COMODO
Creating Trust Online®

COMODO
one

Comodo ONE

Software Version 1.9

RMM - Bulk Enrollment via Active Directory

Guide Version 1.9.113018

Comodo Security Solutions
1255 Broad Street
Clifton, NJ 07013

RMM– Bulk Enrollment via Active Directory

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

Software Requirements

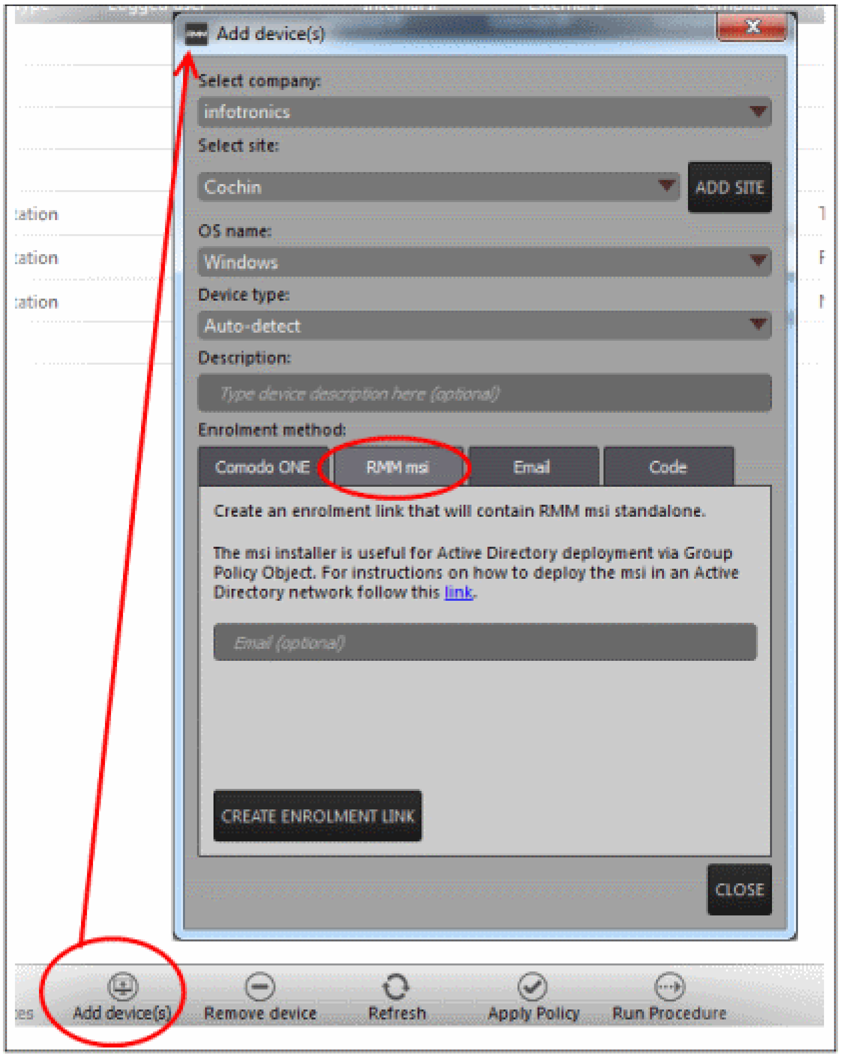
- AD Server – Windows Server 2008 or higher
- Endpoints – Windows 7 or higher

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

Step 1 – Get the enrollment code/link from the RMM admin console

The enrollment code/link for RMM agents is unique for each company site. All endpoints that have an agent installed upon them will be listed under the selected site in the RMM admin console.

To generate a enrollment code/link, click the 'Add Device(s)' button at the bottom of the RMM admin console



Add device(s)

Select company: infotronics

Select site: Cochin

OS name: Windows

Device type: Auto-detect

Description: Type device description here (optional)

Enrolment method: RMM msi

Create an enrolment link that will contain RMM msi standalone.

The msi installer is useful for Active Directory deployment via Group Policy Object. For instructions on how to deploy the msi in an Active Directory network follow this link.

Email (optional)

- **Select company:** Choose the company for which you want to bulk enroll endpoints

- **Select site:** Choose the location from the drop-down. Please note the enrollment code/link for the selected site is unique and endpoints that are installed with the downloaded agent using this enrollment code/link will be listed under the selected site in the RMM admin console.

Step 2 – Download the RMM agent

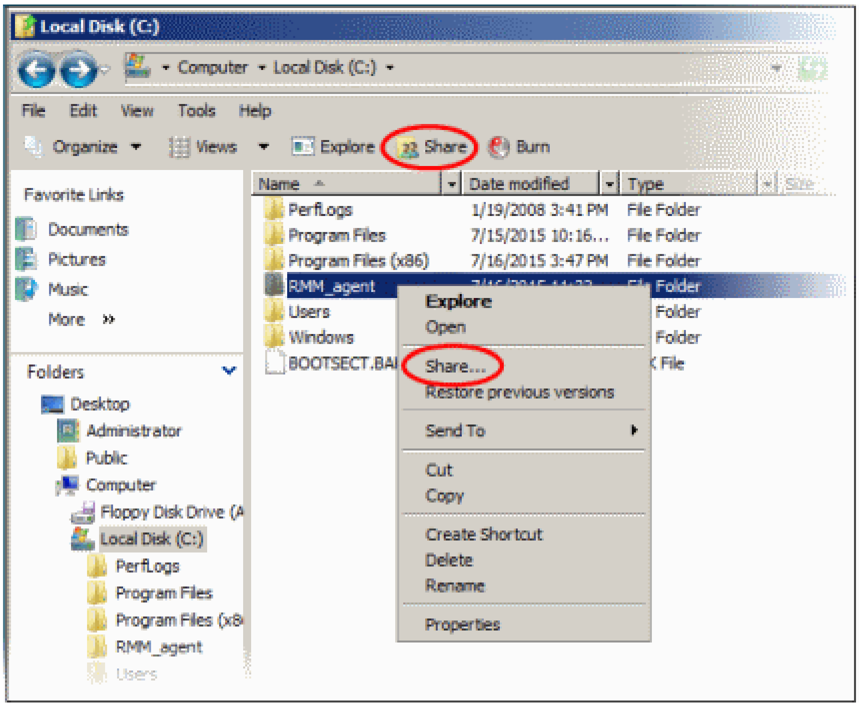
The next step is to download the agent from the 'RMM msi' tab. The standalone RMM installer is used to enroll endpoints in bulk using Active Directory via Group Policy Object method. For more details about the enrollment method and downloading the agent, refer to our page at **https://help.comodo.com/topic-289-1-719-8553-Adding-Devices-for-Managing-and-Monitoring.html**

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

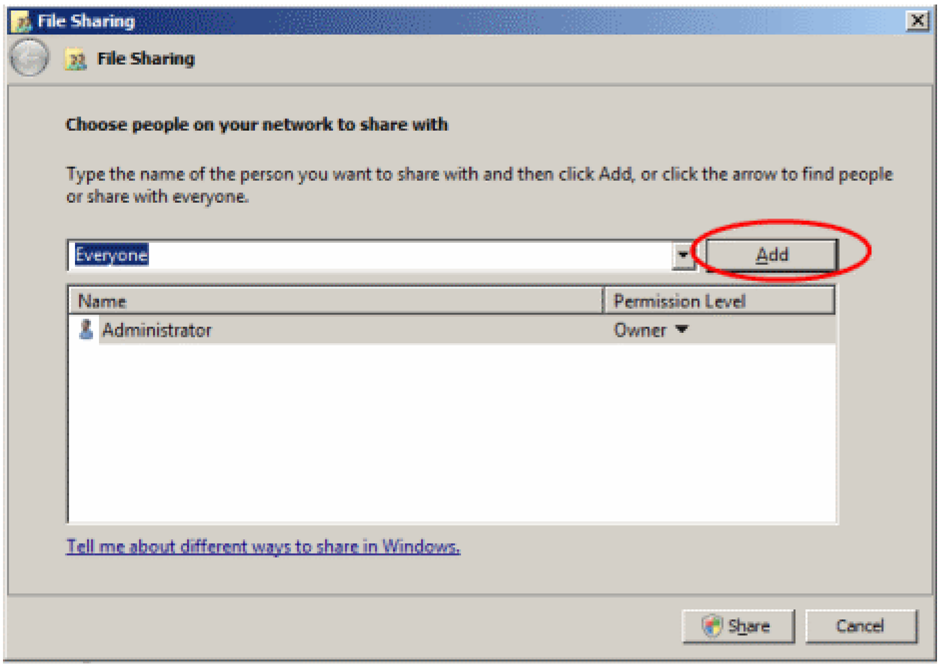
Step 3 – Create a shared network folder and configure permission level

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

- Browse to the location where you want to create a shared folder and create a new folder.
- Name the folder, for example RMM_agent
- Select that folder, right-click and select 'Share' or from the menu toolbar



- Since all endpoints need to have at least read access to this shared folder, select 'Everyone' from the drop-down and click the 'Add' button



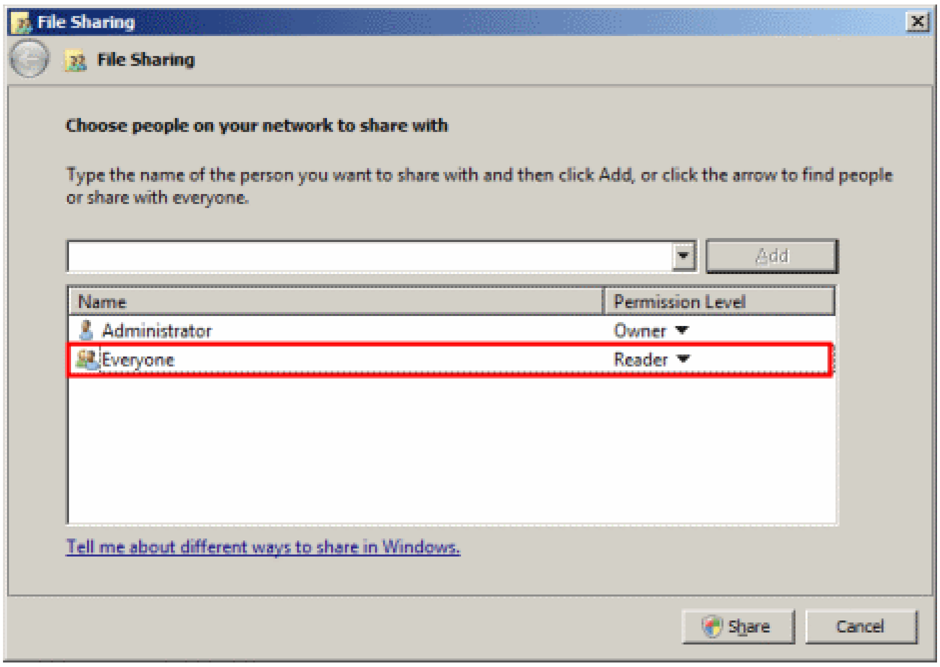
Choose people on your network to share with

Type the name of the person you want to share with and then click Add, or click the arrow to find people or share with everyone.

Everyone

Name	Permission Level
Administrator	Owner

- Ensure the 'Permission Level' is set to 'Reader' and click the 'Share' button at the bottom

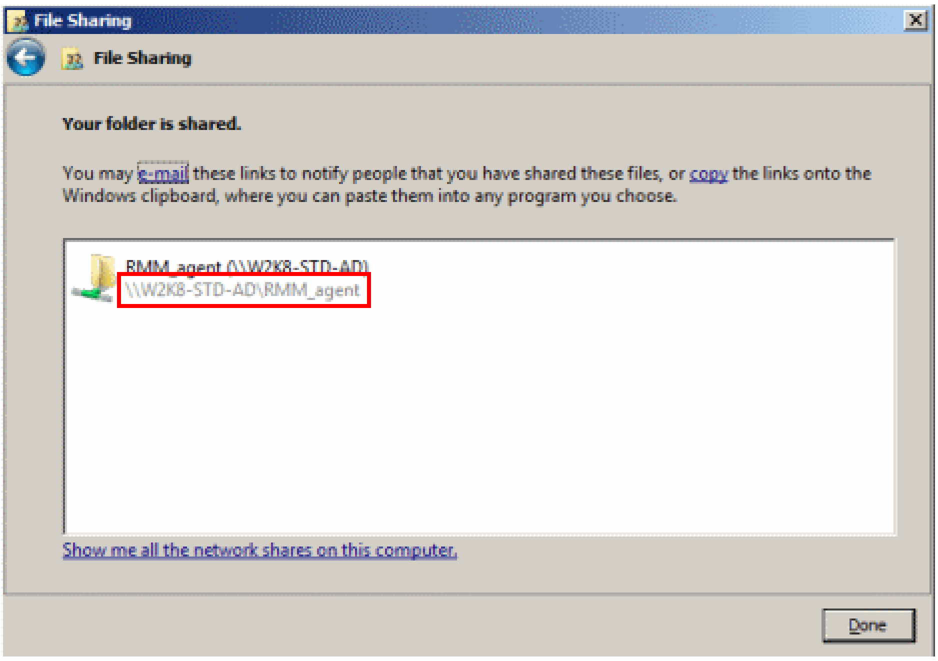


Choose people on your network to share with

Type the name of the person you want to share with and then click Add, or click the arrow to find people or share with everyone.

Name	Permission Level
Administrator	Owner
Everyone	Reader

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



File Sharing

File Sharing

Your folder is shared.

You may e-mail these links to notify people that you have shared these files, or copy the links onto the Windows clipboard, where you can paste them into any program you choose.

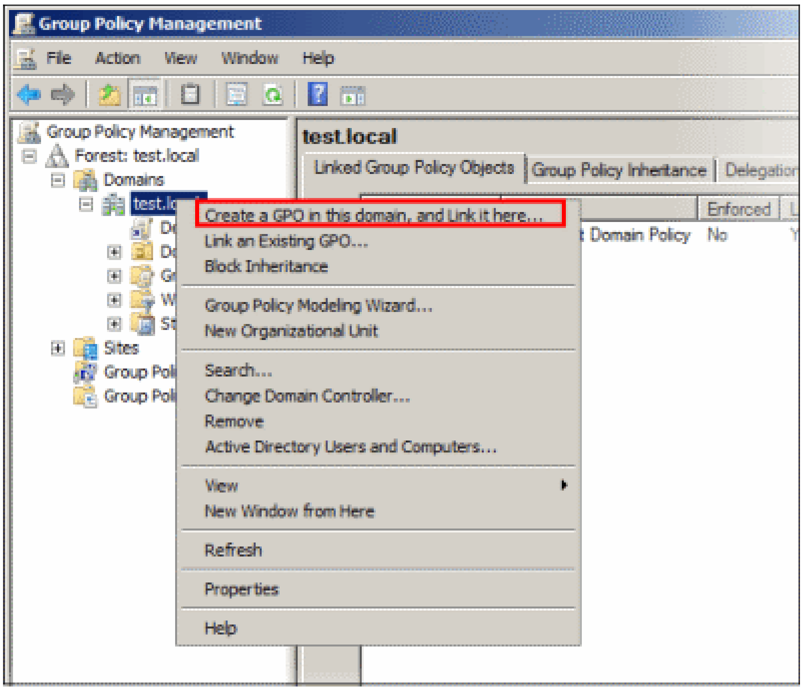
RMM_agent (\\W2K8-STD-AD)
\\W2K8-STD-AD\RMM_agent

Show me all the network shares on this computer.

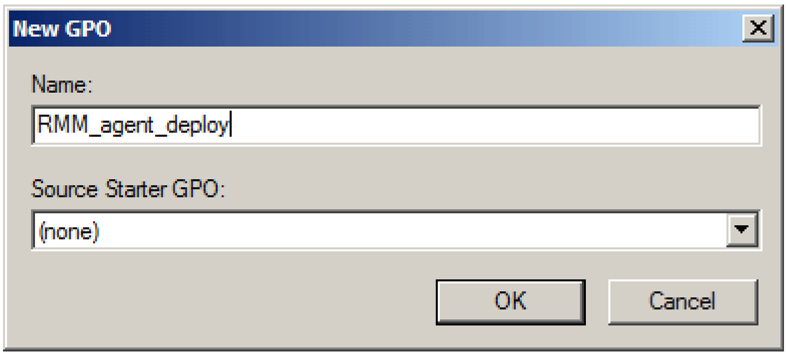
Step 4 – Create a Group Policy and Assign the package

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

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



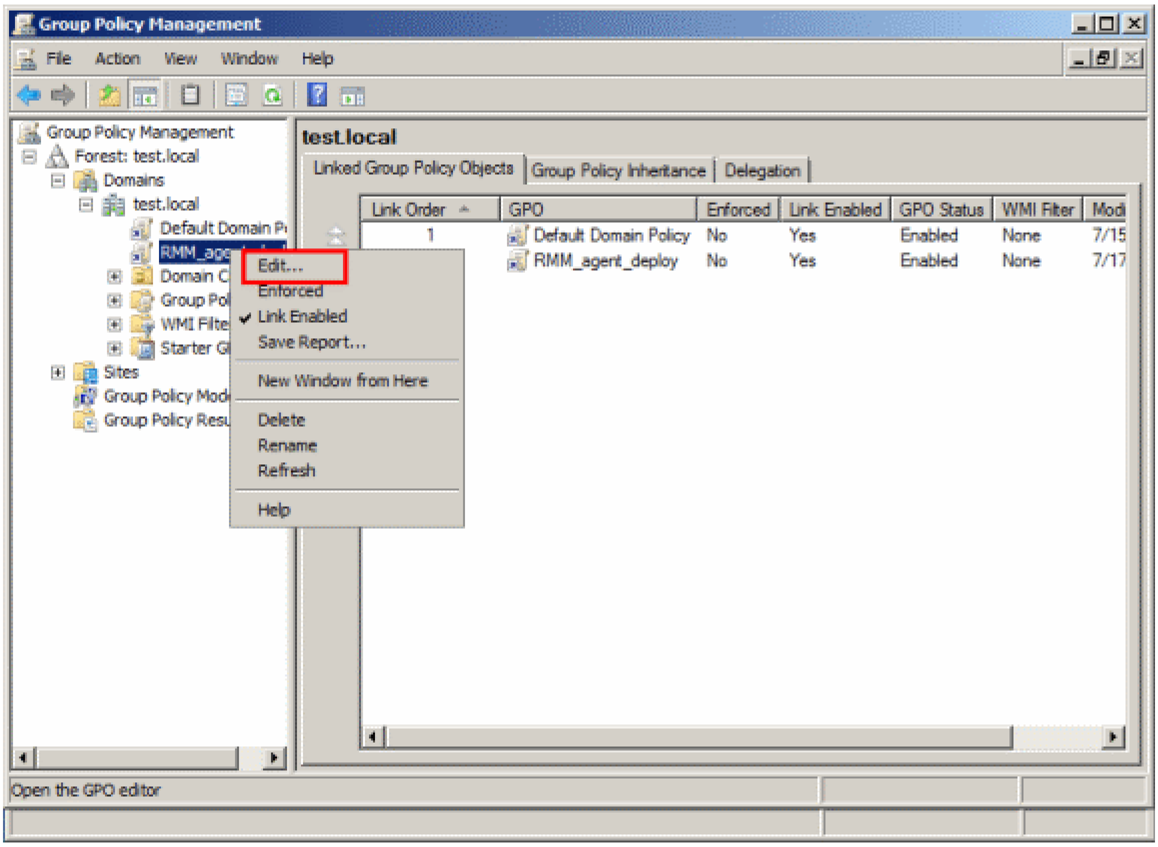
- Enter a name for the group policy in the 'New GPO' dialog



- Click 'OK'

The newly added group policy will be listed.

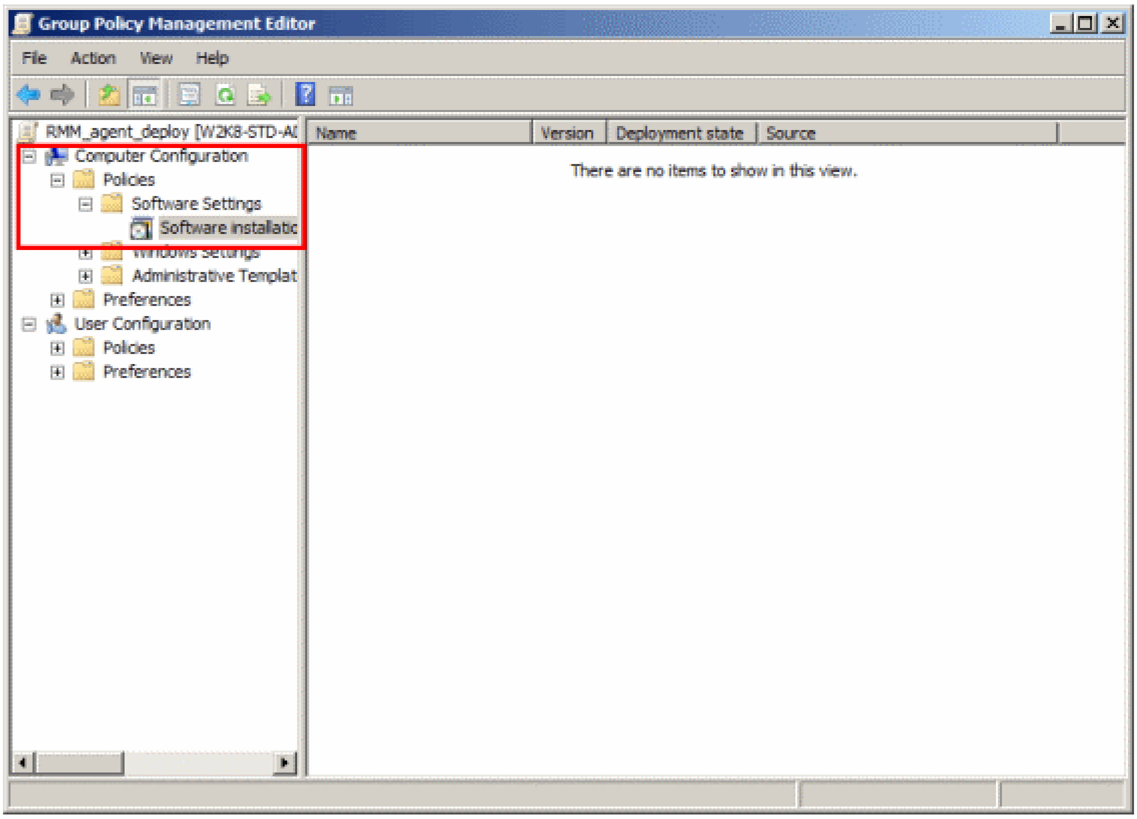
- Right-click on the policy and click the 'Edit' option



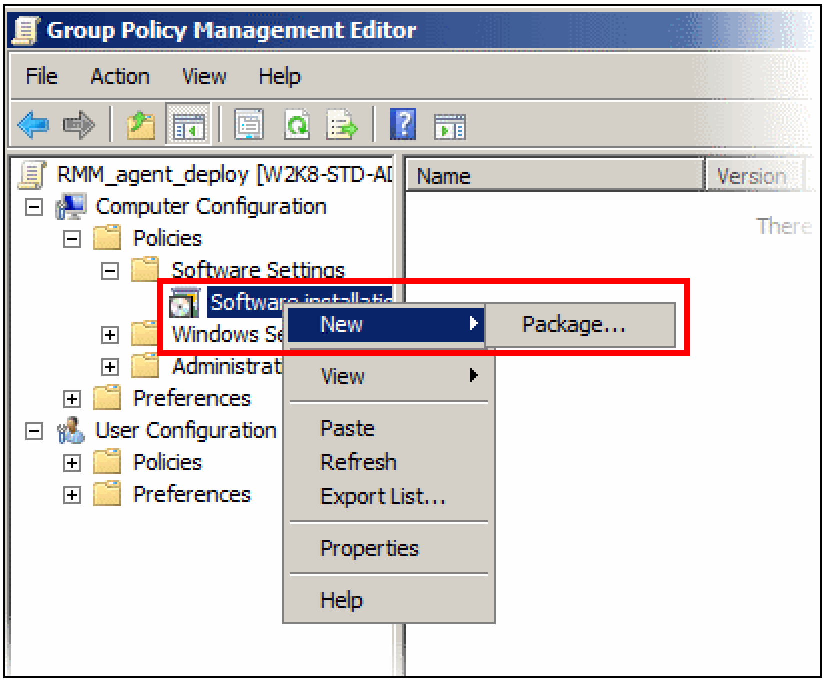
Link Order	GPO	Enforced	Link Enabled	GPO Status	WMI Filter	Modi
1	Default Domain Policy	No	Yes	Enabled	None	7/15
	RMM_agent_deploy	No	Yes	Enabled	None	7/17

The 'Group Policy Management Editor' will be displayed.

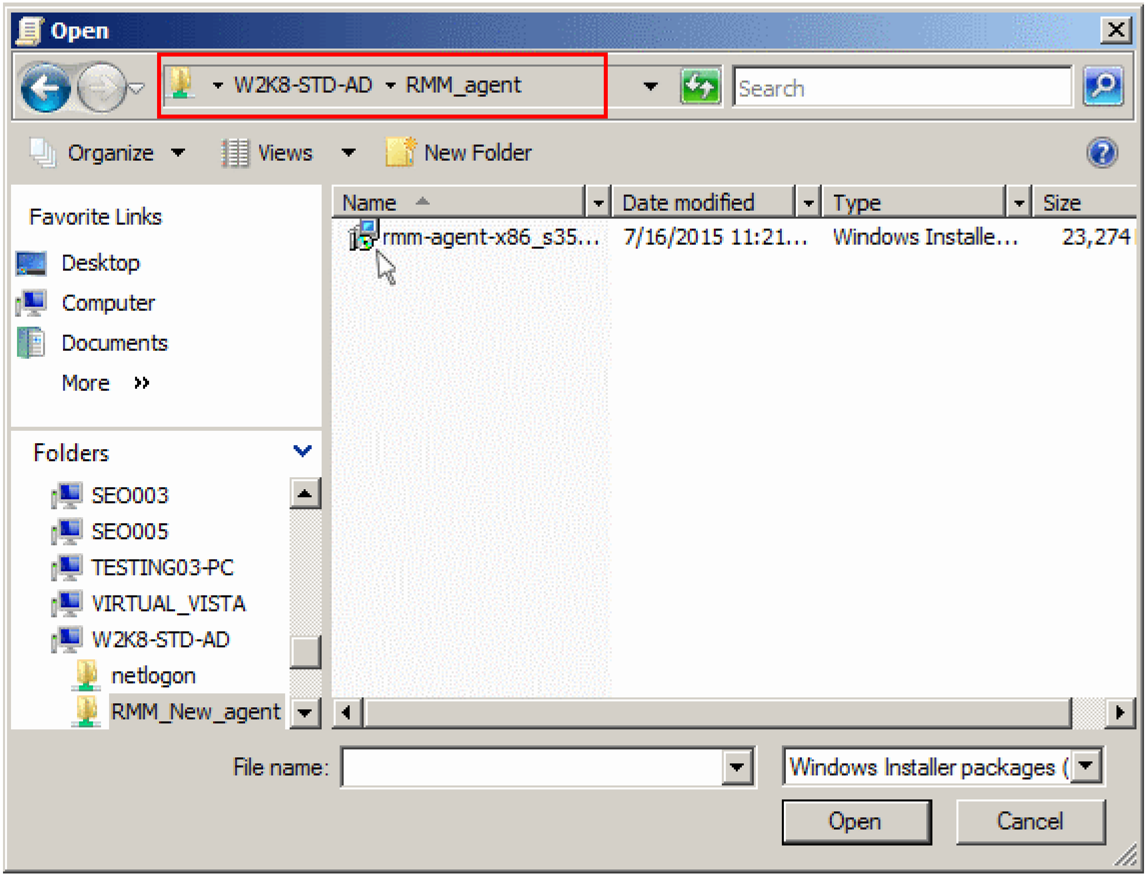
- Expand 'Computer Configuration' > 'Policies' > 'Software Settings'



- 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



W2K8-STD-AD ▸ RMM_agent

Search

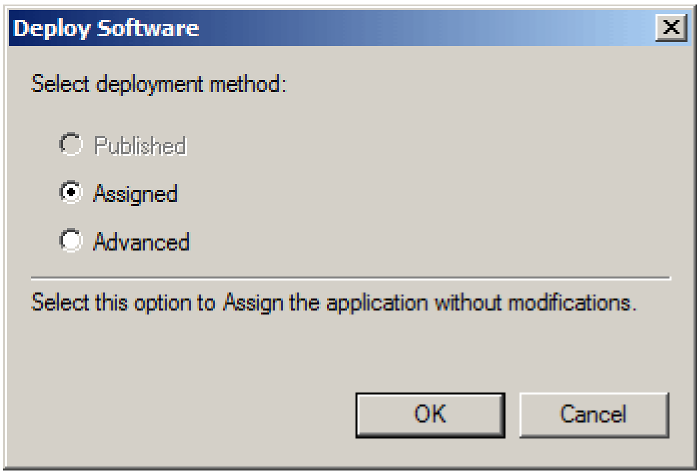
Name	Date modified	Type	Size
rmm-agent-x86_s35...	7/16/2015 11:21...	Windows Installe...	23,274

SE0003
SE0005
TESTING03-PC
VIRTUAL_VISTA
W2K8-STD-AD
netlogon
RMM_New_agent

File name:

Windows Installer packages (

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



Select deployment method:

○ Published
● Assigned
○ Advanced

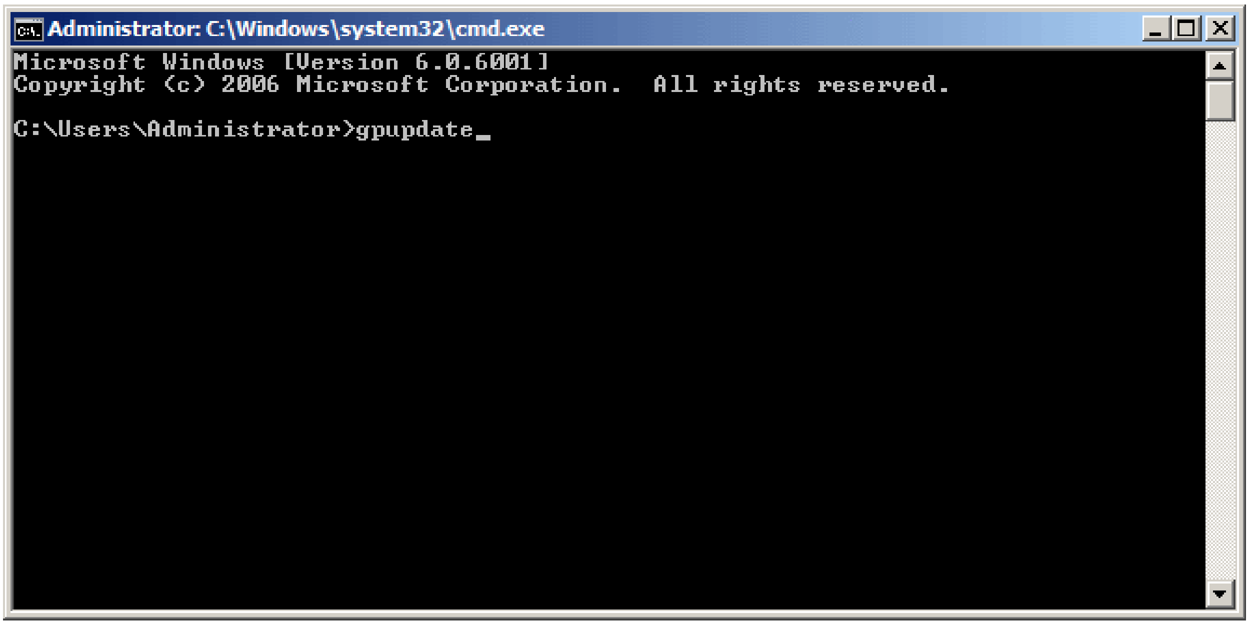
Select this option to Assign the application without modifications.

- Click 'OK'

Step 5 – Run a GPO update

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

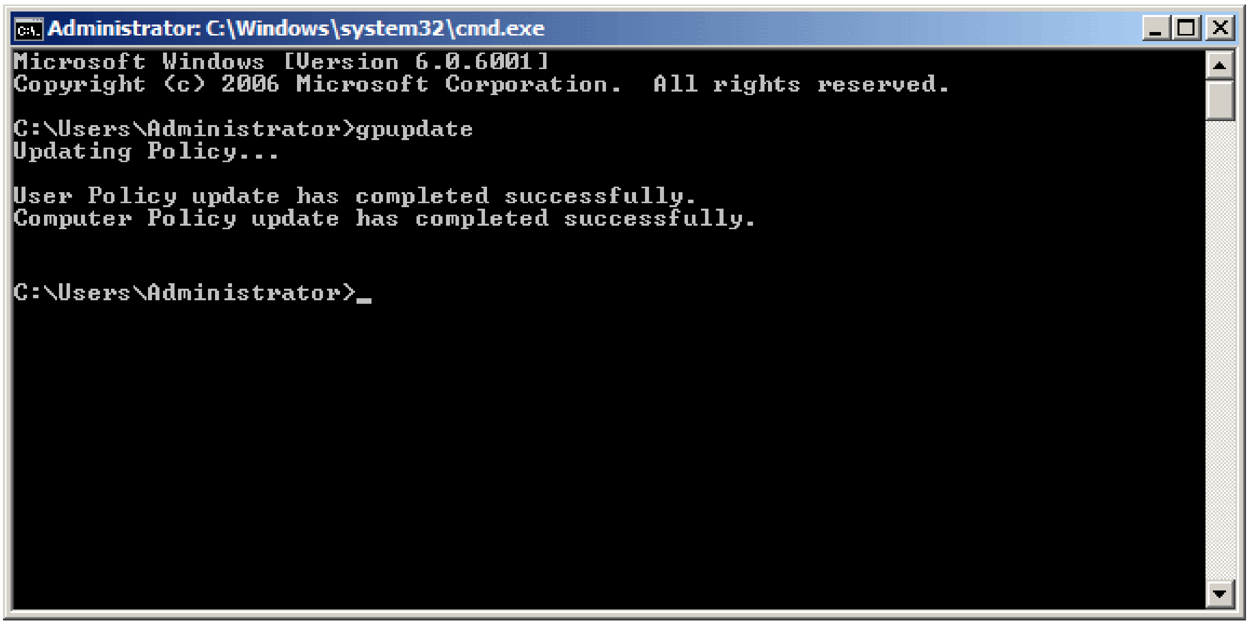
- Open the command prompt and type **gpupdate** and click the 'Enter' button



```
Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.0.6001]
Copyright (c) 2006 Microsoft Corporation.  All rights reserved.

C:\Users\Administrator>gpupdate_
```

The group policy update will be run and a message displayed.



```
Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.0.6001]
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>_
```

Step 6 – Restart the endpoints

After the group policy update is run successfully, the endpoints must be restarted for the RMM agent to be installed.

That's it. You have now successfully enrolled endpoints via AD using the GPO method. You can see the endpoints listed in the RMM admin console under the respective customer site in the 'Devices' screen.

Note: If you try to manually install RMM agent on an endpoint where the GPO was deployed and then removed, you may get an error during the agent installation. Visit the Microsoft support site at **https://support.microsoft.com/en-us/mats/program_install_and_uninstall** and run the tool on the endpoint.

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**