WMI Access - End Machines

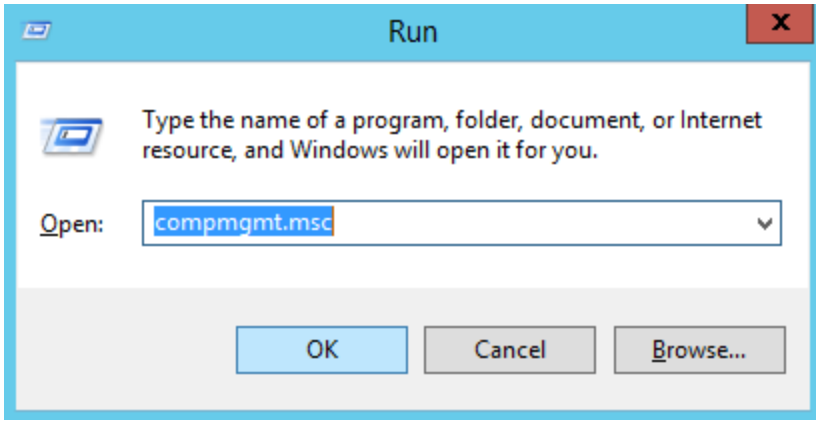
This document outlines how to give WMI access on end machines for users.

Step 1: Enable WMI (Windows Management Instrumentation)

Enable remote WMI requests

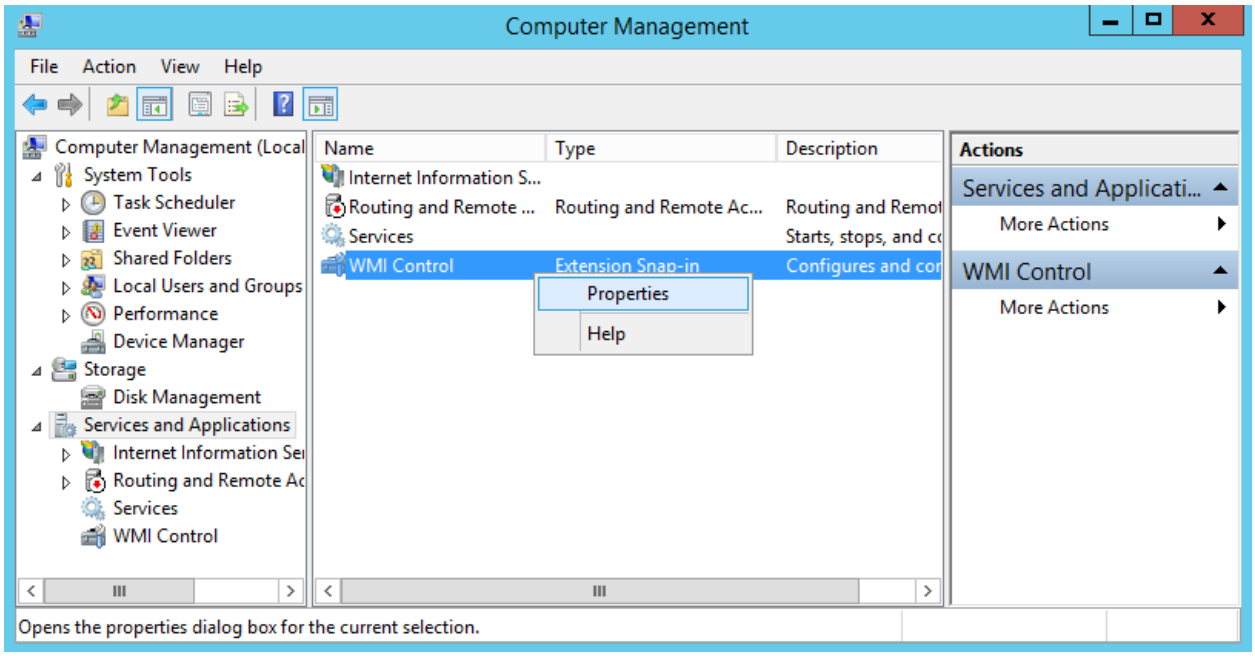
This setting is usually all that needs to be changed on the target server.

1. Through '**Run**' command, execute '**compmgmt.msc**'. 'Computer Management' will be opened.



2. Expand **'Services and Applications'**.

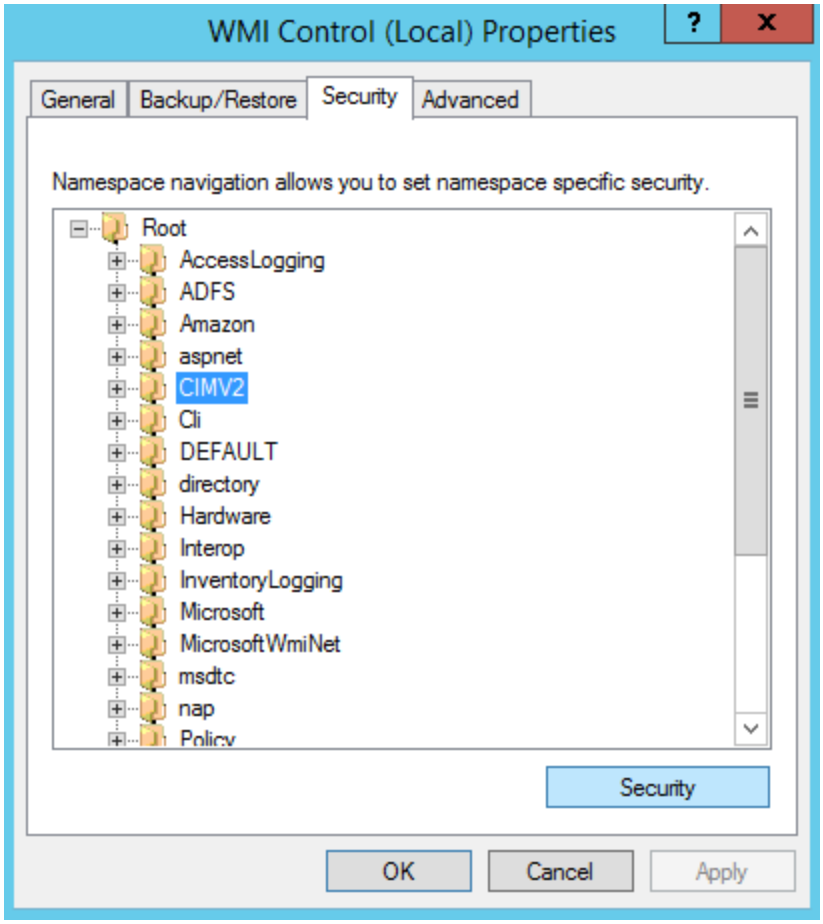
3. Right-click **'WMI Control'** and select '**Properties'**.



4. '**WMI Control Properties**' dialog will open.

5. Select the **'Security'** tab.

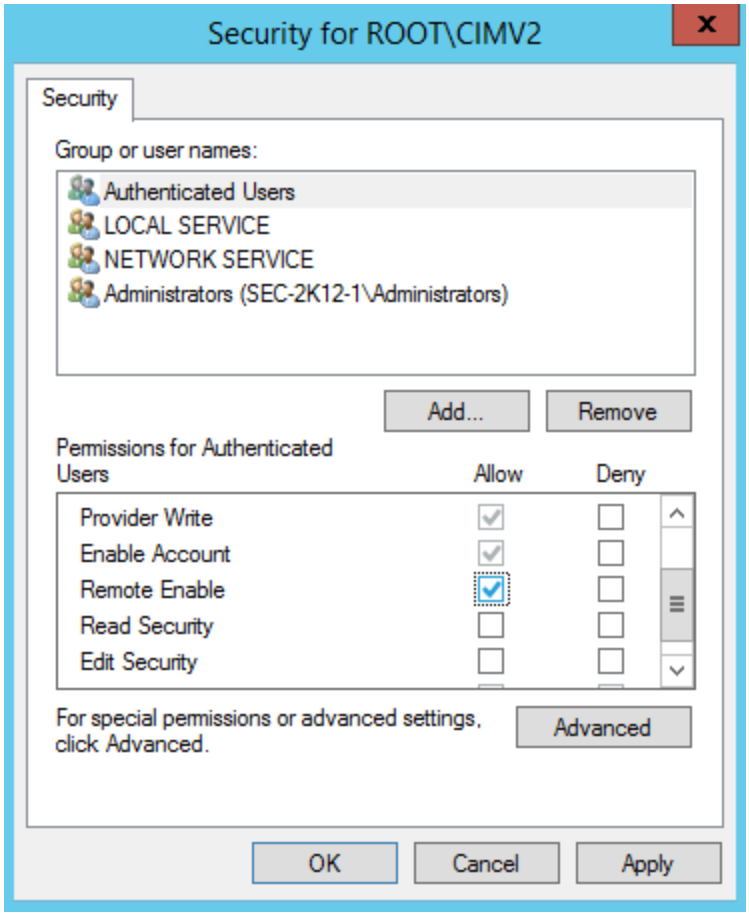
6. Expand to **'Root >> CIMV2**' and then click the **'Security'** button.



7. **'Security for ROOT\CIMV2'** dialog will be opened.

8. Add the local users and local groups for which WMI connectivity has to be allowed and then check '**Remote Enable**' for each user/group added.

   Note: In case, you need to allow WMI connectivity for all users, select the "**Authenticated Users**" group.



9. Apply the changes.

Step 2: Allow WMI through Windows firewall

All users (including non-administrators) should be able to query/read WMI data on the local computer.

For reading WMI data on a remote server, Securden server should be able to establish a connection with the target server. If the target server is running Windows Firewall, you need to instruct it to let remote WMI requests through. Open '**cmd**' as administrator and run the following command on the target computer:

netsh firewall set service RemoteAdmin enable

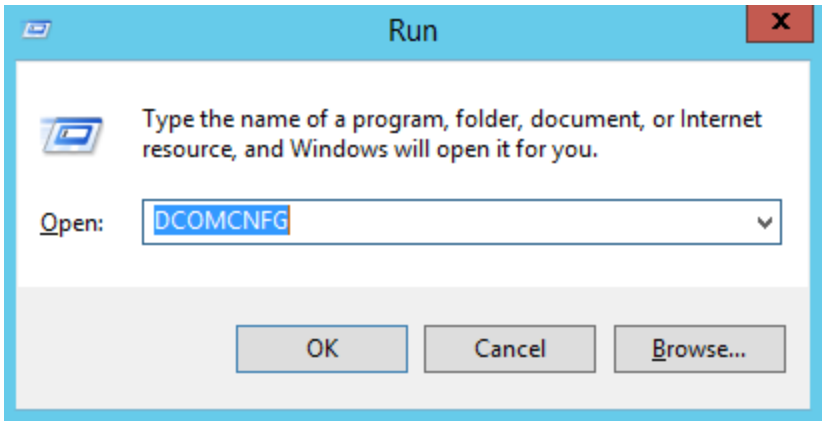
If the target machine runs Windows 10, Windows 2019 or higher, run the following command:

netsh advfirewall firewall set rule group=”Remote Administration” new enable=yes

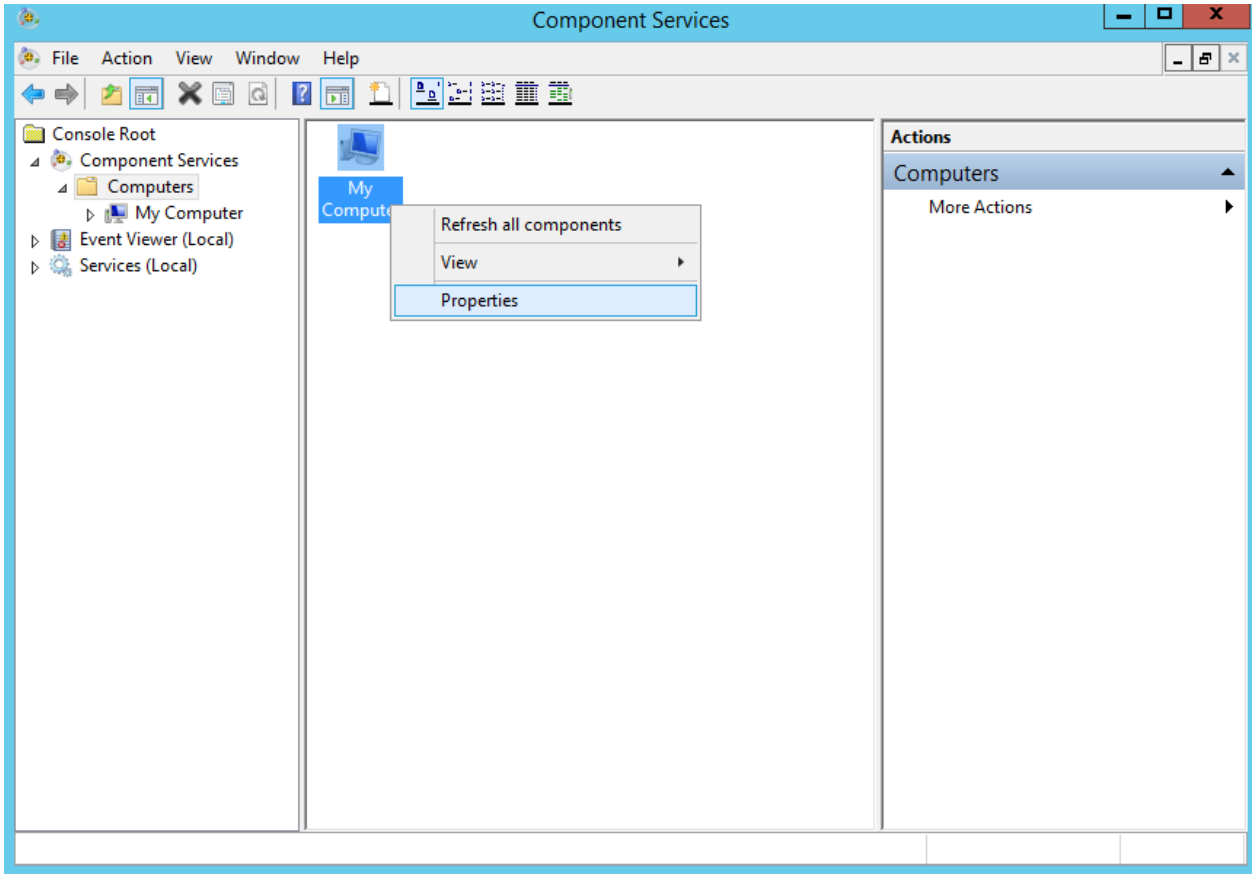
Step 3: Enable DCOM on the remote machine

To grant DCOM remote launch and activation permissions for a user or group:

1. Through ‘**Run**’ command, execute ‘**DCOMCNFG**’. ‘**Component Services**’ dialog will open.

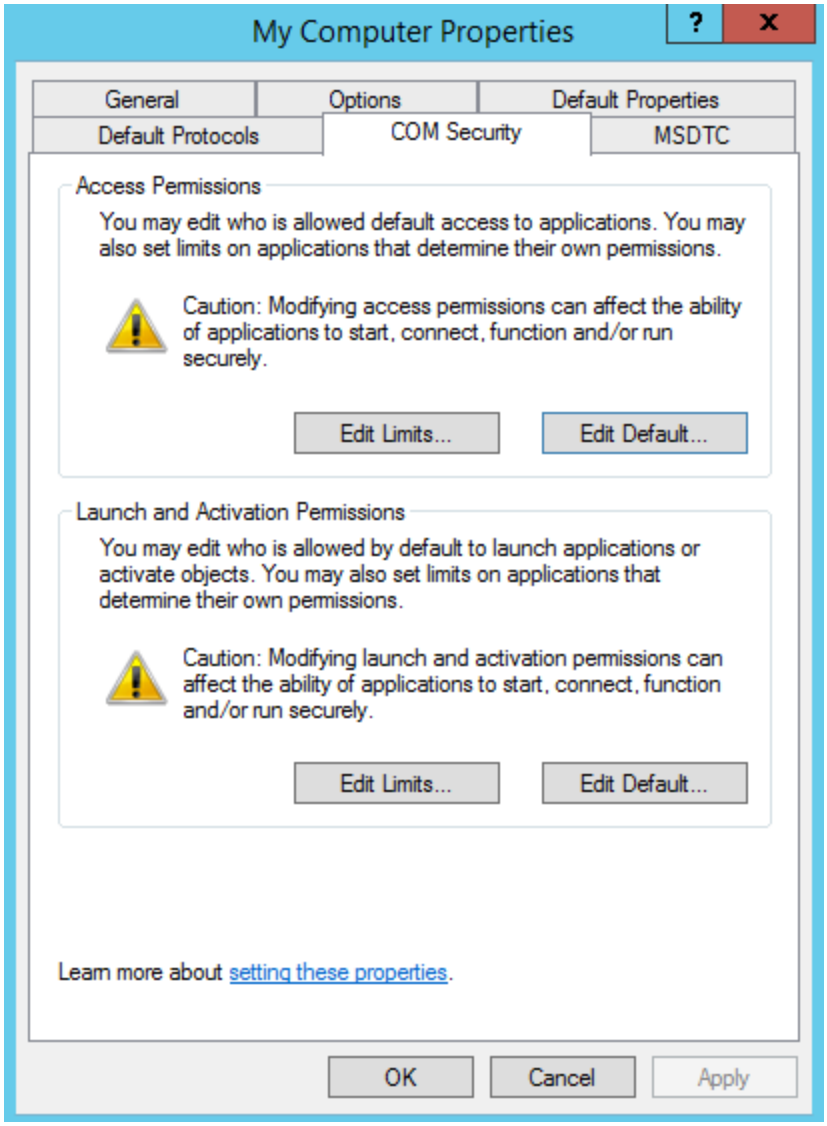


2. Expand ‘**Component Services**’.
3. Right-click ‘**My Computer**’ and click ‘**Properties**’.



4. '**My Computer Properties**' dialog will open.

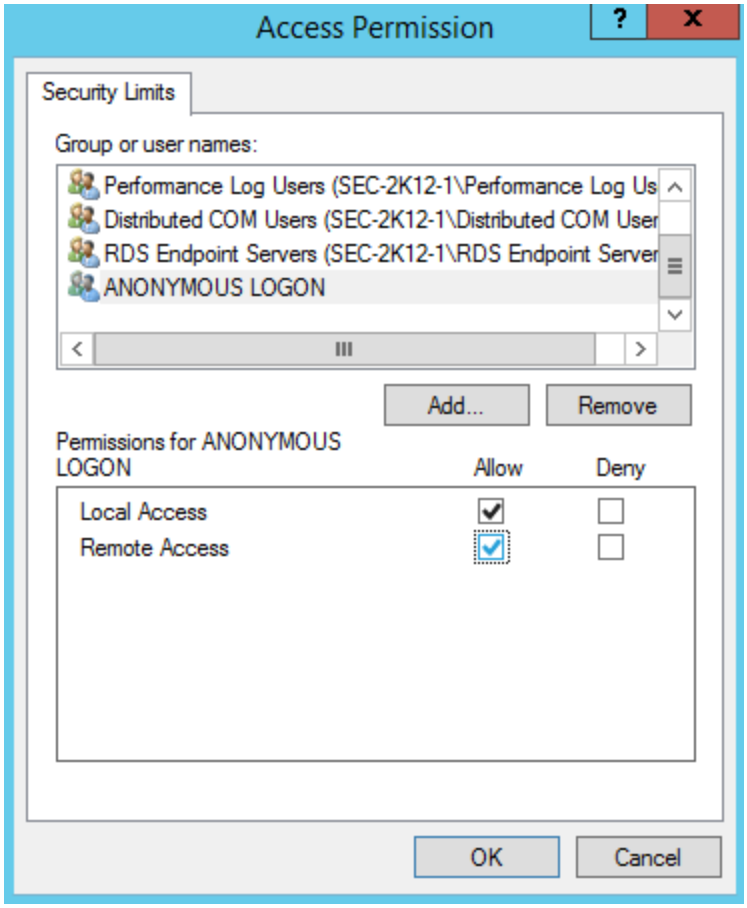
5. Select '**COM Security**' tab.



6. Under '**Access Permissions**', Click '**Edit Limits**'.

7. '**Access Permission**' dialog will open.

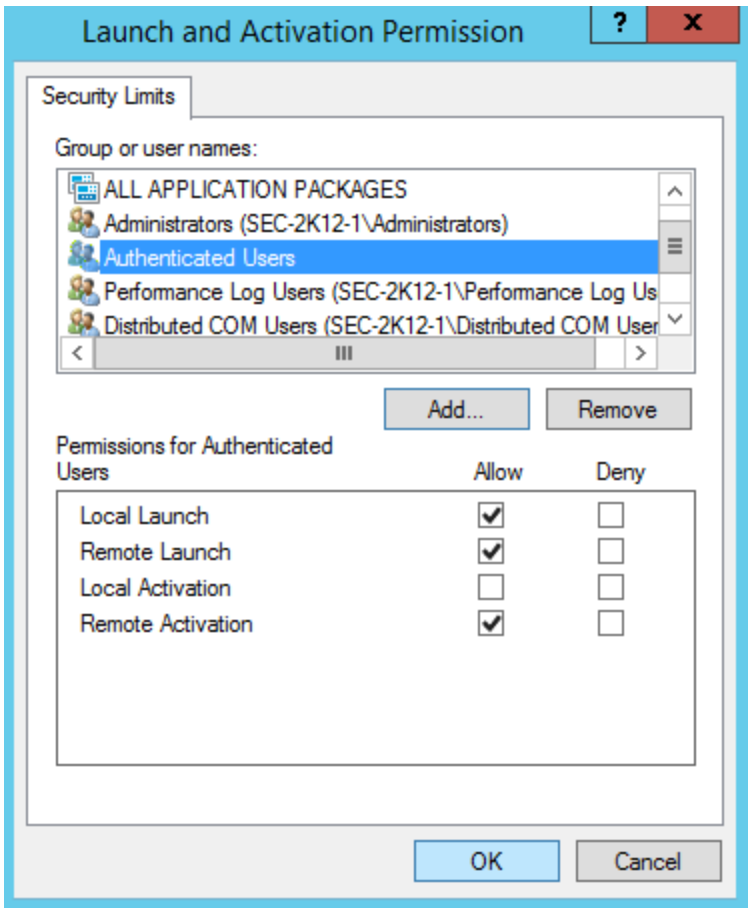
8. Find '**ANONYMOUS LOGON**' and select '**Remote Access**'. Click '**Ok**'.



9. Under '**Launch and Activation Permissions**', click '**Edit Limits**'.

10. '**Launch and Activation Permission**' dialog will open.

11. Add the local users and local groups that you have selected in Step 1 and then select '**Remote Launch**' and '**Remote Activation**' for each user/group. Click '**Ok**'.

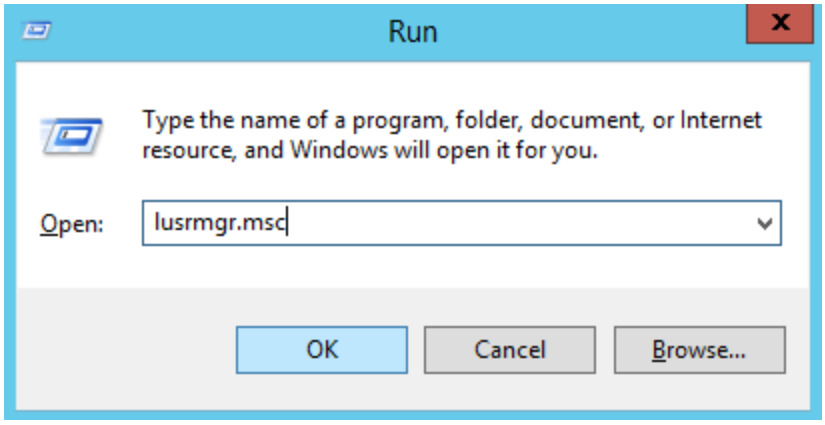


12. Apply the changes.

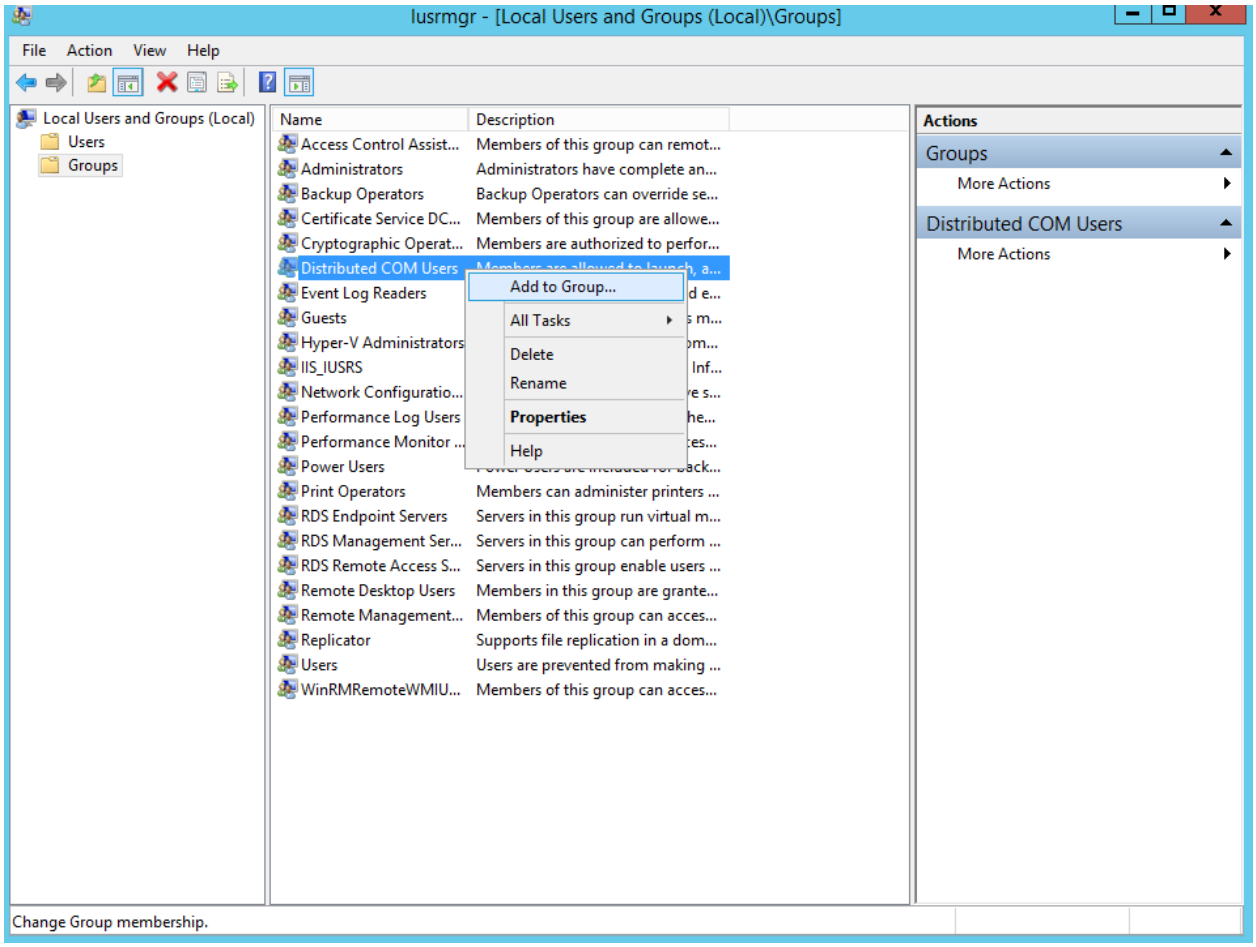
Step 4 Distributed COM Users

The local users have to be added to the "**Distributed COM Users**" group through this step.

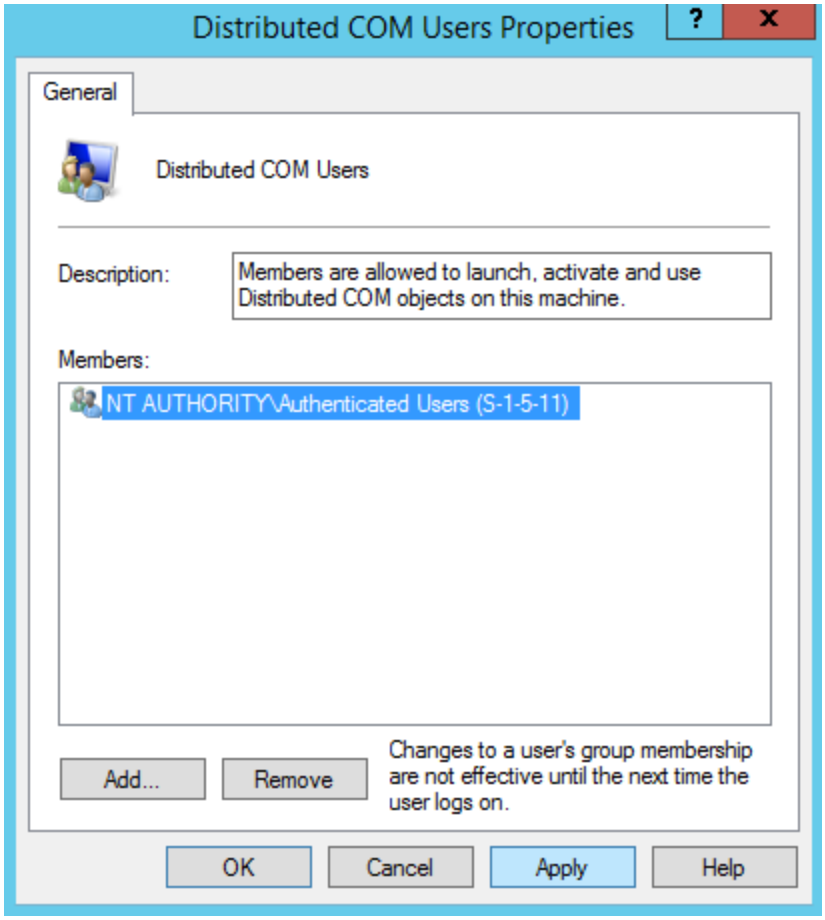
1. Through '**Run**' command, execute '**lusrmgr.msc**'. '**Local Users and Groups**' dialog will open.



2. Expand '**Groups**' and right click '**Distributed COM users**' and select '**Add to Group...**'



3. Add the users and apply the changes.



Notes:

- This document is designed to give WMI access to all users. Also, you can allow access for specific users by adding the respective user in the place of "Authenticated Users" on the steps above.

Reference:

- https://www.poweradmin.com/help/faqs/how-to-enable-wmi-for-remote-access/
- https://docs.microsoft.com/en-gb/windows/desktop/WmiSdk/securing-a-remote-wmi-connection