COMODO
Creating Trust Online®

Comodo
Endpoint Manager

Software Version 6.26

Bulk Enrollment via Active Directory

Guide Version 6.26.021819

Comodo Security Solutions
1255 Broad Street
Clifton, NJ 07013

Endpoint Manager - Bulk Enrollment via Active Directory

This tutorial briefly explains how you can install the EM communication client 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

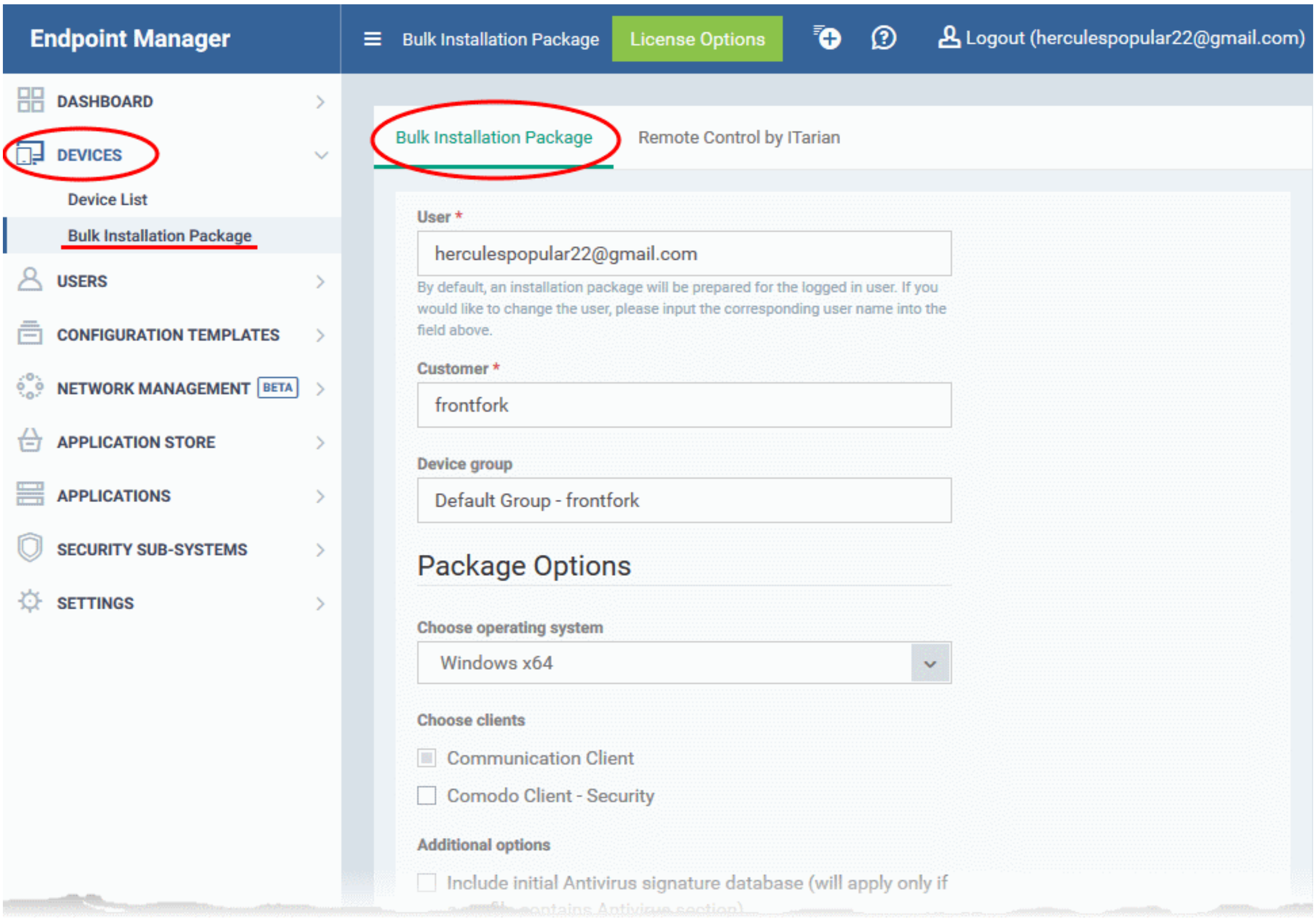
Please note the method described below for creating a group policy (GPO) and deploying them is for Windows Server 2008 Standard. The steps may vary slightly for other Window server versions.

Step 1 - Configure the offline EM package

The Endpoint Manager communication client package is unique for each company and user. All endpoints that have a client 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

- Login to Endpoint Manager
- Click 'Devices' > 'Bulk Installation Package'
- Select the 'Bulk Installation Package' tab



User *

herculespopular22@gmail.com

By default, an installation package will be prepared for the logged in user. If you would like to change the user, please input the corresponding user name into the field above.

Customer *

frontfork

Device group

Default Group - frontfork

Package Options

Choose operating system

Windows x64

Choose clients

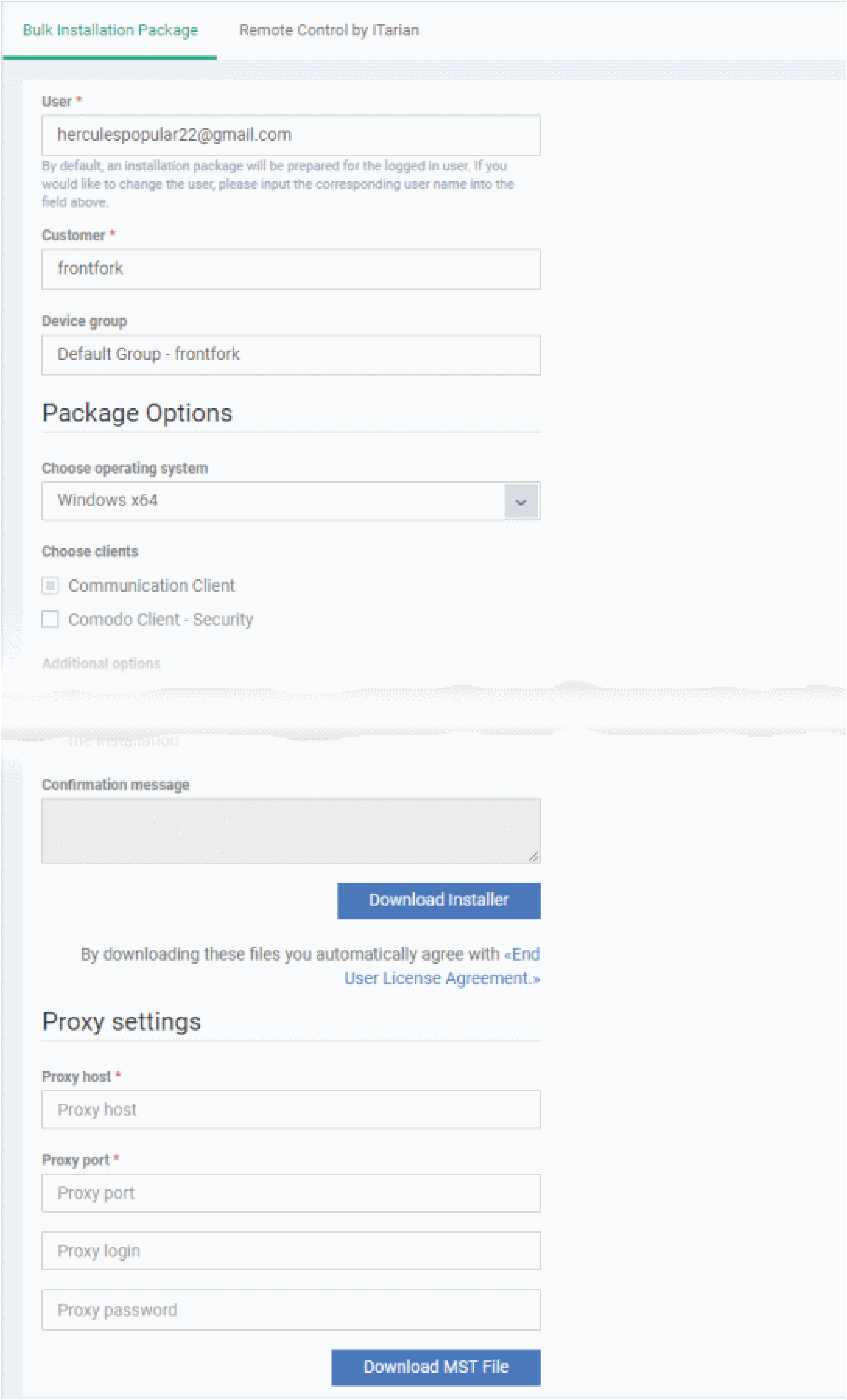
☑ Communication Client

□ Comodo Client - Security

Additional options

□ Include initial Antivirus signature database (will apply only if profile contains Antivirus section)

The interface for configuring and downloading the bulk installation package opens on the right.



Bulk Installation Package | Remote Control by ITarian

User *

herculespopular22@gmail.com

By default, an installation package will be prepared for the logged in user. If you would like to change the user, please input the corresponding user name into the field above.

Customer *

frontfork

Device group

Default Group - frontfork

Package Options

Choose operating system

Windows x64

Choose clients

▣ Communication Client

□ Comodo Client - Security

Additional options

Confirmation message

By downloading these files you automatically agree with «End User License Agreement.»

Proxy settings

Proxy host *

Proxy host

Proxy port *

Proxy port

Proxy login

Proxy password

Bulk Installation Package - Form Parameters	
Parameter	**Description**
User	Devices that are enrolled by installing the communication client through 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. • Start typing the name of a user and choose from the suggestions that appear.
Customer	Choose the company to which the endpoints should be assigned. • This field only applies to C1 MSP and ITarian MSP customers. It does not apply to C1 Enterprise, ITarian Enterprise or EM stand-alone customers.
Device Group	The device group to which the enrolled devices should be added (optional). Any group profiles will also be applied to the devices you add.
Package Options	**Operating system** - Choose the OS of the target endpoints. **Clients**: • **Communication Client (CC)** - Mandatory. This client enrolls the endpoint. • **Comodo Client Security (CCS)** - Optional. This client installs security software such as antivirus, firewall and auto-containment. To create an installation package in MSI/MST file format for bulk enrollment through AD Group Policy, leave only the 'Communication Client' selected and 'Comodo Client Security' unselected. You can remotely install CCS at a later time on required endpoints from the EM. The rest of the configuration options related to CCS will not be enabled, if 'Security' is not selected under 'Choose clients'.
Restart Control Options	CCS only. Endpoints need to be restarted to complete CCS installation. You have the following restart options: • **Force the reboot in**... - Restart the endpoint a certain length of time after installation. Select the delay period from the drop-down. A warning message will be shown to the user prior to the restart. • **Suppress reboot** - Endpoint is not auto-restarted. The installation will be finalized when the user next restarts the endpoint. • **Warn about reboot and let users postpone it** - Shows a message to the user which tells them that the endpoint needs to be restarted. The user can choose when the restart happens. Optional. Type a custom message in the 'Reboot Message' field.
UI Options	Configure which messages are shown to the user regarding the installation. • **Show error messages if installation failed** - Notifies the user if the installation is not successful. • **Show a confirmation message upon completion of installation** - Notifies the user if the installation is successful. Type your message in the box provided.
Proxy Settings	Proxy settings allows you to specify a proxy server through which Comodo Client Security (CCS) and the communication client (CC) on the endpoints should connect to EM management portal and Comodo servers. If you choose not to set these, then CCS and CC will connect directly as per the network settings. • 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 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.

- If you do not wish to use a proxy server for CCS and CC 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 it has been configured as explained in the steps given below.

Step 2 - Download the EM client package

The next step is to download the EM communication client package for Windows devices.

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

The client package is 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 client is installed, it establishes communications with EM to begin importing the device.

- To download the installation file to include a proxy server for CC and CCS communication to EM and Comodo servers, click 'Download MST File'

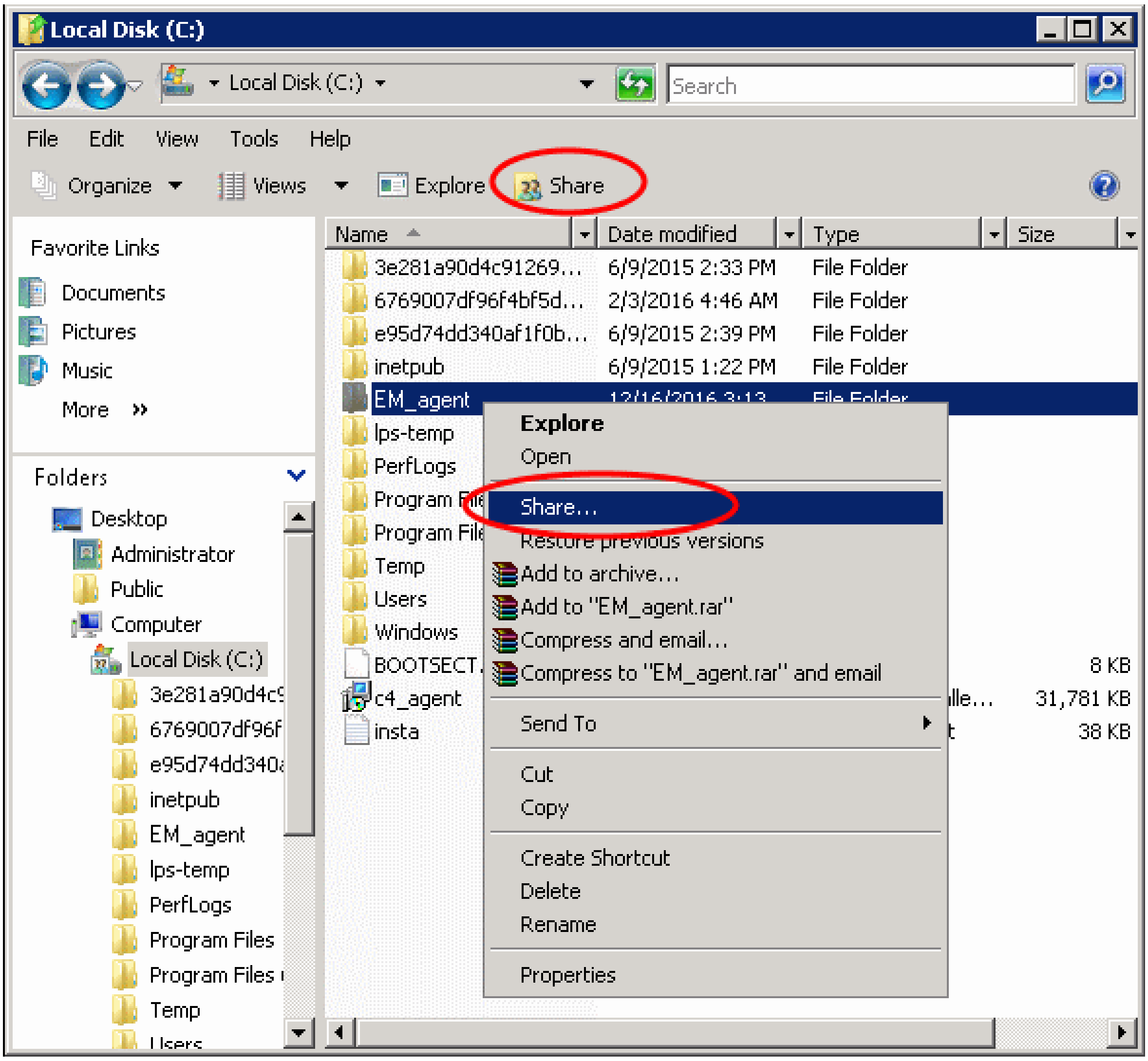
EM will create a .mst transform file containing the proxy server installation commands. As above, you can save the file on the AD server from where you want to enroll the endpoints, and add to the GPO created for .msi file. After the client is installed, it establishes communications with EM via the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

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

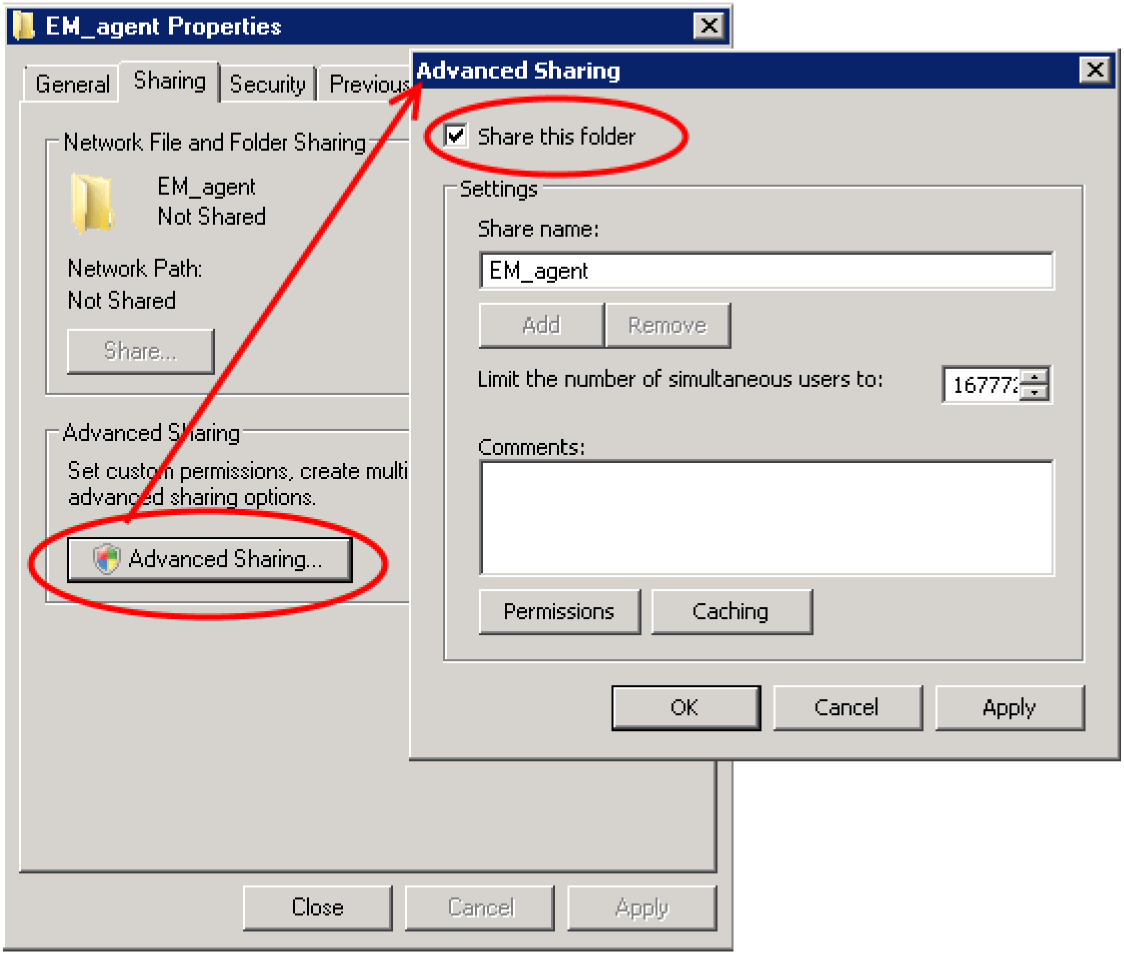
Step 3 - Create a shared network folder and configure permission level

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

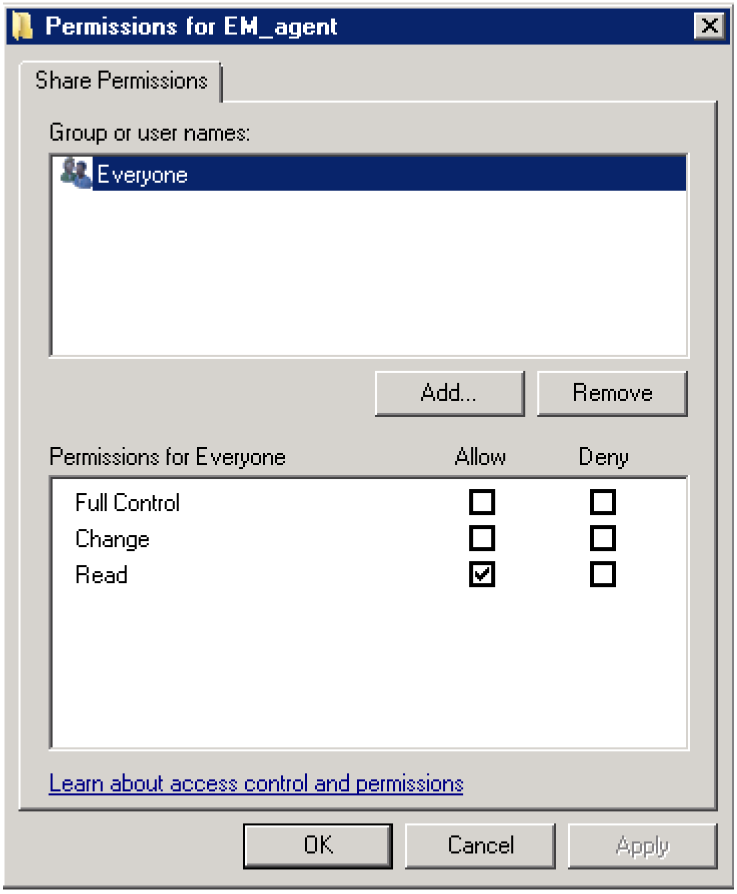
- Create a new folder in your desired location
- Name the folder appropriately. For example 'EM_agent'
- Select the folder, right-click and select 'Share' or from the menu toolbar



- 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'



Permissions for EM_agent

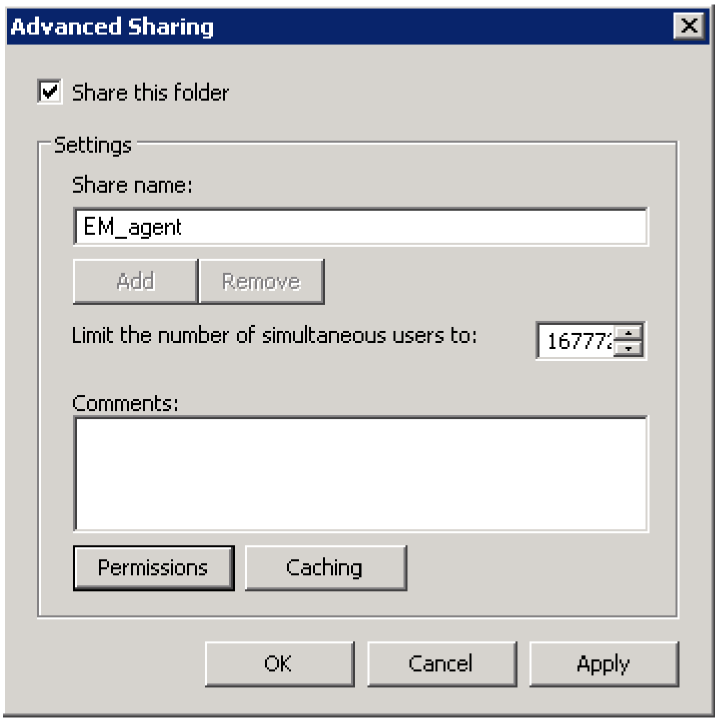
Share Permissions

Group or user names:

Everyone

Permissions for Everyone	Allow	Deny
Full Control	□	□
Change	□	□
Read	☑	□

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



Advanced Sharing

☑ Share this folder

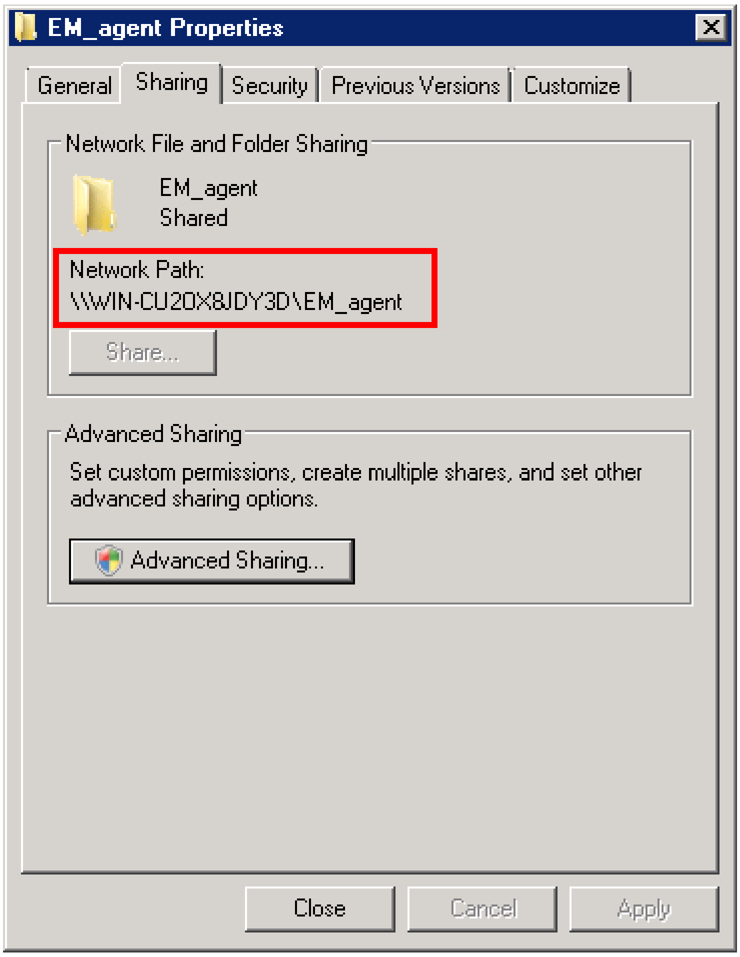
Settings

Share name: EM_agent

Limit the number of simultaneous users to: 16777

Comments:

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



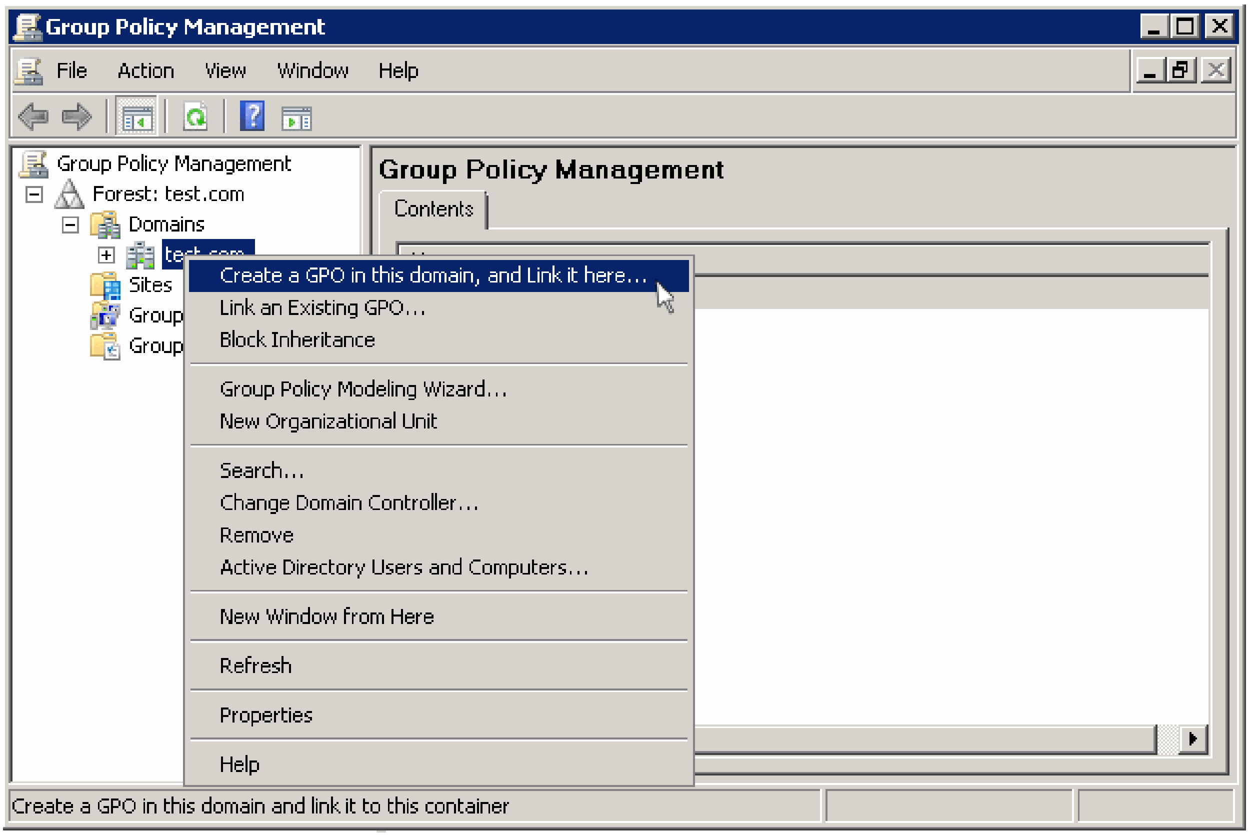
- Note down the location of this shared folder and click the 'Close' button

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

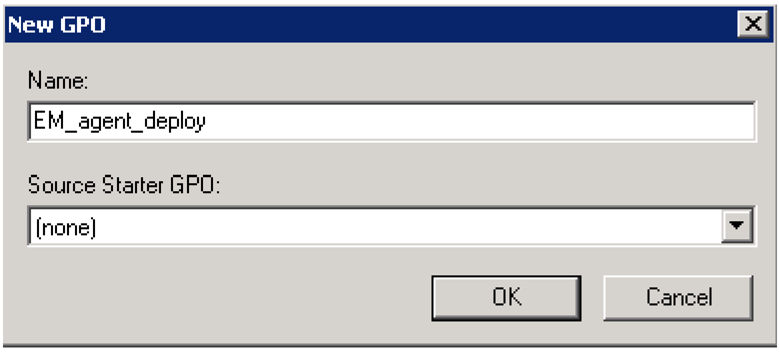
The next step is to create a group policy that will install the client package onto the endpoints.

- 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



Create a GPO in this domain and link it to this container

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



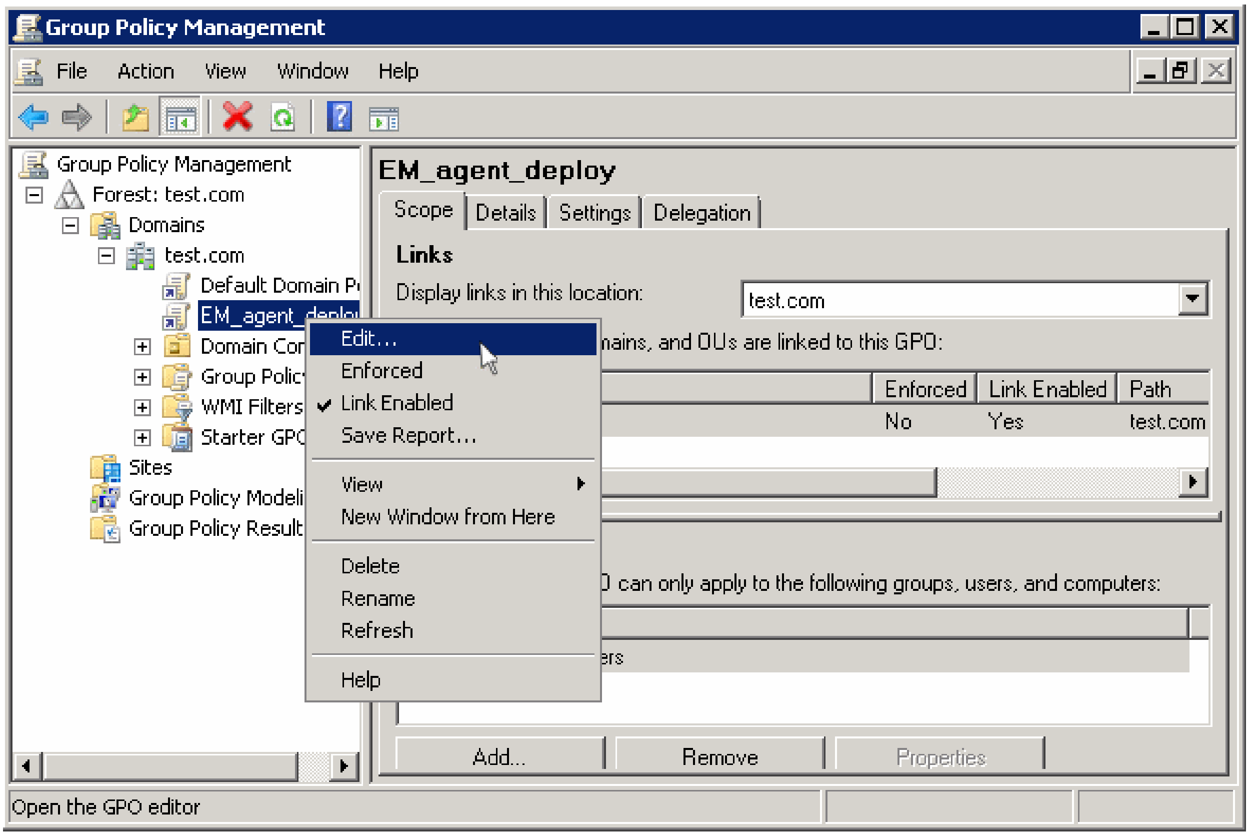
Name: EM_agent_deploy

Source Starter GPO: (none)

- Click 'OK'

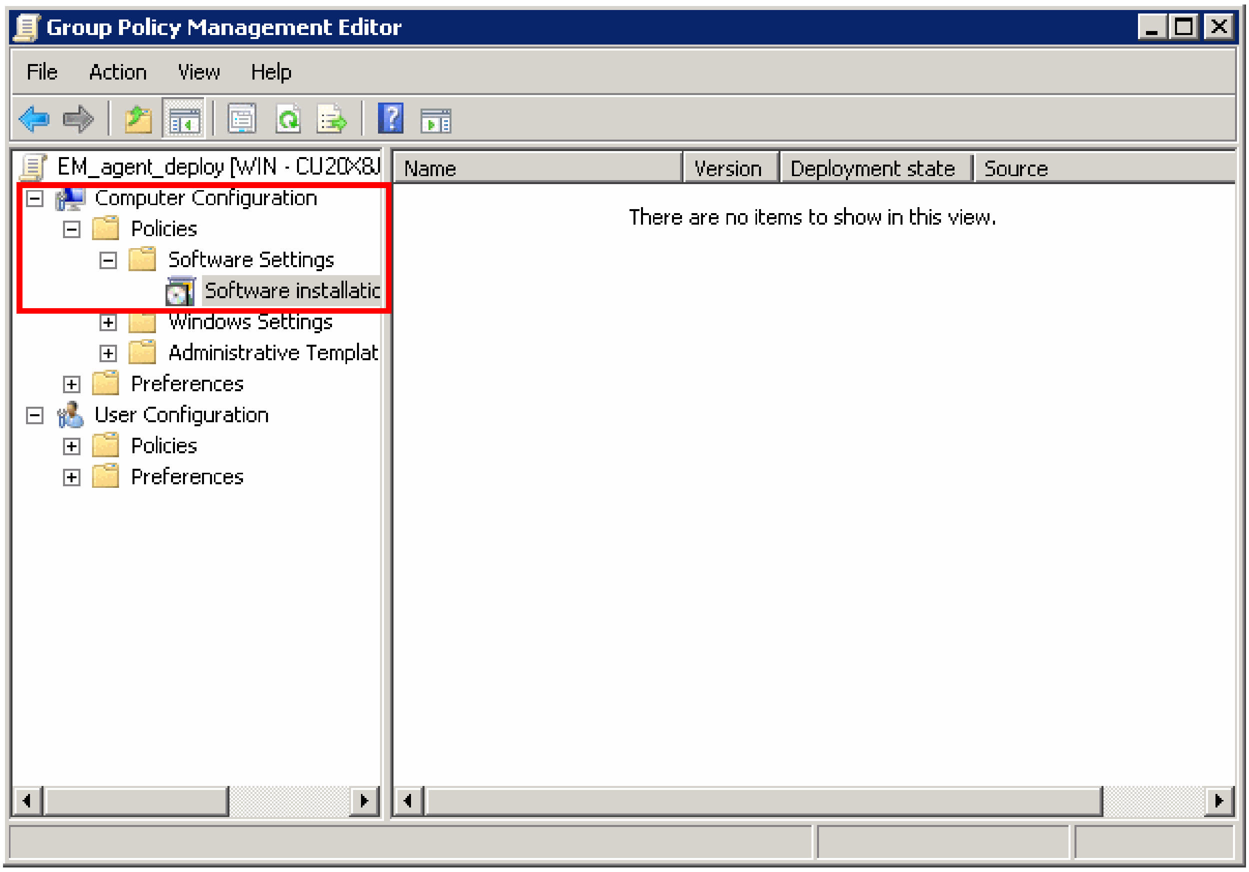
The newly added group policy will be listed.

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

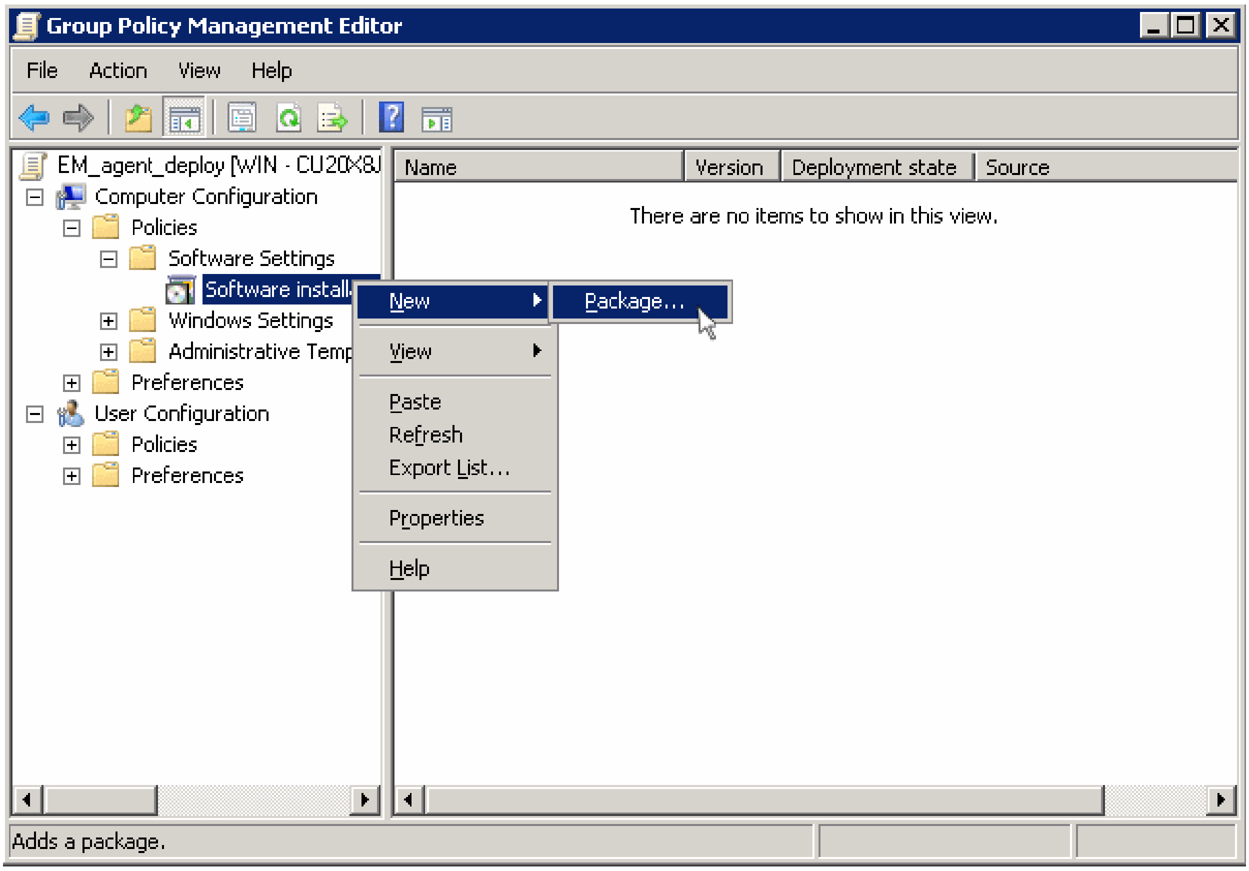


The 'Group Policy Management Editor' will be displayed.

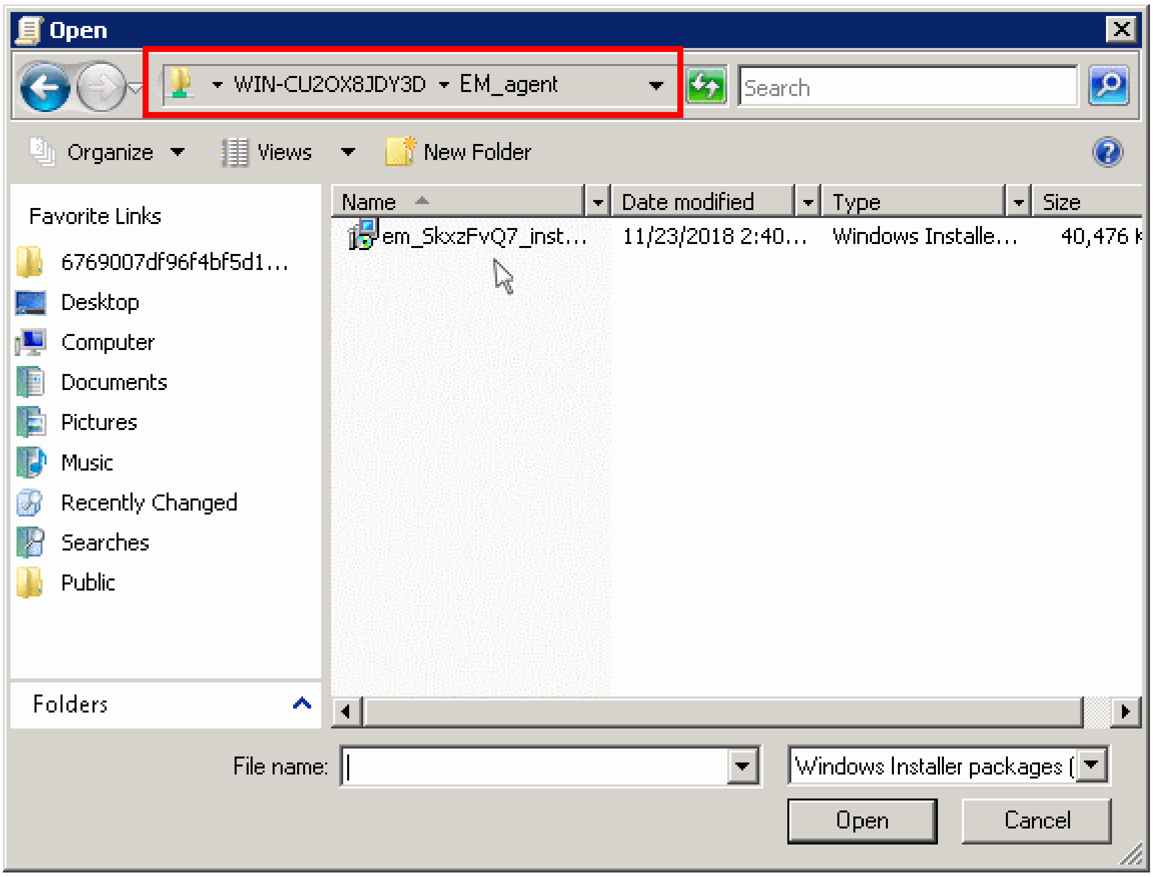
- Expand 'Computer Configuration' > 'Policies' > 'Software Settings'



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



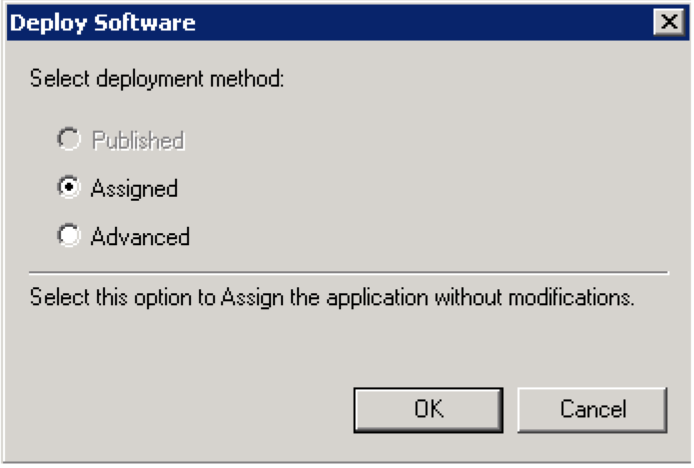
- In the 'Open' dialog, enter the path of the shared folder that was noted before, select the file and click the 'Open' button



- 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.

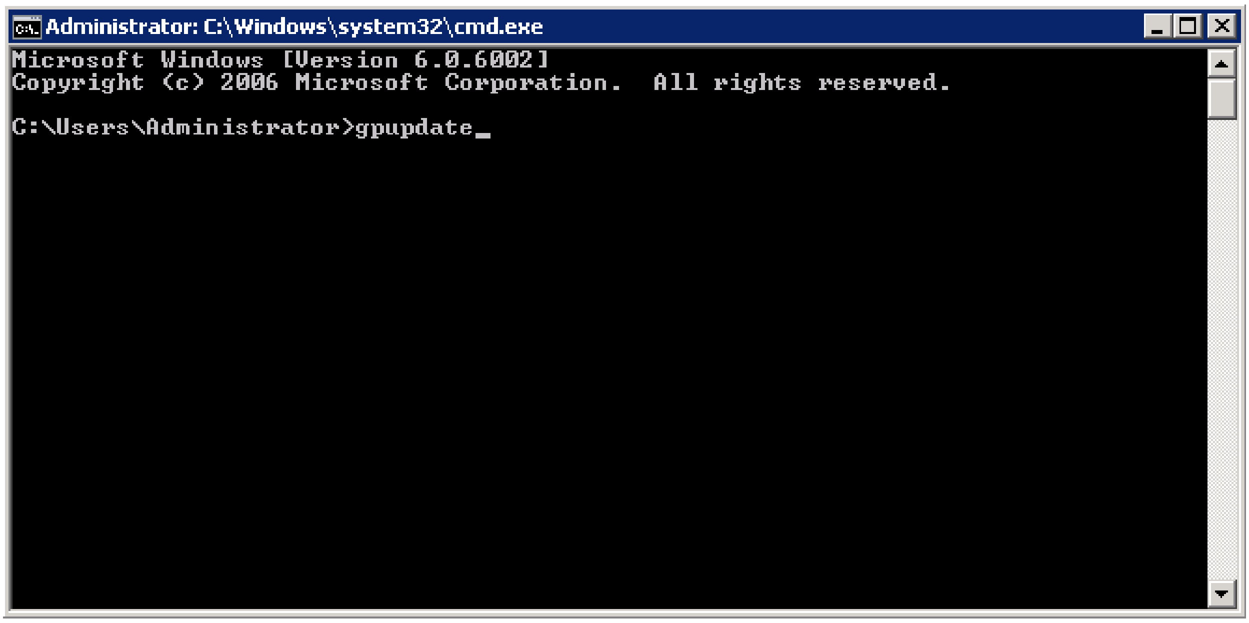

Deploy Software
Select deployment method:
○ Published
● Assigned
○ Advanced
Select this option to Assign the application without modifications.
OK
Cancel

- Click 'OK'

Step 5 - Run a GPO update

In order to install the EM client package, you need to run a GPO update in the command prompt.

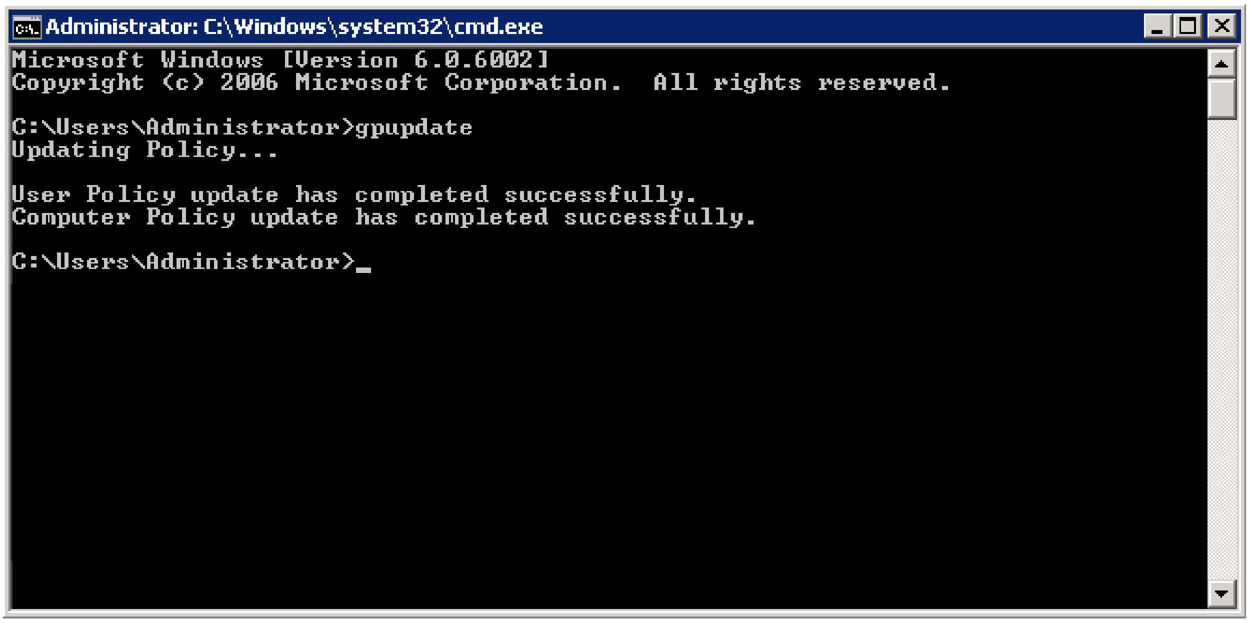
- Open the command prompt, type "gpupdate" and press enter.



```
Microsoft Windows [Version 6.0.6002]
Copyright (c) 2006 Microsoft Corporation.  All rights reserved.

C:\Users\Administrator>gpupdate_
```

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



```
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 EM communication client 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 EM communication client 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.

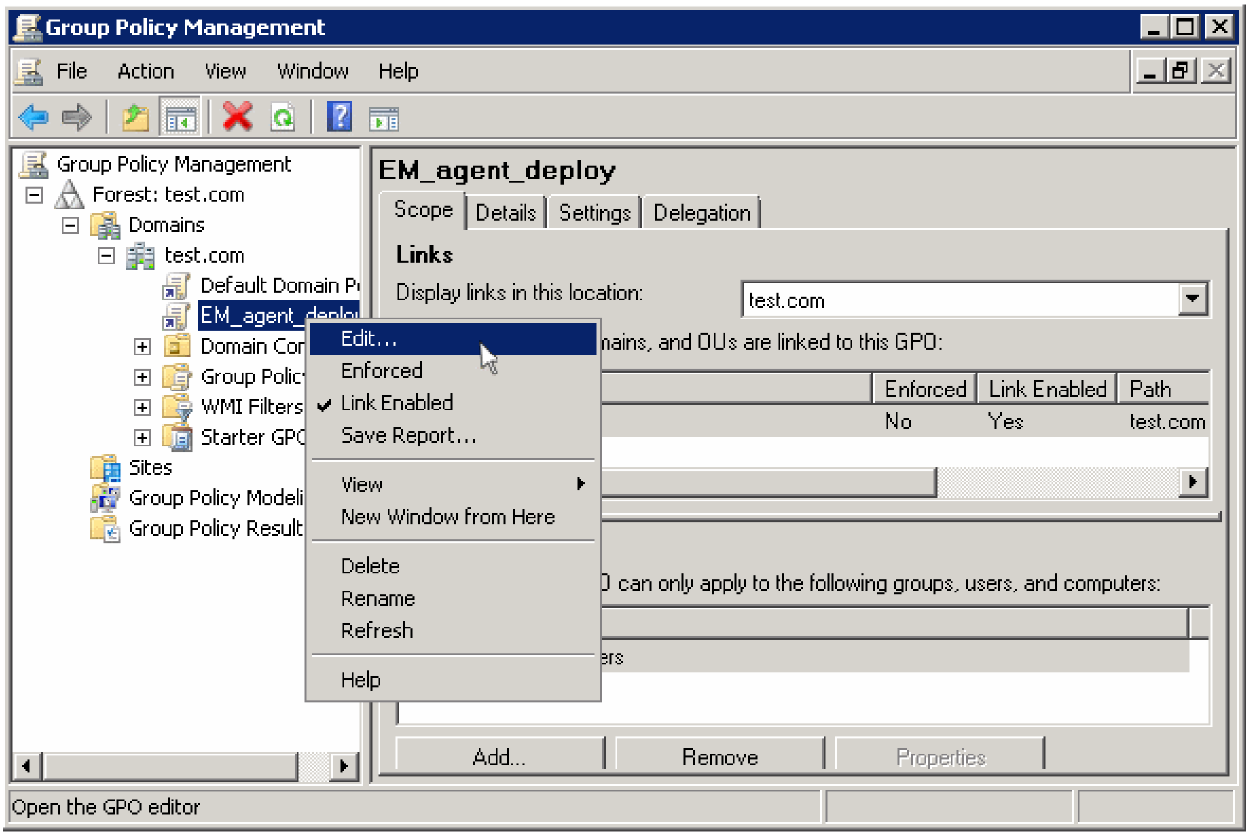
The device group policy that was selected in the enrollment form will be applied to the enrolled devices automatically.

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.

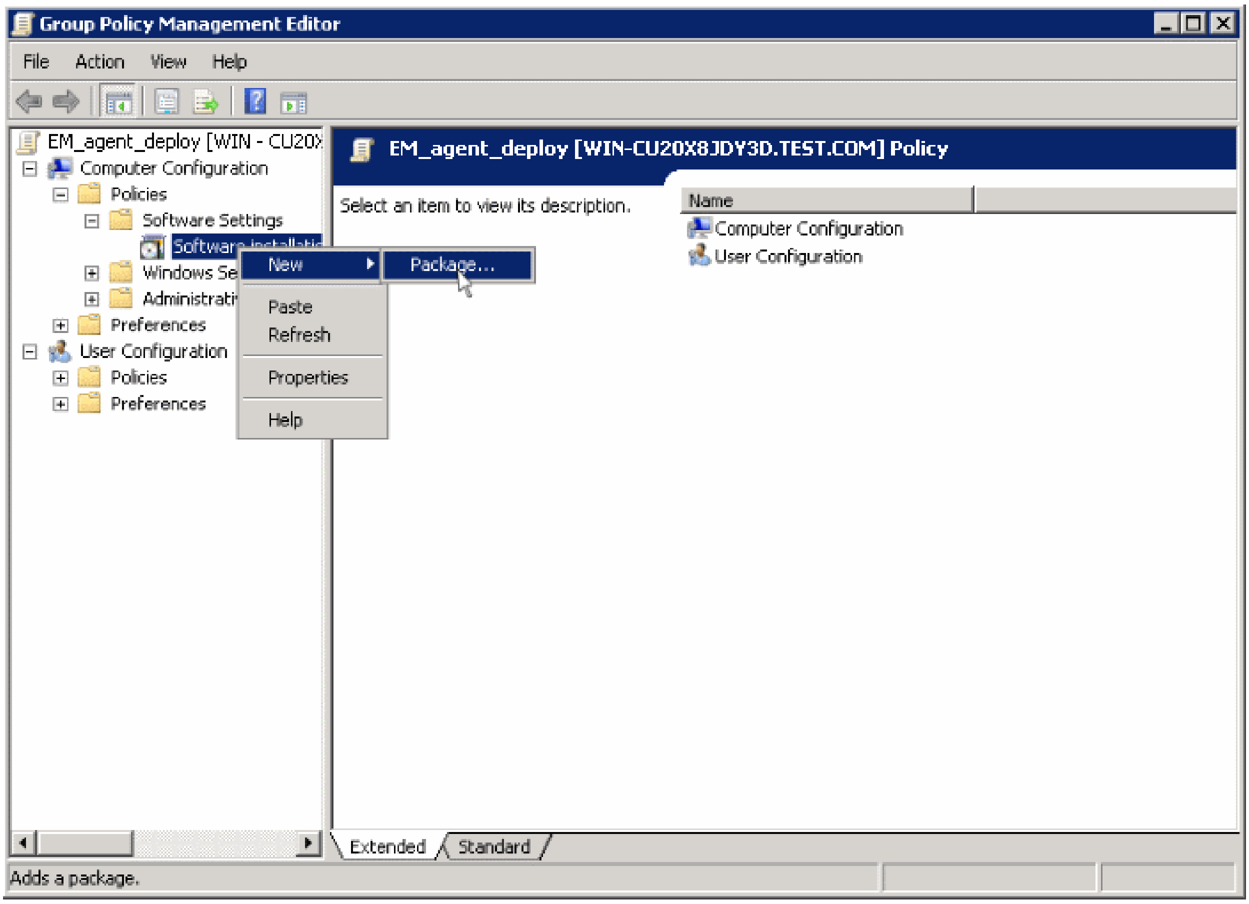
Step 6 - Add MST file to the GPO

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'

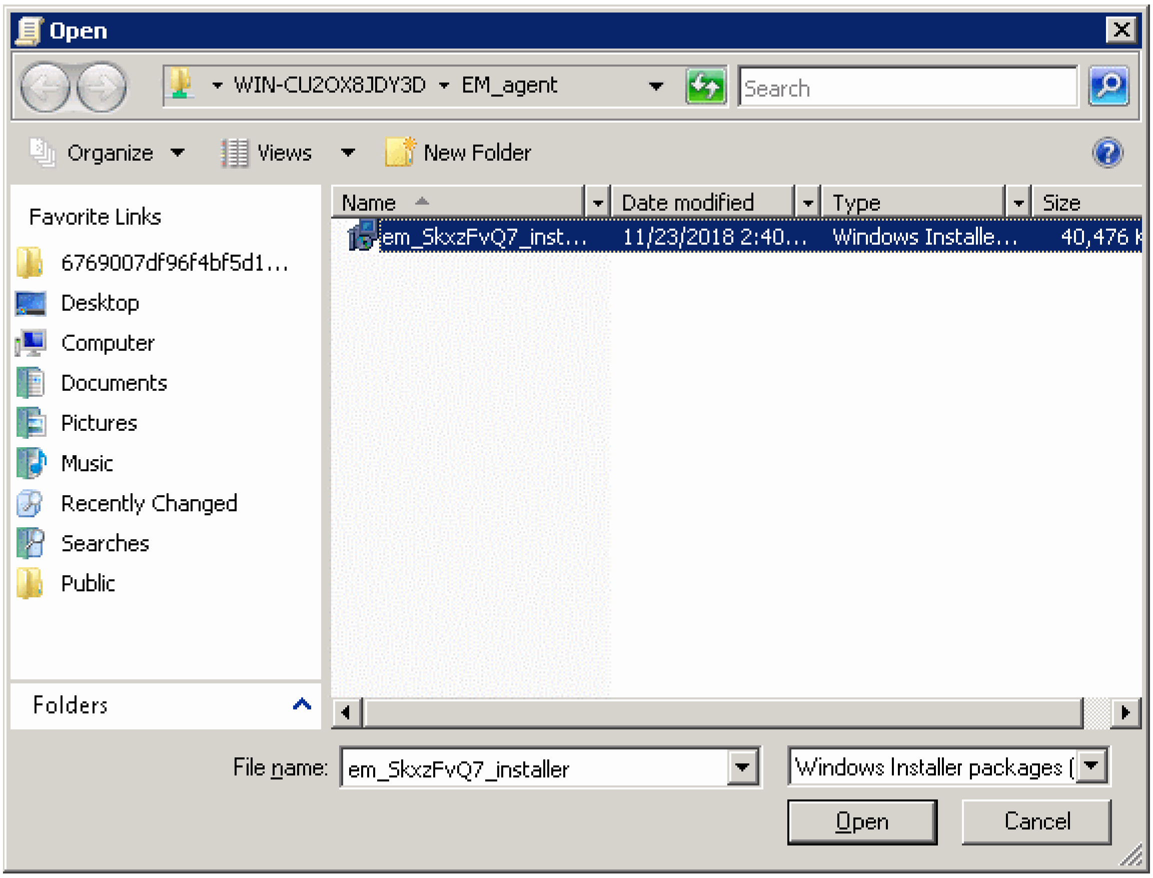


The 'Group Policy Management Editor' will open.



- Expand 'Computer Configuration' and right-click on 'Software Installation'

- Click 'New', then 'Package'



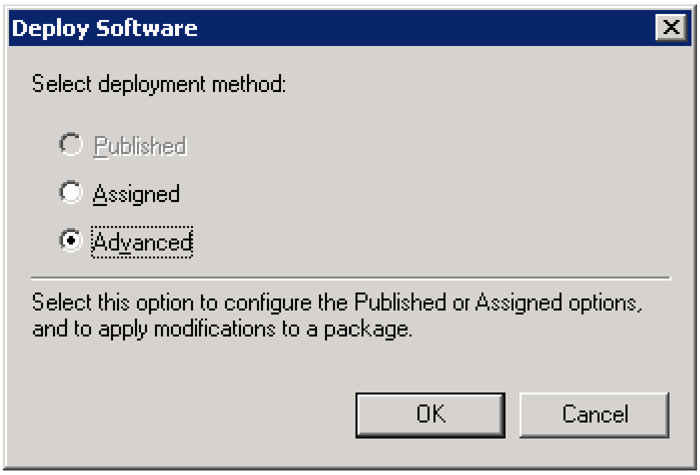
Name	Date modified	Type	Size
em_SkxzFvQ7_inst...	11/23/2018 2:40...	Windows Installe...	40,476 k

File name: em_SkxzFvQ7_installer

Windows Installer packages (

- Click 'Open'

The 'Deploy Software' dialog will open.



Deploy Software

Select deployment method:

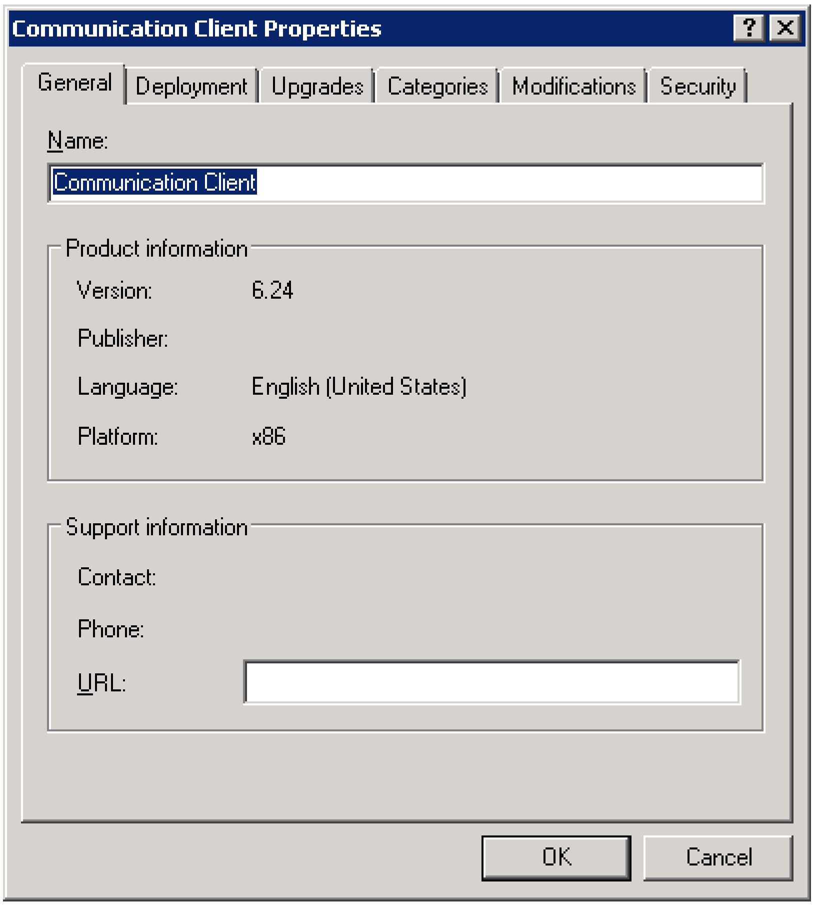
○ Published

○ Assigned

● Advanced

Select this option to configure the Published or Assigned options, and to apply modifications to a package.

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



Communication Client Properties

Name: Communication Client

Product information

Version: 6.24

Publisher:

Language: English (United States)

Platform: x86

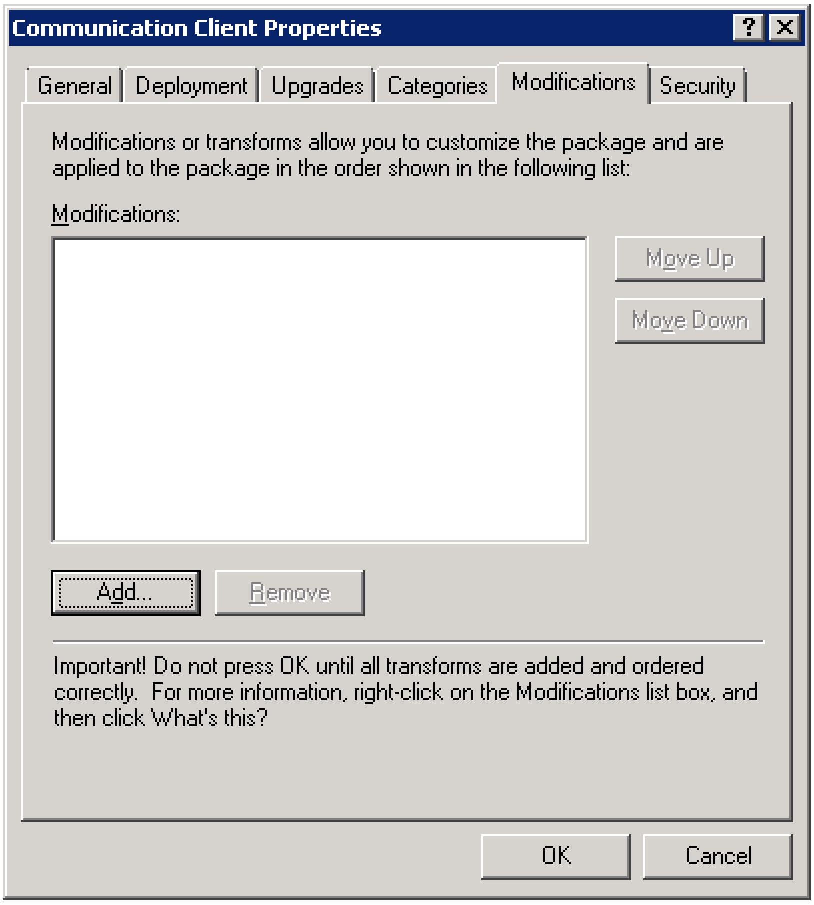
Support information

Contact:

Phone:

URL:

- Click 'Modifications' tab



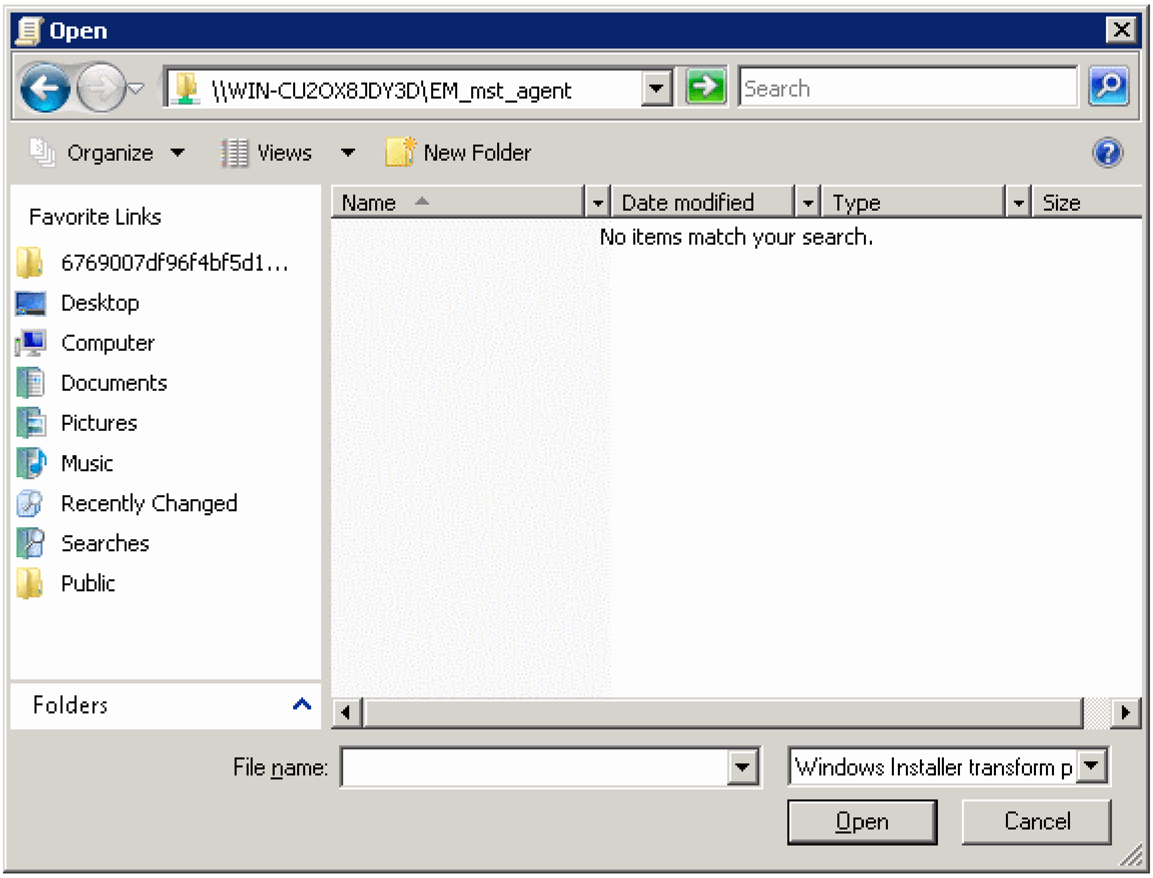
Communication Client Properties

Modifications or transforms allow you to customize the package and are applied to the package in the order shown in the following list:

Modifications:

Important! Do not press OK until all transforms are added and ordered correctly. For more information, right-click on the Modifications list box, and then click What's this?

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



\\WIN-CU2OX8JDY3D\EM_mst_agent

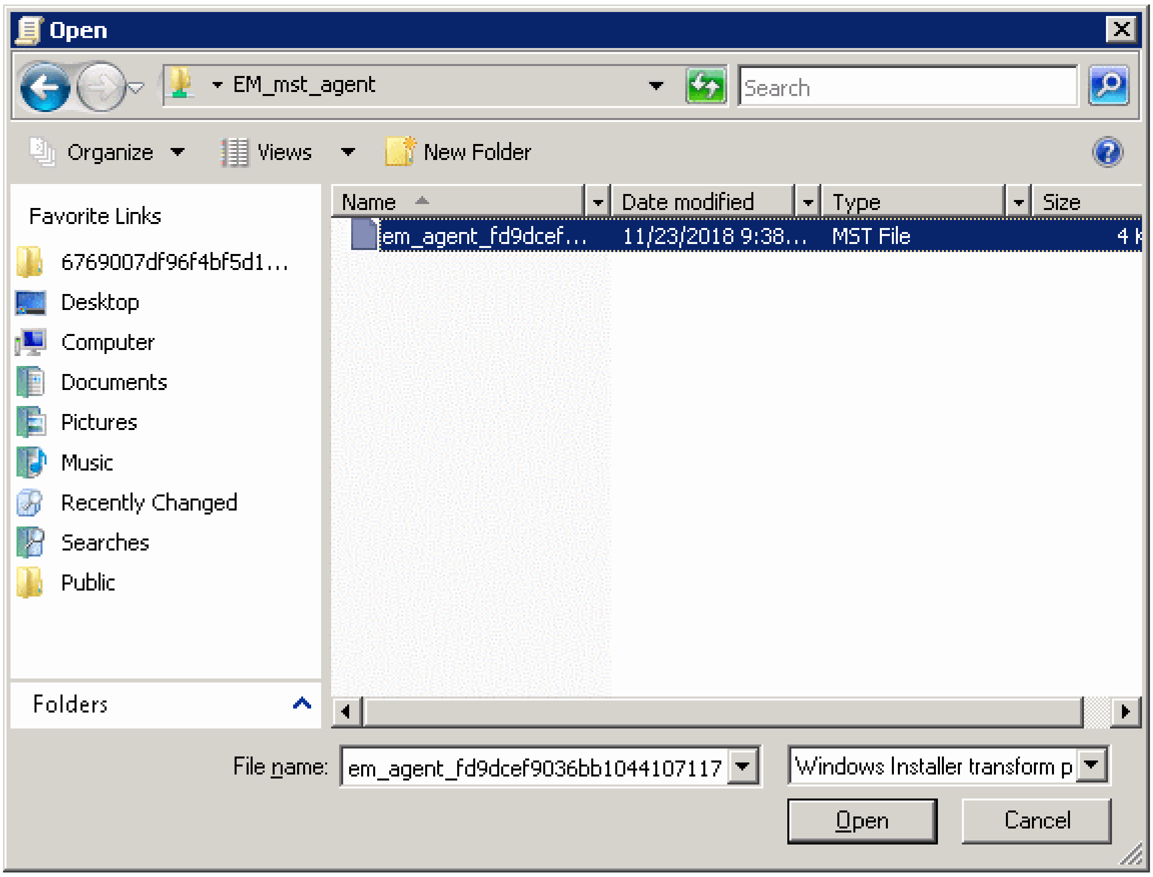
No items match your search.

File name:

Windows Installer transform p

- Click 'Open'

The file name will be displayed in the dialog.



EM_mst_agent

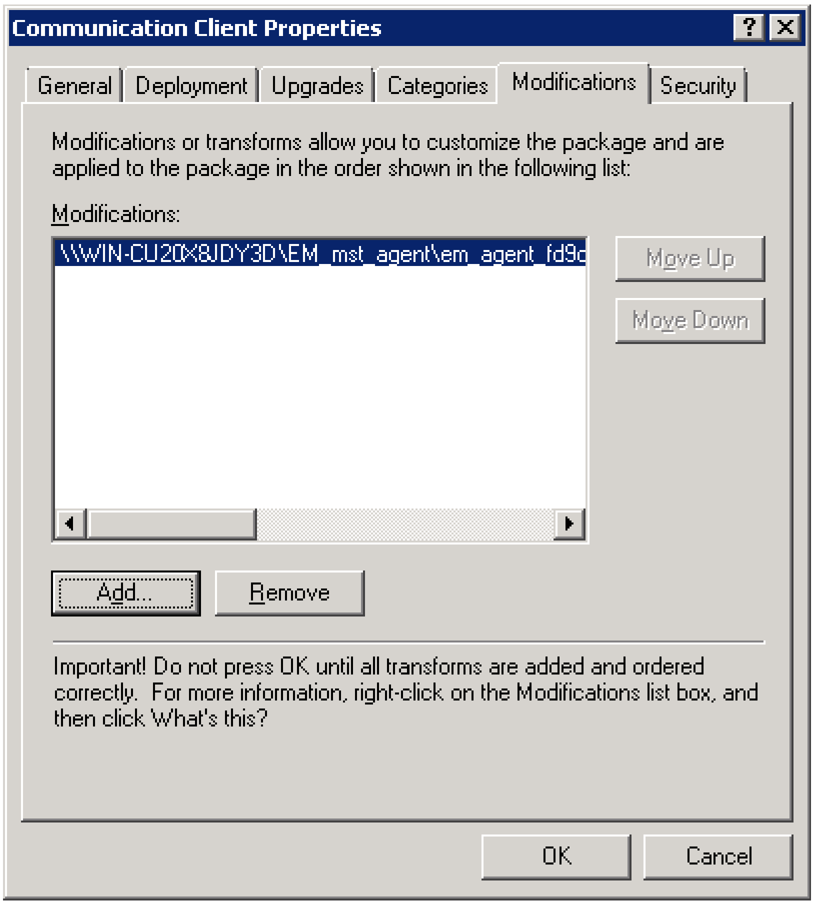
em_agent_fd9dcef... 11/23/2018 9:38... MST File 4 K

File name: em_agent_fd9dcef9036bb1044107117

Windows Installer transform p

- Click 'Open' again.

The MST file will be added to GPO.



Modifications or transforms allow you to customize the package and are applied to the package in the order shown in the following list:

Modifications:

\\WIN-CU20X8JDY3D\EM_mst_agent\em_agent_fd9c

Important! Do not press OK until all transforms are added and ordered correctly. For more information, right-click on the Modifications list box, and then click What's this?

- 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 Security Solutions

Comodo Security Solutions is a global innovator of cybersecurity solutions, protecting critical information across the digital landscape. Comodo provides complete, end-to-end security solutions across the boundary, internal network and endpoint with innovative technologies solving the most advanced malware threats. With over 80 million installations of its threat prevention products, Comodo provides an extensive suite of endpoint, website and network security products for MSPs, enterprises and consumers.

Continual innovation and a commitment to reversing the growth of zero-day malware, ransomware, data-breaches and internet-crime distinguish Comodo Security Solutions as a vital player in today's enterprise and home security markets.

About Comodo Cybersecurity

In a world where preventing all cyberattacks is impossible, Comodo Cybersecurity delivers an innovative cybersecurity platform that renders threats useless, across the LAN, web and cloud. The Comodo Cybersecurity platform enables customers to protect their systems and data against even military-grade threats, including zero-day attacks. Based in Clifton, New Jersey, Comodo Cybersecurity has a 20-year history of protecting the most sensitive data for both businesses and consumers globally. For more information, visit comodo.com or our **blog**. You can also follow us on **Twitter** (@ComodoDesktop) or **LinkedIn**.

1255 Broad Street

Clifton, NJ 07013

United States

Tel : +1.877.712.1309

Tel : +1.888.551.1531

https://www.comodo.com

Email: **EnterpriseSolutions@Comodo.com**