communication' selected and leave 'Security' deselected. You can remotely install CCS later on target endpoints from the ITSM console.</p> <p>The rest of the configuration options related to CCS will be grayed out if 'Security' is not selected.</p>
Restart Control Options	<p>CCS requires endpoint(s) to be restarted for the installation to take effect. You can configure the restart options:</p> <ul style="list-style-type: none"> To restart the end-point a certain period of time after installation, choose 'Force the reboot in...' and select the delay period from the drop-down. A warning message will be displayed to the user and the endpoint will be restarted automatically when the time period elapses. To continue without restarting, choose 'Suppress reboot'. The installation will take effect only when the user restarts the endpoint.

	<ul style="list-style-type: none"> To restart the end-point at the user's convenience, choose 'Warn about reboot and let user(s) postpone the reboot'. Enter a message to be displayed to the user in the 'Reboot Message' field. The message dialog will be displayed to the user when installation is complete. The user can choose to restart the endpoint immediately by clicking 'Reboot now' or postpone the restart until a later time.
<p>UI Options</p>	<p>Allows you configure the messages to be displayed to the user regarding the CCS installation status.</p> <p>If you wish the user to be notified about an unsuccessful installation, select 'Show error messages if installation failed'</p> <p>If you wish the user to be notified about a successful installation, choose 'Show a confirmation message upon completion of installation' and enter a message in the 'Confirmation Message' field.</p>
<p>Proxy Settings</p>	<p>Proxy settings allows you to specify a proxy server through which Comodo Client Security (CCS) and Comodo Client Communication (CCC) in the endpoints should connect to ITSM management portal and Comodo servers. If you choose not to set these, then CCS and CCC will connect directly as per the network settings.</p> <ul style="list-style-type: none"> Enter the IP address/hostname of the proxy server and port in the respective fields. Enter the user-name and password of an administrative account on the proxy server in the Proxy Login and Proxy Password fields <p>Note: If proxy is used then it is mandatory to configure the same proxy settings in client proxy settings in the profile(s) applied to the enrolled devices.</p>

- If you do not wish to use a proxy server for CCS and CCC then click 'Download Installer' after configuring user, company, group and client options.
- If you wish to use a proxy then additionally complete the 'Proxy settings' section and click 'Download MST File'

Please note .mst file can be added to the GPO only after .msi has been configured as explained in the below steps.

Step 2 – Download the ITSM agent

The next step is to download the ITSM agent for Windows devices.

- Read the EULA in full by clicking the 'End User License Agreement' link.
- Click 'Download Installer' to download the agent setup file for direct installation via Group Policy Object (GPO),

The agent package will be downloaded in .msi format. You can save the file on the AD server from where you want to enroll the endpoints, and create a software installation policy for deployment to network endpoints. After the agent is installed, it will establish communications with ITSM to begin importing the device.

- To download the installation file to include a proxy server for CCC and CCS communication to ITSM and

Comodo servers, click 'Download MST File'

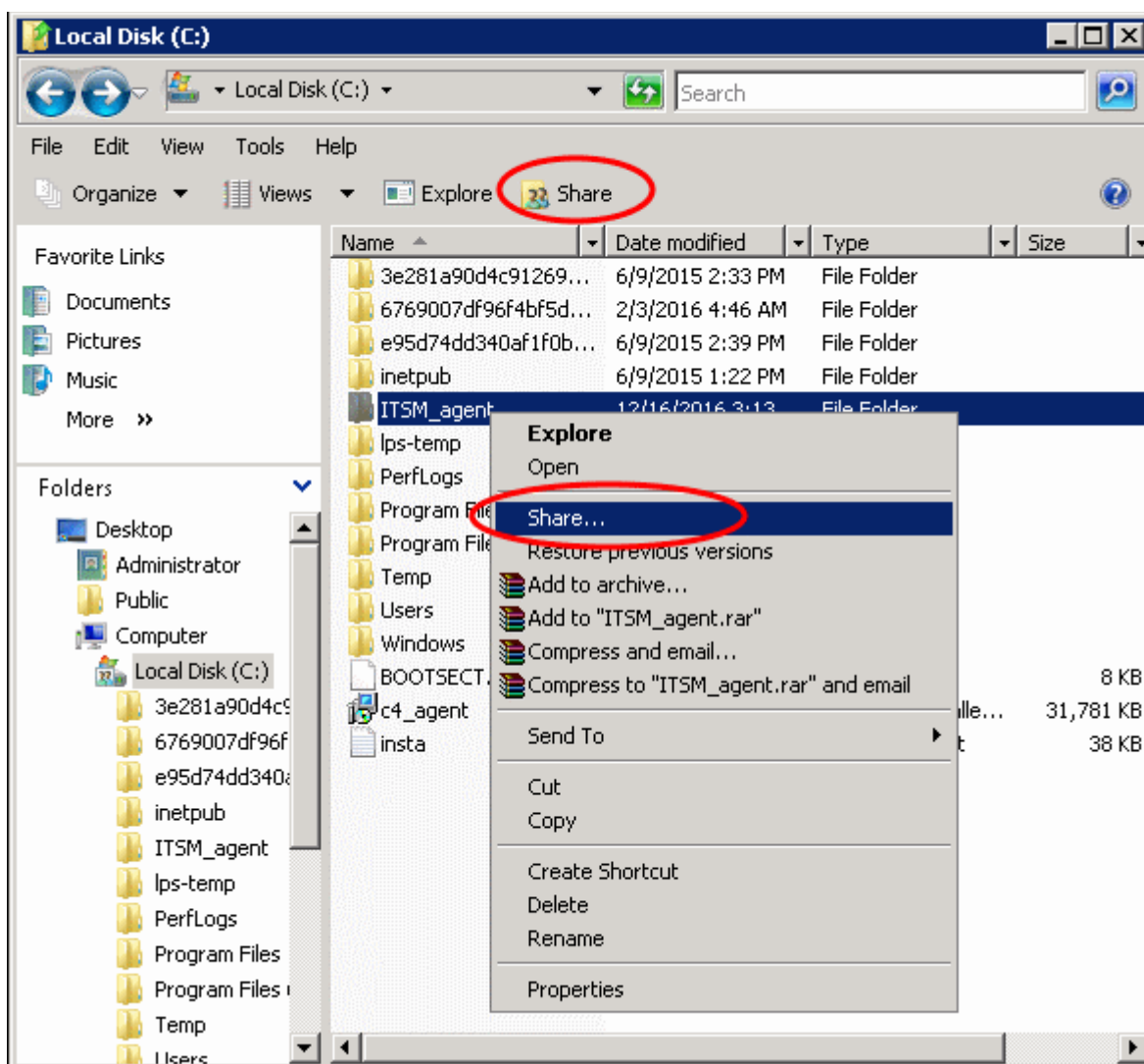
ITSM will create a .mst transform file containing the proxy server installation commands. As above, you can save the file on the AD server from where you want to enroll the endpoints, and add to the GPO created for .msi file. After the agent is installed, it will establish communications with ITSM via the configured proxy servers to begin importing the device.

After downloading the agent, save it on the AD server from where you want to enroll the endpoints.

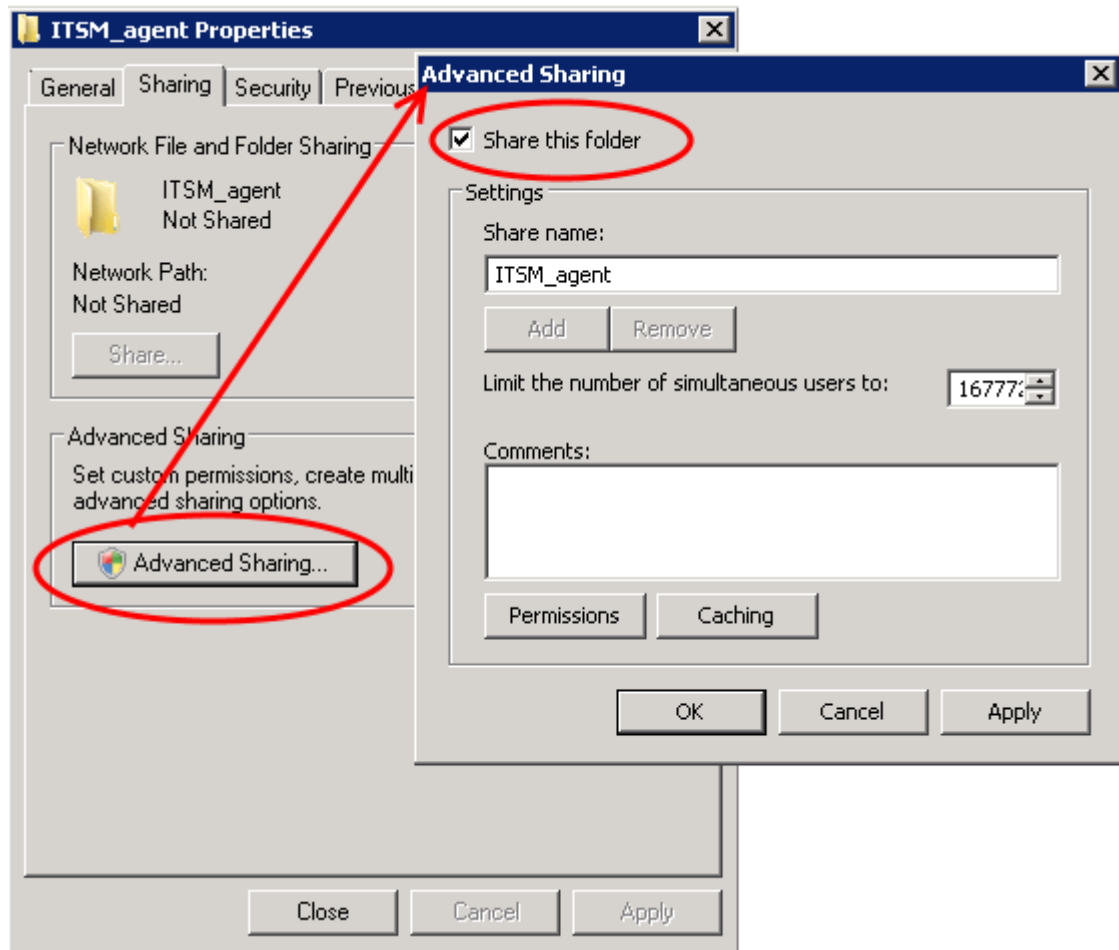
Step 3 – Create a shared network folder and configure permission level

Now that you have downloaded the .msi agent setup file, the next step is to create a shared folder in the network.

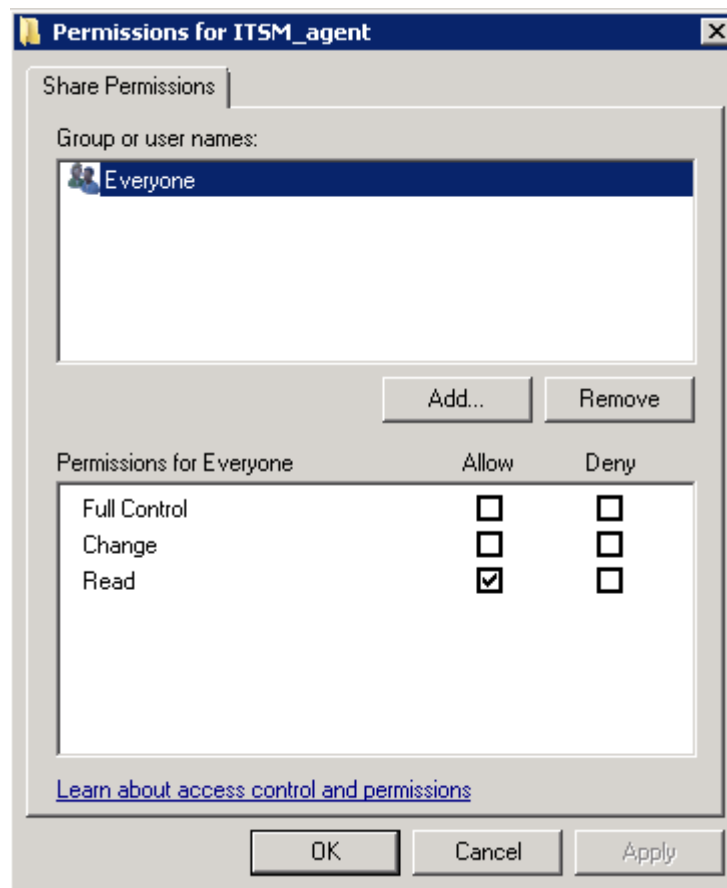
- Create a new folder in your desired location
- Name the folder appropriately. For example ITSM_agent
- Select the folder, right-click and select 'Share' or from the menu toolbar



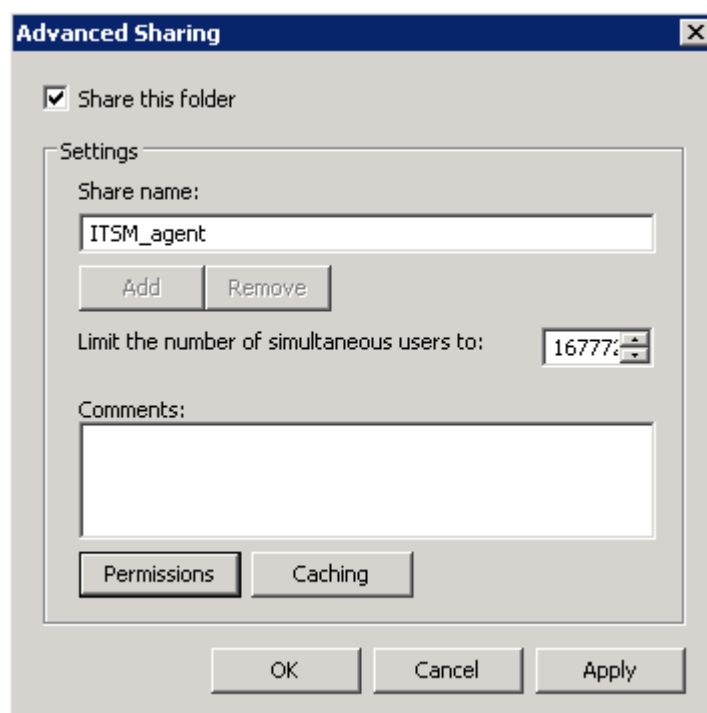
- Click 'Advanced Sharing...', then select the 'Share this folder' check box



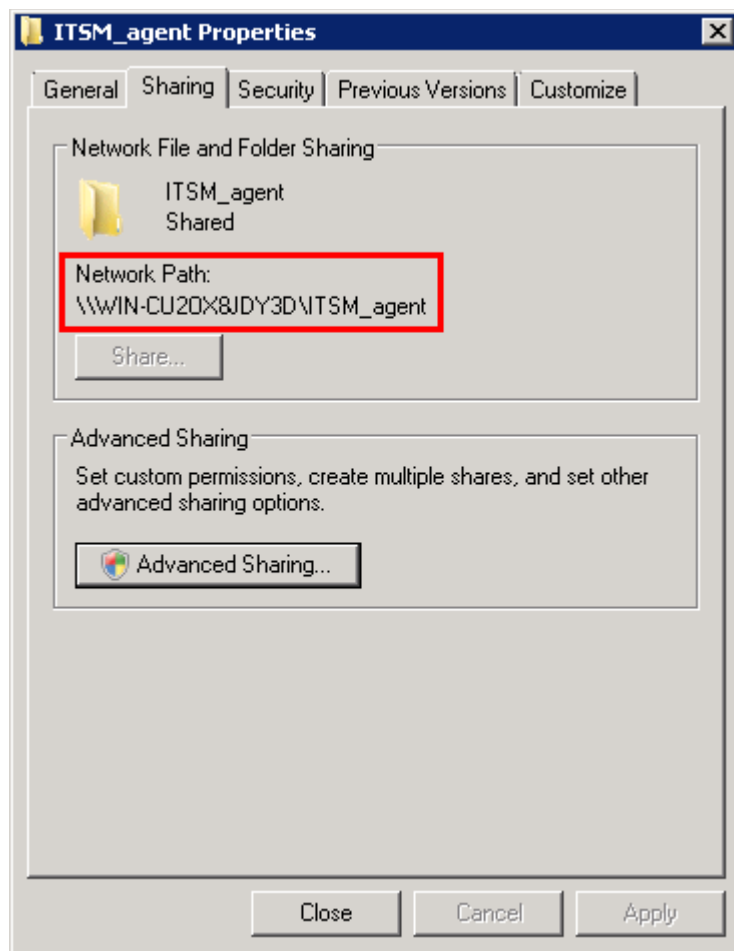
- Click 'Permissions'. By default, 'Everyone' will be selected. Since all endpoints need to have at least read access to this shared folder, make sure the permission is configured for 'Everyone'



- Ensure the 'Permission Level' is set to 'Read' and click 'OK'.



- Click 'Apply', then 'OK' in the 'Advanced Sharing' dialog.



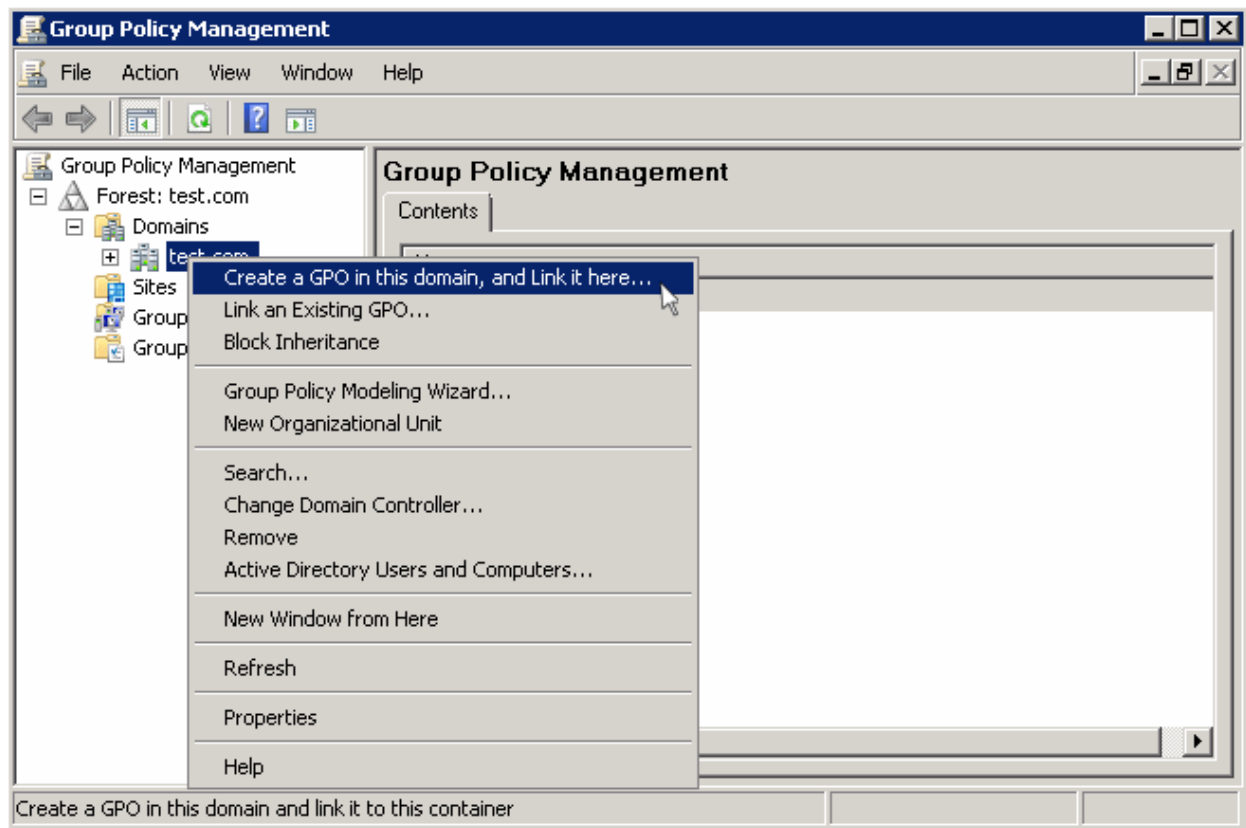
- Note down the location of this shared folder and click the 'Close' button

Follow the similar steps to create a shared file location for .mst file, if required.

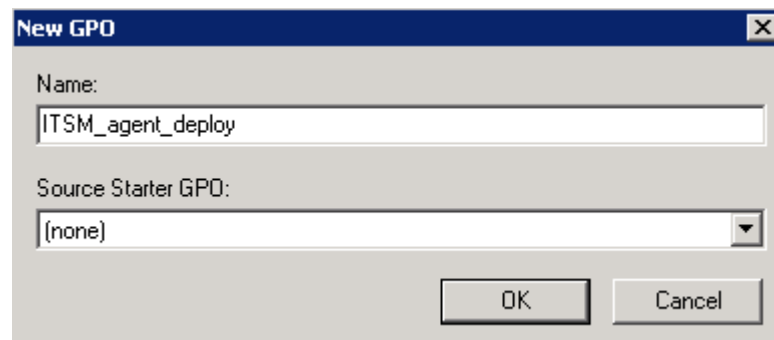
Step 4 – Create a Group Policy and Assign the package

The next step is to create a group policy that will install the ITSM agent onto the endpoints.

- Click 'Start' > 'Administrative Tools' > 'Group Policy Management'
- Right-click on the domain name and select the 'Create a GPO in this domain and Link it here...' option



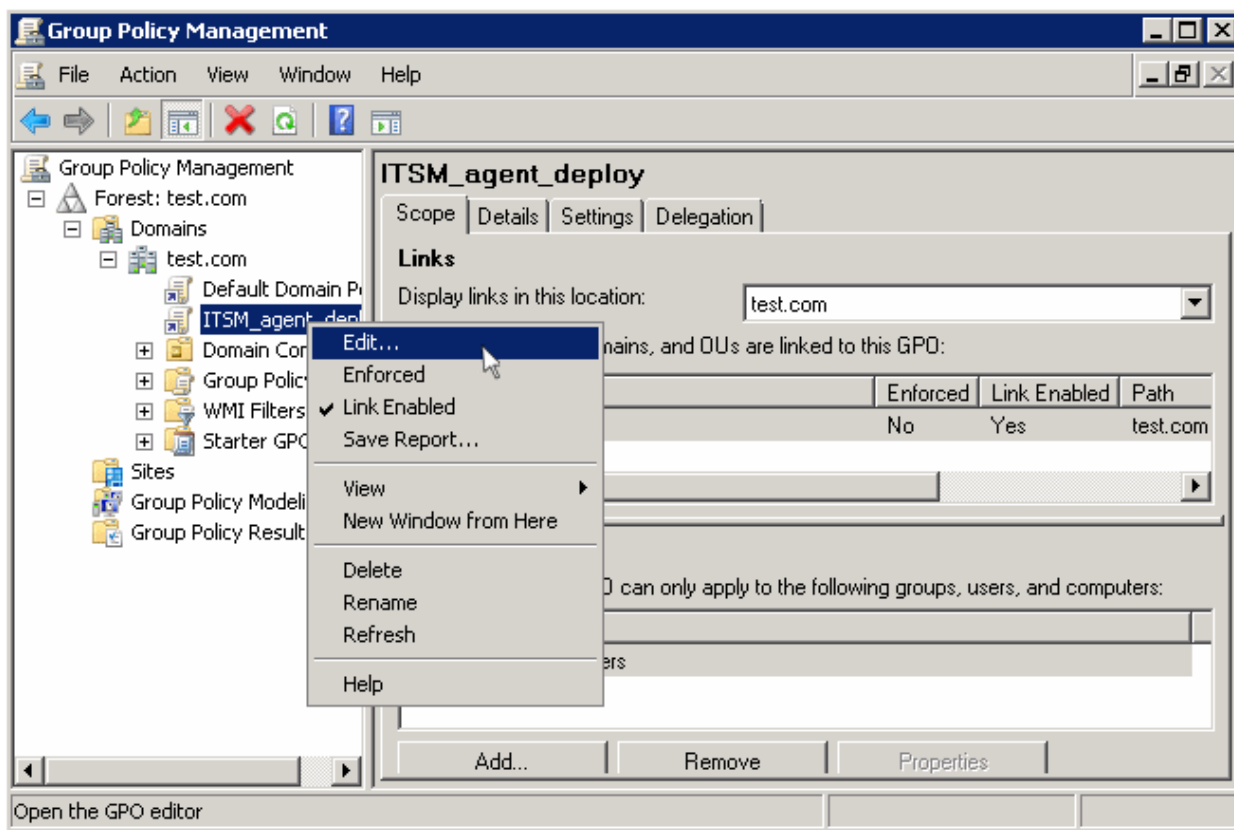
- .Enter a name for the group policy in the 'New GPO' dialog



- Click 'OK'

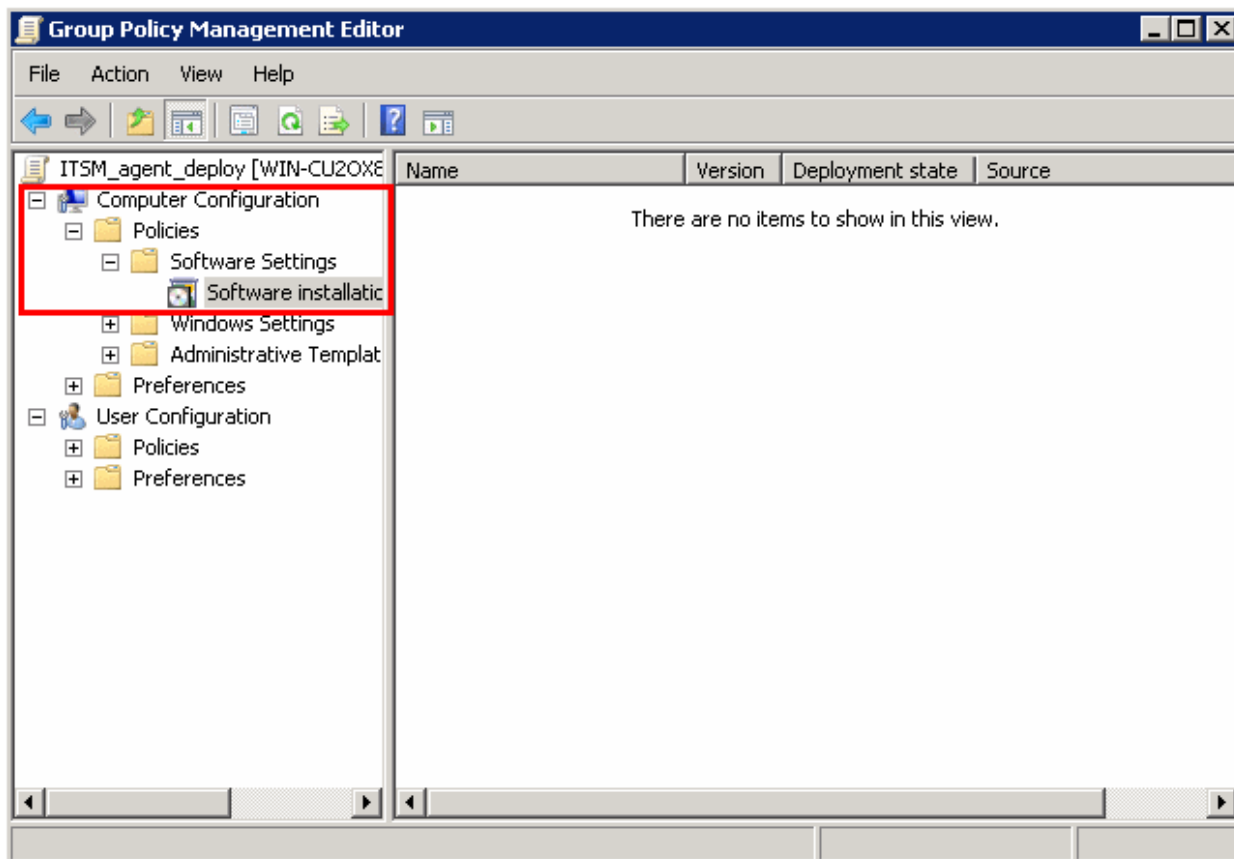
The newly added group policy will be listed.

- Right-click on the policy and click the 'Edit' option

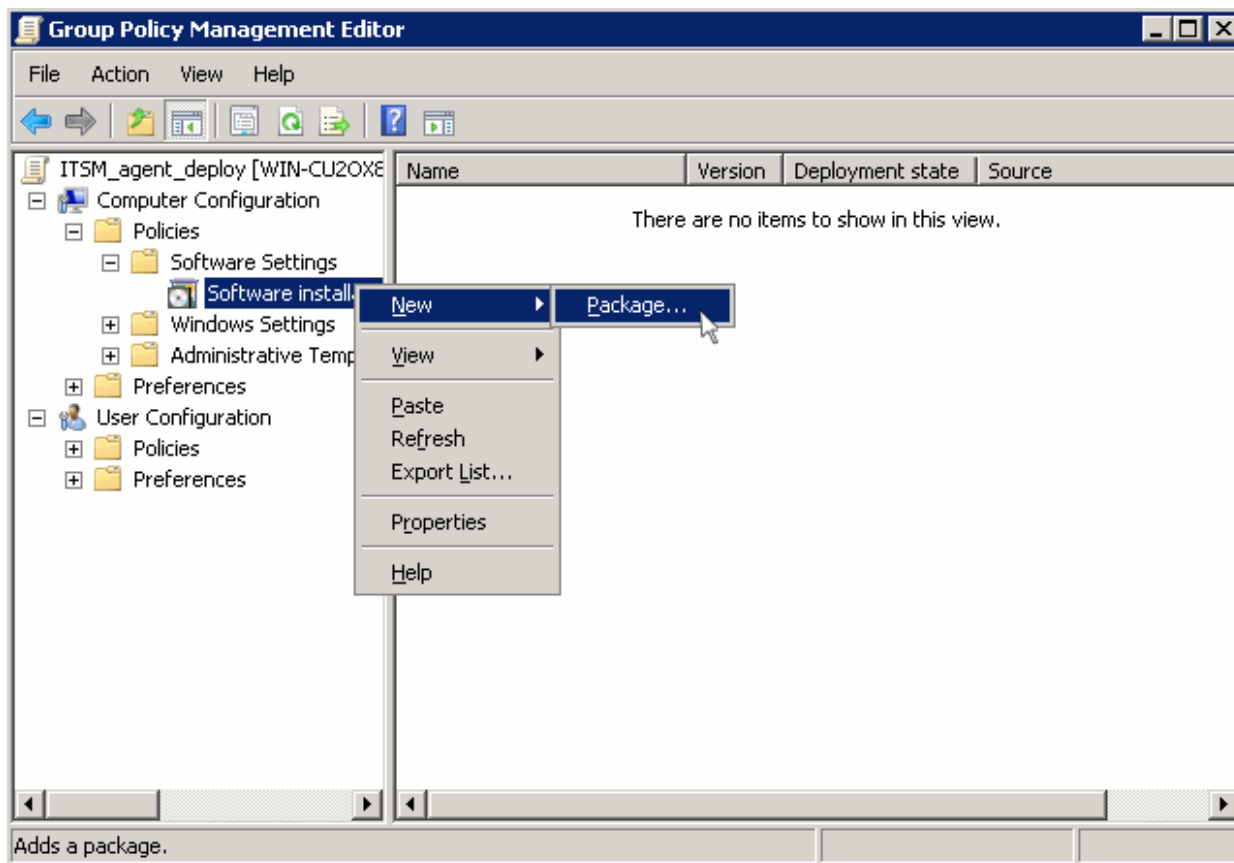


The 'Group Policy Management Editor' will be displayed.

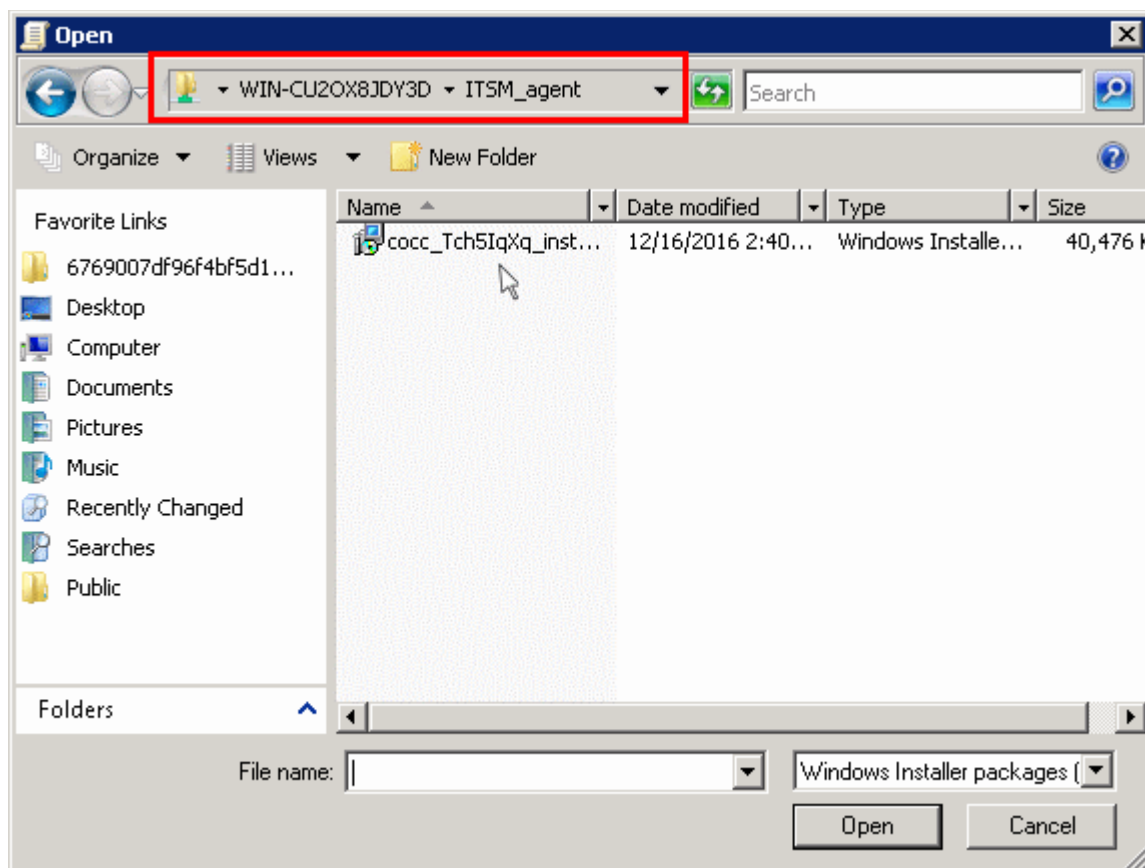
- Expand 'Computer Configuration' > 'Policies' > 'Software Settings'



- Right-click on 'Software installation' and select 'New' > 'Package'



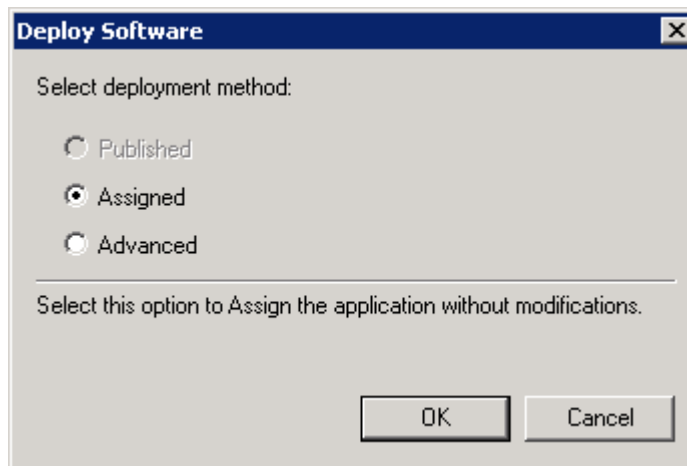
- In the 'Open' dialog, enter the path of the shared folder that was noted before, select the file and click the 'Open' button



- Select the file and click 'Open'

- In the 'Deploy Software' dialog, select 'Assigned'

Note: If you want to add the MST file also to the GPO, then select 'Advanced' and move to 'Deploy Software' instruction in Step 6. If you want to add the .mst file later then see the instructions from Step 6.

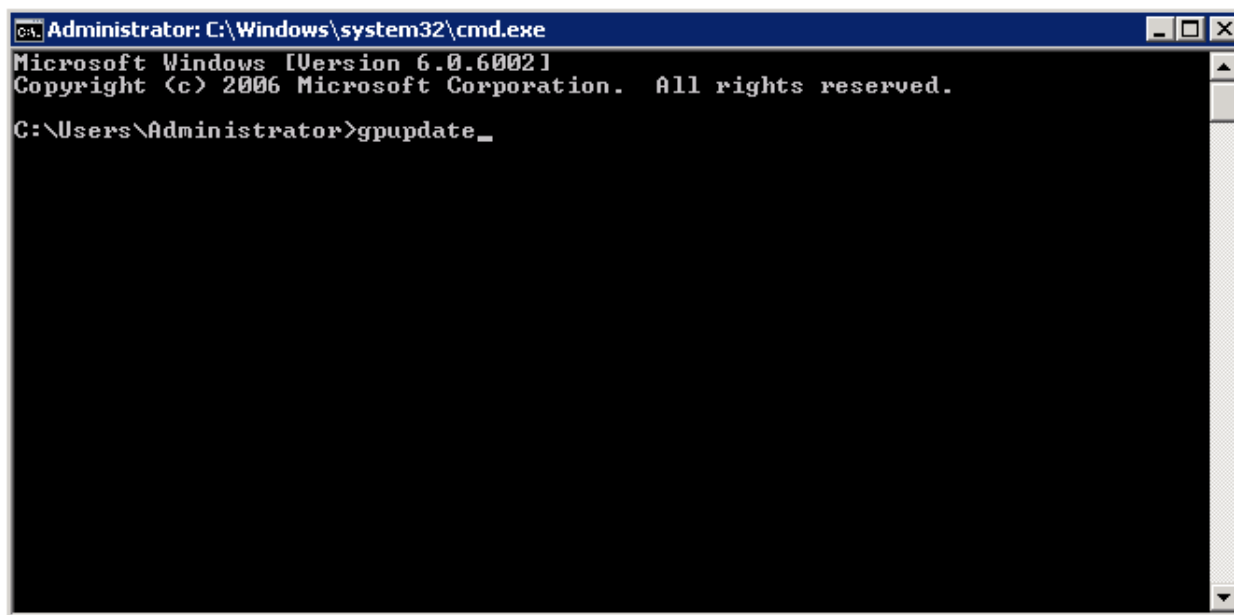


- Click 'OK'

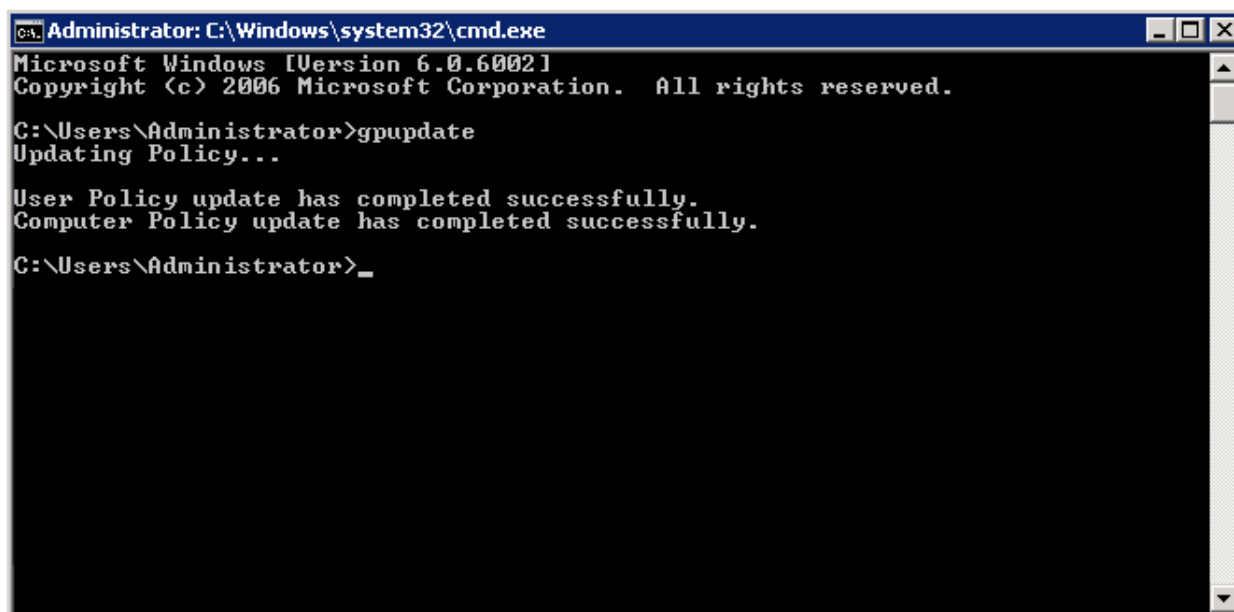
Step 5 – Run a GPO update

In order to install the ITSM agent, you need to run a GPO update in the command prompt.

- Open the command prompt, type “gpupdate” and press enter.



The group policy update will run and a confirmation message displayed:



```
Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.0.6002]
Copyright (c) 2006 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>gpupdate
Updating Policy...

User Policy update has completed successfully.
Computer Policy update has completed successfully.

C:\Users\Administrator>_
```

After the group policy has been successfully updated, the endpoints must be restarted for the ITSM agent to be installed.

That's it. You have now successfully enrolled Windows endpoints via AD using the GPO method. You can see the endpoints listed in the 'Devices List' screen.

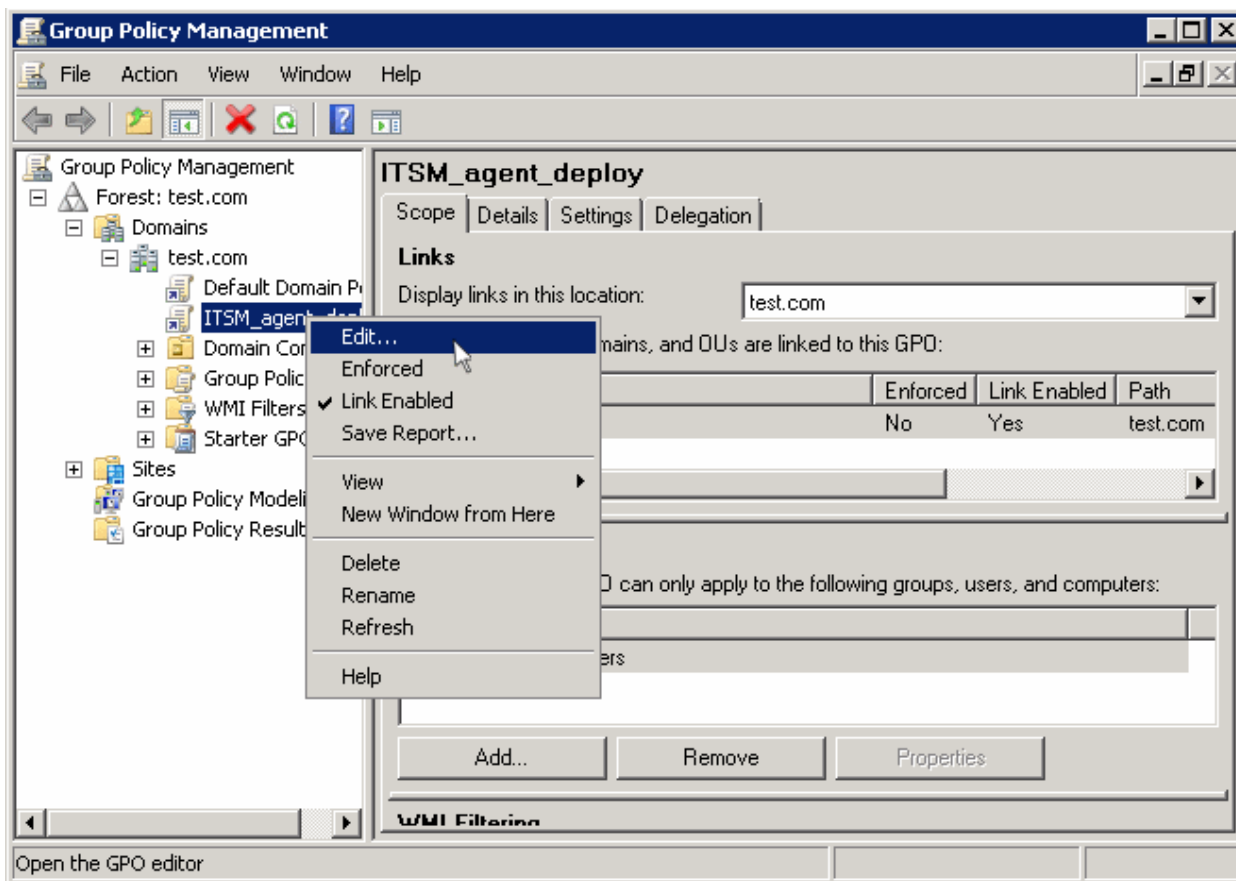
Note: You may get an error message if you try to manually install the ITSM agent on an endpoint where the GPO was deployed and then removed. Visit the Microsoft support site at https://support.microsoft.com/en-us/mats/program_install_and_uninstall and run the tool on the endpoint.

The device group policy that was selected in the enrollment form will be applied to the enrolled devices automatically. If you have configured proxy settings and downloaded the .mst file then go to Step 6 to add the MST file to the newly created GPO.

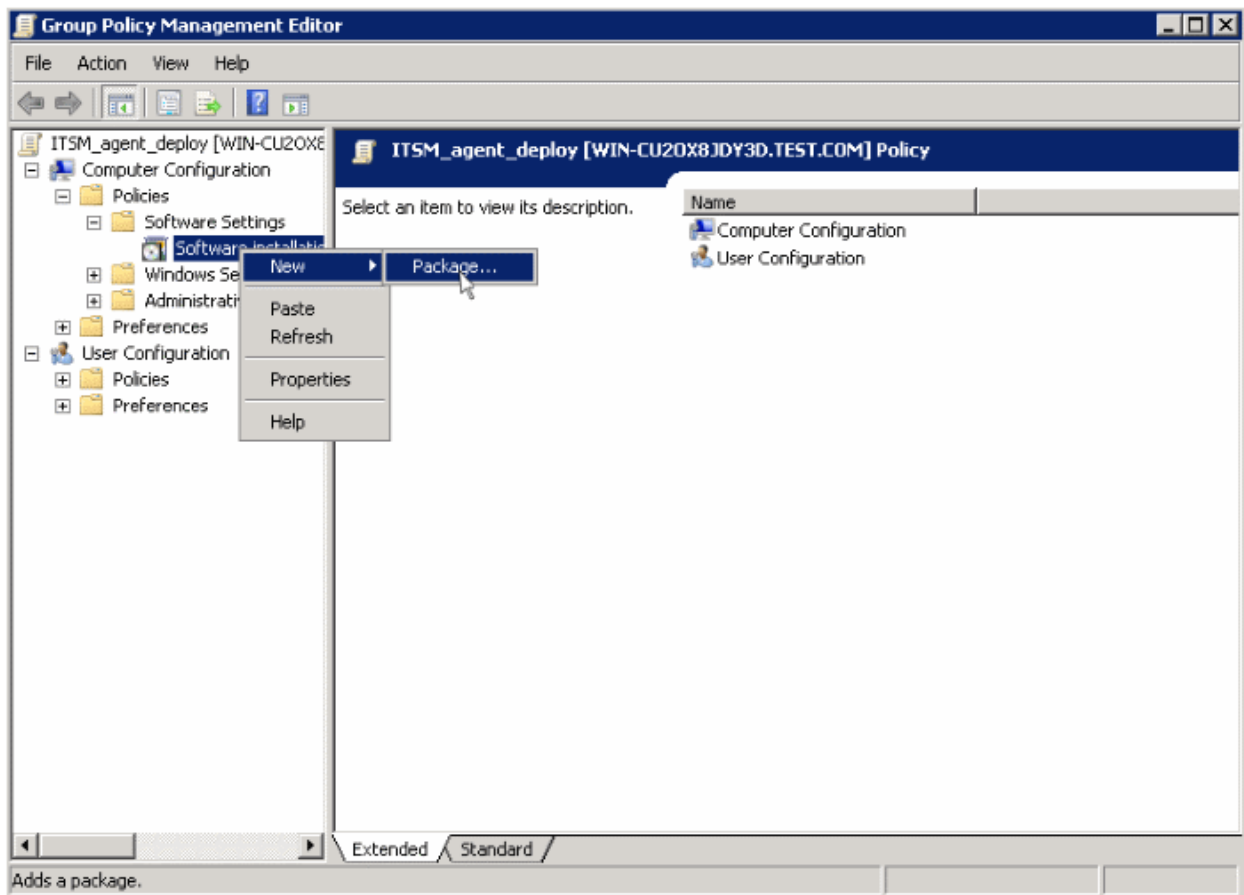
Step 6 – Adding MST file to the GPO

If you want to include the MST file to the GPO, then download the file after providing the details in the proxy settings fields in the form.

- After downloading the file, save it on the AD server and create a shared folder as explained in Step 3.
- If you are adding both MSI and MST files at one go, then select 'Advanced' at the end of Step 4.
- If you are adding the file later on, then open Group Policy Management, right click on the policy, then click 'Edit'

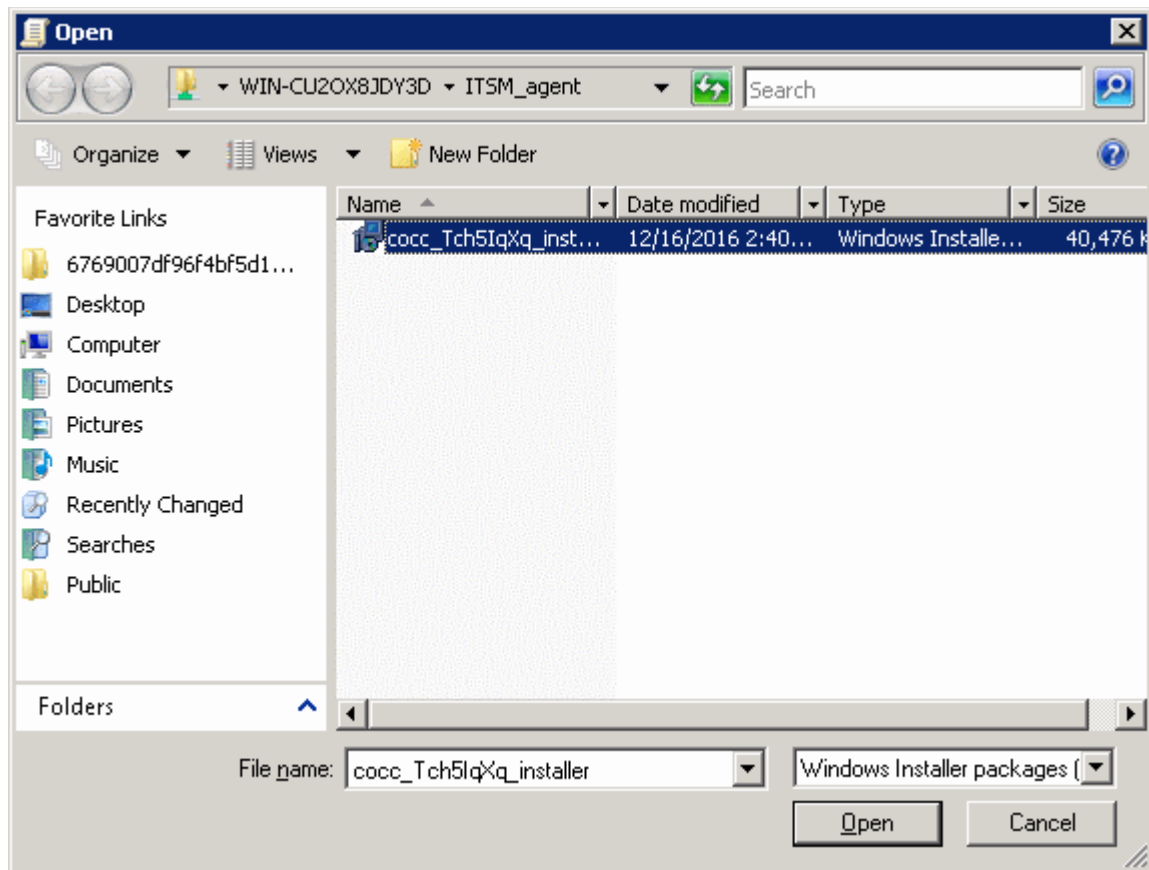


The Group Policy Management Editor will open.



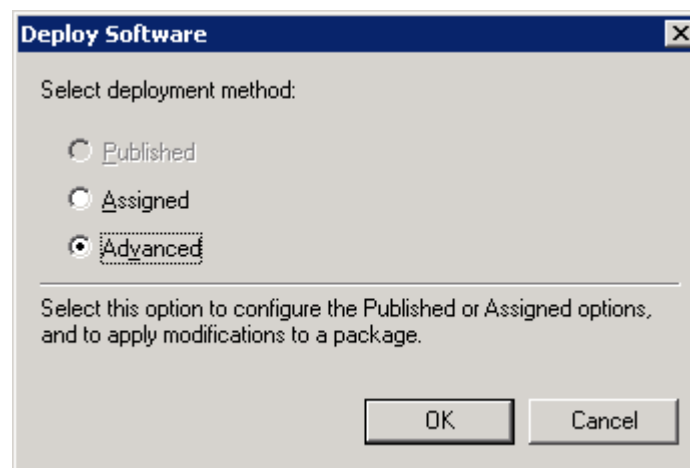
- Expand 'Computer Configuration' and right-click on 'Software Installation'
- Click 'New', then 'Package'

The policy item dialog will open.

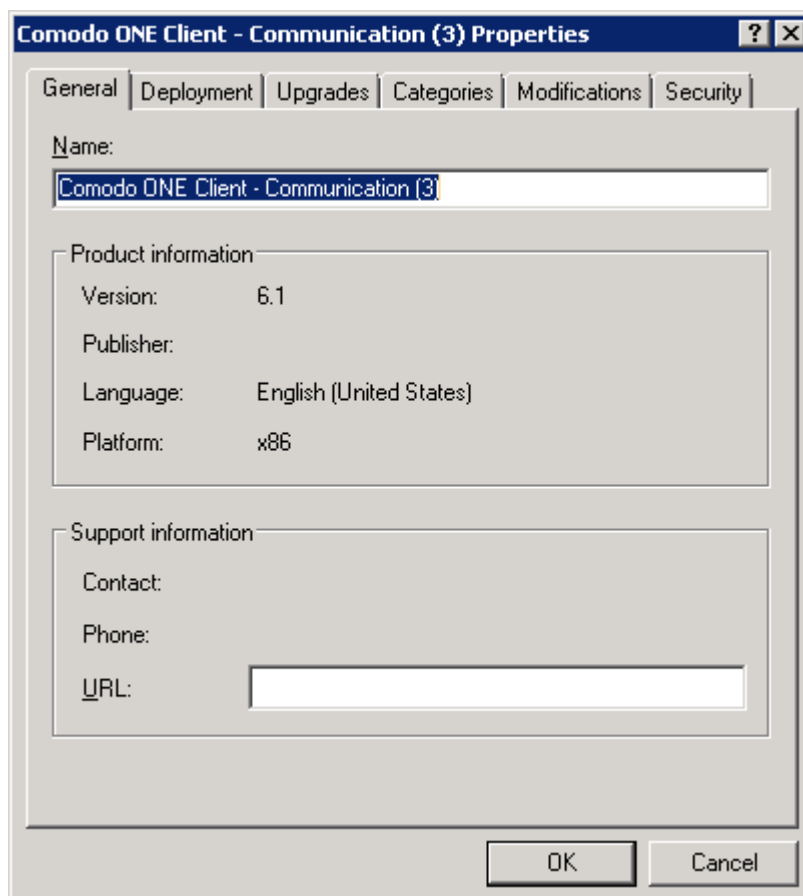


- Click 'Open'

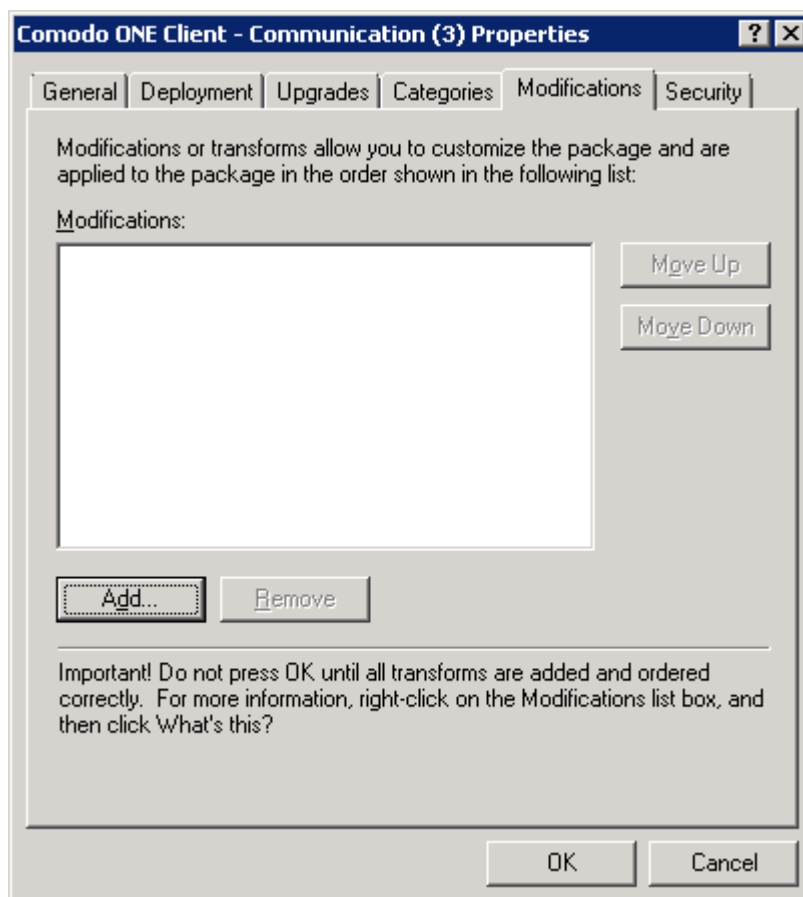
The 'Deploy Software' dialog will open.



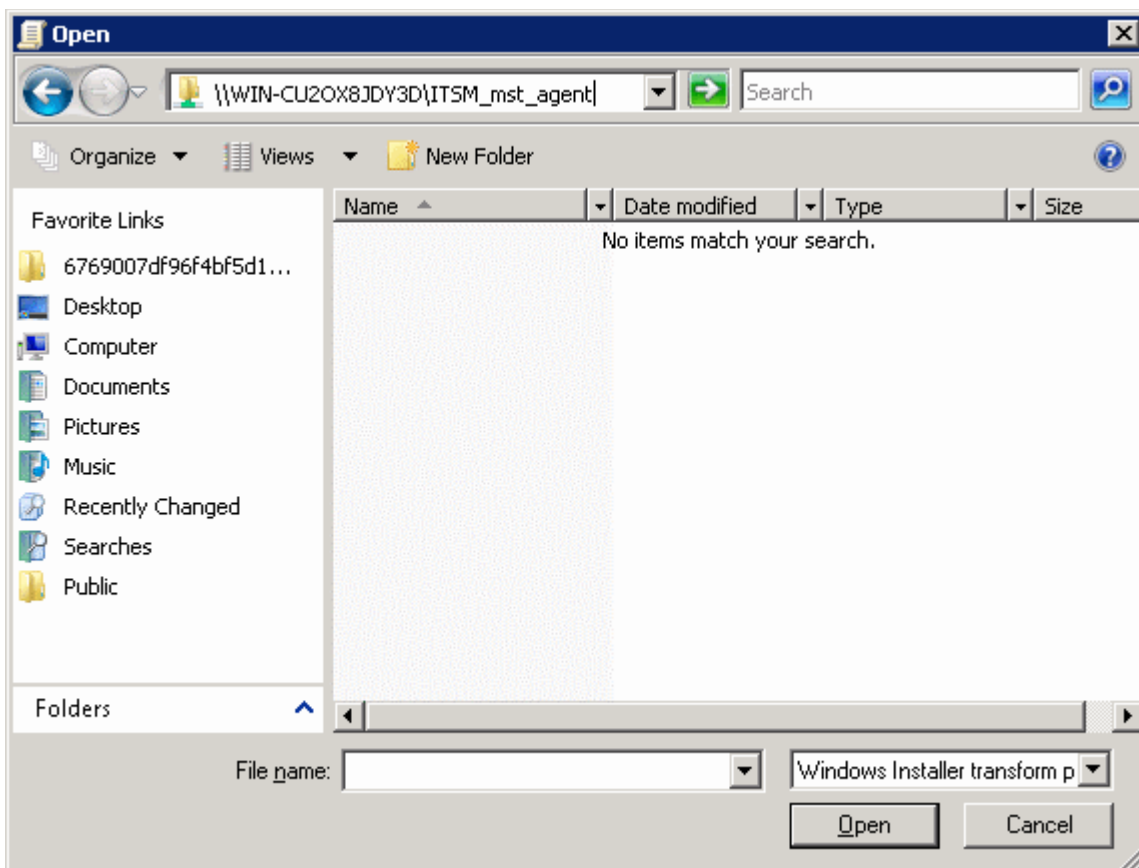
- Select 'Advanced' and click 'OK'. If you select any other option, then you won't be able to add the MST file.



- Click 'Modifications' tab

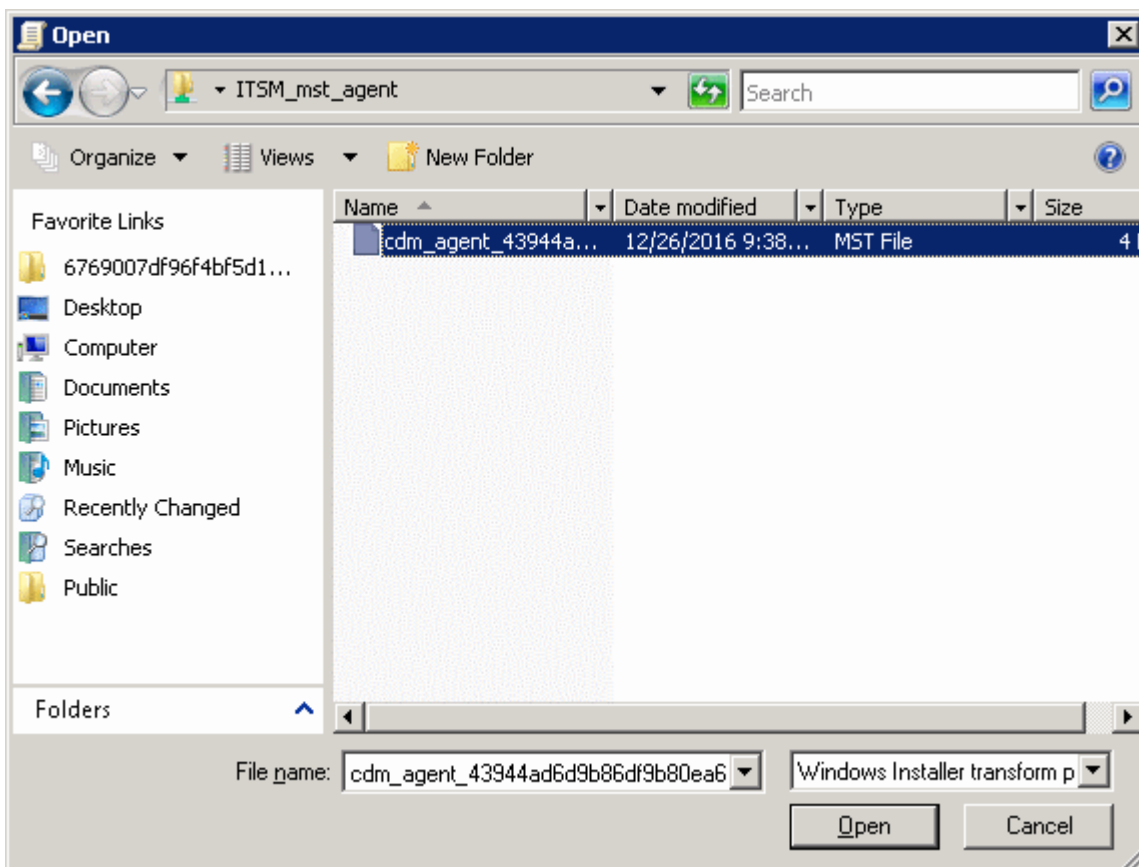


- Click 'Add' and enter the location of the shared MST file in the open dialog.



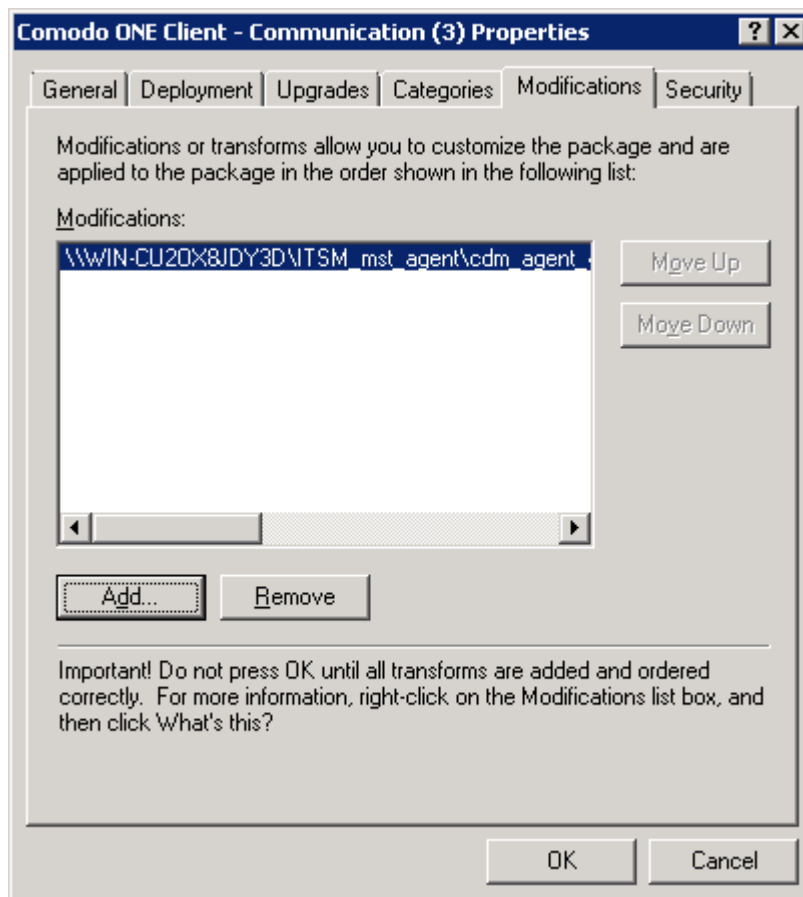
- Click 'Open'

The file name will be displayed in the dialog.



- Click 'Open' again.

The MST file will be added to GPO.



- Click 'OK' to complete the setup.
- Open the command prompt, type gpupdate and press enter to update the GPO.

That's it, you have successfully added MST file to the GPO.

After first successful connection, the device group profile(s) will be applied and the client proxy settings will take over. Make sure the profile(s) (via device, device group, user and/or user group profiles) applied to the enrolled devices contain the same proxy settings in the client proxy settings component.

About Comodo

The Comodo organization is a global innovator of cybersecurity solutions, protecting critical information across the digital landscape. Building on its unique position as the world's largest certificate authority, Comodo authenticates, validates and secures networks and infrastructures from individuals to mid-sized companies to the world's largest enterprises. Comodo provides complete end-to-end security solutions across the boundary, internal network and endpoint with innovative technologies solving the most advanced malware threats, both known and unknown. With global headquarters in Clifton, New Jersey, and branch offices in Silicon Valley, Comodo has international offices in China, India, the Philippines, Romania, Turkey, Ukraine and the United Kingdom. For more information, visit comodo.com.

Comodo Security Solutions, Inc.

1255 Broad Street

Clifton, NJ, 07013

United States

Email: EnterpriseSolutions@Comodo.com

Comodo CA Limited

3rd Floor, 26 Office Village, Exchange Quay, Trafford Road, Salford, Greater Manchester M5 3EQ,

United Kingdom.

Tel : +44 (0) 161 874 7070

Fax : +44 (0) 161 877 1767

For additional information on Comodo - visit <http://www.comodo.com>.