# **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.

	Run 🗙
	Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.
<u>O</u> pen:	compmgmt.msc 🗸
	OK Cancel <u>B</u> rowse

- 2. Expand 'Services and Applications'.
- 3. Right-click 'WMI Control' and select 'Properties'.

🔄 Computer Management 📃 🗖 🗙				
File Action View Help				
🗢 🏟 🙇 📰 🖼 👔				
🛃 Computer Management (Local	Name	Туре	Description	Actions
Image: System Tools Image: Image: System Tools Image: Image: Image: Image: System Tools Image: I	Internet Information S Routing and Remote	Routing and Remote Ac	Routing and Remot Starts, stops, and co	Services and Applicati  More Actions
<ul> <li>Shared Folders</li> <li>Local Users and Groups</li> <li>Performance</li> <li>Device Manager</li> <li>Storage</li> <li>Disk Management</li> <li>Services and Applications</li> <li>Internet Information Set</li> <li>Routing and Remote Ac</li> </ul>	WMI Control	Extension Snao-in Properties Help	Configures and cor	WMI Control
WMI Control	the current selection.	Ш	> 	

- 4. 'WMI Control Properties' dialog will open.
- 5. Select the **'Security'** tab.
- **6.** Expand to **'Root >> CIMV2**' and then click the **'Security'** button.

WMI Control (Local) Properties ? ×
General Backup/Restore Security Advanced
Namespace navigation allows you to set namespace specific security.
Root   AccessLogging   ADFS   Amazon   aspnet   CIMV2   CIMV2   Ci   DEFAULT   Interop
InventoryLogging      Microsoft      MicrosoftWmiNet      modtc      modt     nap      Policy
Security
OK Cancel Apply

- 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.

Security for R	OOT\CIMV2	x
Security		
Group or user names:		
& Authenticated Users		
& LOCAL SERVICE		
NETWORK SERVICE		
Administrators (SEC-2K12-1)A	aministrators)	
	Add	Remove
Permissions for Authenticated	All	Dami
	Allow	
	✓	
Bemote Enable		
Read Security		
Edit Security		
E		
click Advanced.	eu settings,	Advanced
ОК	Cancel	Apply

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:

 Through 'Run' command, execute 'DCOMCNFG'. 'Component Services' dialog will open.

	Run X
	Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.
<u>O</u> pen:	DCOMCNFG ✓
	OK Cancel <u>B</u> rowse

- 2. Expand 'Component Services'.
- 3. Right-click 'My Computer' and click 'Properties'.

File Action View Window Help     Console Root     Console Root     Computers     My   Computer   My   My   Computer   My   Properties     More Actions     More Actions	۱	Component Servic	tes	_ <b>_</b> X
<ul> <li>◆ ● ② ① ② ② ② ② ② ② ② ② ② ③ ② ③ ③ ③ ③ ③ ③ ③</li></ul>	le Action View Window Help			_ 8 ×
Console Root  Computers  Computer  Refresh all components  Computers  My Computer  Refresh all components  Nore Actions  More Actions  Nore Actions  Computers  Compu				
A Computers A My Computer B My Computer Computer Viewer (Local) Computers View Properties More Actions More Actions	Console Root		Actions	
More Actions     More Actions     More Actions     More Actions     More Actions	△ Component services		Computers	•
> Services (Local)         View          Properties	My Computer      Event Viewer (Local)	Refresh all components	More Actions	•
Properties	<ul> <li>Services (Local)</li> </ul>	View +		
		Properties		
	I			

- 4. 'My Computer Properties' dialog will open.
- 5. Select **COM Security**' tab.

1	My Computer Pro	perties	? X	
General	Options	Defau	It Properties	
Default Protocols	COM Secu	unity	MSDTC	
Access Permissions	1			
You may edit who also set limits on	o is allowed default acce applications that determi	ess to applica ne their own	tions. You may permissions.	
Caution of applic securely	Modifying access permi ations to start, connect,	ssions can a function and	ffect the ability I/or run	
	Edit Limits	Ed	it Default	
Launch and Activat You may edit whi activate objects. determine their or Activate determine their or Caution affect the and/or r	Launch and Activation Permissions You may edit who is allowed by default to launch applications or activate objects. You may also set limits on applications that determine their own permissions. Caution: Modifying launch and activation permissions can affect the ability of applications to start, connect, function and/or run securely.			
	Edit Limits Edit Default			
Leam more about <u>set</u>	Leam more about <u>setting these properties</u> .			
	ОК	Cancel	Apply	

- 6. Under 'Access Permissions', Click 'Edit Limits'.
- 7. 'Access Permission' dialog will open.
- 8. Find **'ANONYMOUS LOGON**' and select **'Remote Access**'. Click **'Ok**'.

Access Pe	ermission	? X
Security Limits		
Group or user names:		
Performance Log Users (SEC & Distributed COM Users (SEC-	-2K12-1\Performa 2K12-1\Distribute	n ce Log Us 🔨 d COM User
RDS Endpoint Servers (SEC-	2K12-1\RDS End	point Server ≡
<		>
	Add	Remove
Permissions for ANONYMOUS LOGON	Allow	Deny
Local Access Remote Access	<ul><li>✓</li></ul>	
	ОК	Cancel

- 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**'.

Launch and Activation	Permission	? X
Security Limits		
Group or user names:		
ALL APPLICATION PACKAG	iES Administrators)	^
Authenticated Users		=
Performance Log Users (SEC     Sec     Distributed COM Users (SEC     III	C-2K12-1\Performa -2K12-1\Distribute	nce Log Us d COM User <sup>V</sup> >
	Add	Remove
Permissions for Authenticated Users	Allow	Deny
Local Launch	~	
Remote Launch		
Remote Activation		
	_	
	ОК	Cancel

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.

	Run 🗙
	Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.
<u>O</u> pen:	lusrmgr.msc 🗸 🗸
	OK Cancel <u>B</u> rowse

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

æ	lusrmgr - [	Local Users and Groups (Local)\Groups]	_ <b>D</b> X
File Action View Help			
🗢 🔿 🖄 🗊 🗙 🗒 🛃 🗊			
💭 Local Users and Groups (Local) 🛛 Name	e Des	cription Actio	ons
📔 Users 🖉 👰 Act	cess Control Assist Mer	mbers of this group can remot Gro	ups 🔺
Groups & Ad	Iministrators Adr	ninistrators have complete an	More Actions
A Bac	ckup Operators Bac	kup Operators can override se	more Actions 7
See Cer	ertificate Service DC Mer	mbers of this group are allowe Dist	ributed COM Users
See Cry	yptographic Operat Mei	mbers are authorized to perfor	More Actions
an Dis	ent Log Peadors	Add to Group	
A Gu			
A Hv	per-V Administrators	All Tasks P . m.	
	IUSRS	Delete Inf	
💀 Net	- etwork Configuratio	Rename /e s	
👰 Per	rformance Log Users	Properties he	
🧶 Per	rformance Monitor	Help :es	
See Por	wer Users	er osers are menaded for pack	
See Prin	int Operators Mer	mbers can administer printers	
See RD:	S Endpoint Servers Serv	rers in this group run virtual m	
	S Management Ser Serv	vers in this group can perform	
are ND.	mote Deckton Users Mer	mbers in this group enable users	
A Rer	mote Management Mer	mbers of this group can acces	
👧 Rep	plicator Sup	ports file replication in a dom	
💀 Use	ers Use	rs are prevented from making	
🕭 Wii	inRMRemoteWMIU Mer	mbers of this group can acces	
Change Group membership.			

3. Add the users and apply the changes.

Di	stributed COM Users Properties 2		
General			
Distribu	Distributed COM Users		
Description:	Members are allowed to launch, activate and use Distributed COM objects on this machine.		
Distributed COM objects on this machine.         Members:         Image: NT AUTHORITY Authenticated Users (S-1-5-11)			
Add Remove Changes to a user's group membership are not effective until the next time the user logs on.			
	OK Cancel Apply Help		

#### 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