



**Getac BIOS Configuration
with
Windows Management
Instrumentation
for Meteor Lake Platform**

Rev 1.00

May 28, 2024

Revision History

Rev	Date	Description
R1.00	2024/5/28	First version

Table of Contents

Revision History	2
1. Modify 2.4.2 Item table & Appendix A-1.Models Mapping Table.錯誤! 尚未定義書籤。	
Chapter 1.Introduction	5
1.1. Overview	5
1.2. Disclaimer	6
Chapter 2.Getac WMI Interface.....	7
2.1. Configure the BIOS Settings	7
2.2. Query BIOS User Password Status.....	7
2.3.Set BIOS User Password	7
2.4.Switch to the BIOS Configure Mode.....	8
2.4.1.Load the default BIOS settings	9
2.4.2.Query/Change the Getac BIOS Settings	9
Appendix A-1.Models Mapping Table.....	13
Appendix B.VB Script to set the supervisor password.....	15
Appendix C.VB Script to Query the OS Select	16
Appendix D.Check Procedure for Remote Access	17
E.1. DCOM permissions	17

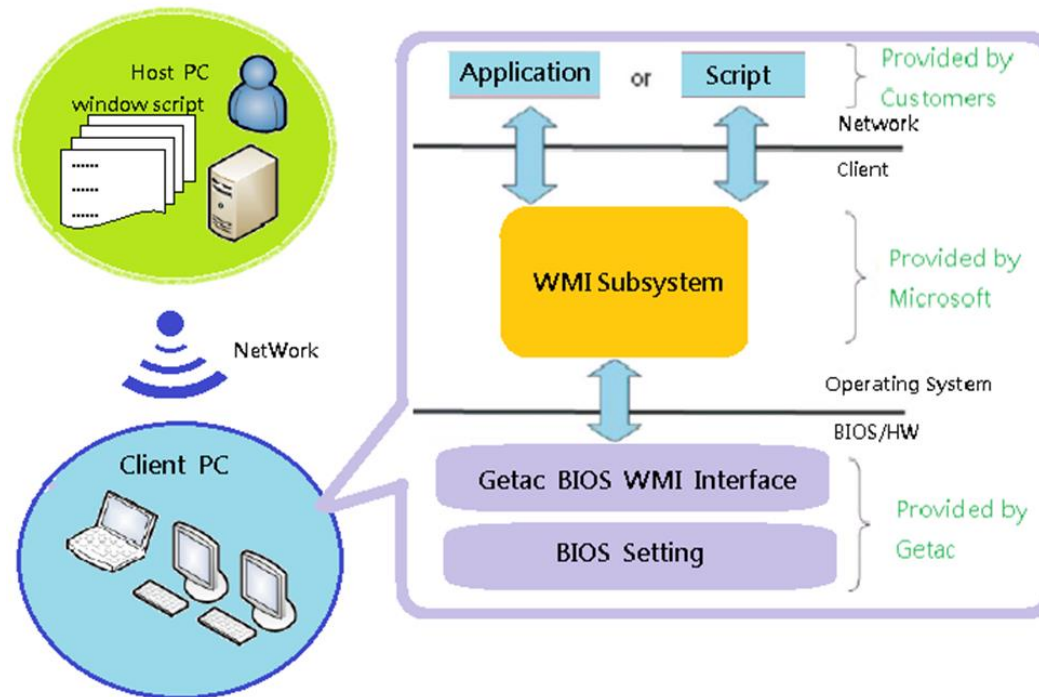
E.2. WMI permissions 18
E.3. WMI impersonation Rights 20
E.4. Network Access 22

Chapter 1.Introduction

This chapter will introduce the Getac WMI and provide users with an overview.

1.1. Overview

Most of Windows® operating systems provide Windows Management Instrumentation (WMI), providing users with the information of local or remote PCs. Getac BIOS WMI interface receives the instruction from Operating system and access the BIOS settings. IT administrator can query and set all the BIOS settings (except read only items), recover the BIOS to factory settings, set and change passwords, and modify the boot order in remote PCs.



1.2. Disclaimer

BIOS settings are related to the WMI instruction and the computer device. Getac assumes no liability for damages incurred directly or indirectly from errors, omissions or discrepancies between the computers' BIOS and the manual.

Chapter 2. Getac WMI Interface

In this chapter, details of how to operate the Getac WMI Interface to access the BIOS settings in remote PCs are illustrated.

2.1. Configure the BIOS Settings

The following interface accesses the Getac BIOS settings.

Namespace: “\root\WMI”

2.2. Query BIOS User Password Status

Users can check if the password is registered in this class.

Class name/Method name: Query_GetacBIOSPassWord

Type: Method

Example: “SUIPW”

Item table:

Page	Item	WMI Item	Attr.
Security	Set Supervisor password	SUIPW	R
	Set User password	USERPW	R

Return value: “Registered”, “Null”, “Not support”

2.3. Set BIOS User Password

Supervisor Password and User Password are set in this class. If users want to set User Password, the Supervisor Password must be set first.

If the Supervisor Password is clear, then the User Password will be clear as well.

Class name/Method name: Set_GetacBIOSPassWord

Type: Method

Example: “SUIPW,1e234,AB4567”



Item table:

Page	Item	WMI Item	Attr.	Current PW	New PW
Security	Set Supervisor password	SUVPW	W	*note1	*note2/3
	Set User password	USERPW	W	*note1	*note2/3

*note1: If the password is not registered, the blank is set to Current PW for password setting.

*note2: If the blank is set to New PW, the current password will be deleted.

*note3: By default, the maximum length of a password is 10. For models supporting “StrongPassword”, the maximum length of a password can be up to 64 and the minimum length as 4.

Return value: “Success”, “Fail”, “Not support”

Note : If the WMI item is not provided, the return value will be “Not support”

2.4.Switch to the BIOS Configure Mode

Regarding BIOS security, users must switch to the BIOS configure mode before accessing the Getac WMI Interface. If Getac WMI interface receives wrong Supervisor Password 3 times, Getac WMI interface will lock down due to security reasons. If the Getac WMI interface is locked, any access will return “Locked”. Users can enter BIOS setup utility to unlock.

Class name/Method name: Set_GetacBIOSConfigMode

Type: Method

Example: “1234,SetStart” (if Supervisor password [SUVPW] is 1234.)

Item table:

WMI Item	Description
SUVPW	Supervisor password(*note1)
SetStart	Start of the access mode of BIOS when the supervisor is registered.
SetEnd	End of the access mode of BIOS.

*note1: By default, the maximum length of a password is 10. For models supporting “StrongPassword”, the maximum length of a password can be up to 64 and the minimum length as 4.

Return value: “Success”, “Fail”, “Not support” , “Locked”

2.4.1.Load the default BIOS settings

This class name can recover BIOS to default settings.

Class name: Load_GetacDefaultSettings

Type: Method

Return value: "Success", "Fail", "Locked"

Note: As security-related options, the password is not recovered even if "load default" is requested.

2.4.2.Query/Change the Getac BIOS Settings

This section contains details on the WMI implementation for Query/Change Getac BIOS settings.

The queries can be used to retrieve setting values currently set.

Class name/Method name: Query_GetacBIOSSettings

Type: Method

Example: "OSSelect"

Note: If the Query item is not provided, the return value will be "Not support"

To change/set the BIOS settings,

Class name/Method name: Set_GetacBIOSSettings

Type: Method

Example1: "LegacyUSBSupport,Enabled"

Example2 : "BootTypeOrder, HardDisk, USBDisk,USBFloppy ,Network,USBCD"

Return value: "Success", "Fail", "Locked","Not Support"

Item table:

Page	Item	WMI Item/ Return Item	Attr.	Return/AcceptValues	
Information	EC Version	ECVersion	R	R1.00.070520	
	Virtual MAC Address (*Note1)	VirtualMAC	R	XX-XX-XX-XX-XX-XX	
Main	Internal Numlock	InternalNumlock	R/W	"Disabled","Enabled"	
	FN and Ctrl Key Placement	FNCtrlKeyPlacement	R/W	"CtrlFN","FNCtrl"	
	WMI Version	WMIVersion	R	"0.00"- "9.99"	
Advanced	Wake Up Capability	HomeButtonWakeup	R/W	"Disabled", "Enabled"	
	Power Button Delay	PowerButtonDelay	R/W	"NoDelay", "1sec", "2sec"	
	AC Initiation	ACInitiation	R/W	"Disabled", "Enabled"	
	Hybrid Power	HybridPower	R/W	"Disabled", "Enabled"	
	Magnetic Sensor	MagneticSensor	R/W	"Enabled", "Disabled"	
	USB Power-off Charging	USBPowerOffCharging	R/W	"Disabled", "Enabled"	
	Screen Tapping for Boot Options	ScreenTappingforBootOp	R/W	"Disabled", "Enabled"	
	MAC Address Pass Through	MACAddressPassThrough	R/W	"Disabled", "Enabled"	
	Active Management Tech. Support (*Note2)	IntelAMTSupport	IntelAMTSupport	R/W	"Disabled", "Enabled"
		IntelAMTSetupPrompt	IntelAMTSetupPrompt	R/W	"Disabled", "Enabled"
		IntelAMTUSBProvision	IntelAMTUSBProvision	R/W	"Disabled", "Enabled"
		IntelTME	IntelTME	R/W	"Disabled", "Enabled"
	Virtualization Tech.	IntelVT	IntelVT	R/W	"Disabled", "Enabled"
VTd		VTd	R/W	"Disabled", "Enabled"	
Device	WirelessLAN	R/W	"Disabled", "Enabled"		

Page	Item	WMI Item/ Return Item	Attr.	Return/AcceptValues
	Configuration	WWAN	R/W	"Disabled", "Enabled"
		Bluetooth	R/W	"Disabled", "Enabled"
		MediaCardReader	R/W	"Disabled", "Enabled"
		SmartCardReader	R/W	"Disabled", "Enabled"
		RFID	R/W	"Disabled", "Enabled"
		FingerprintScanner	R/W	"Disabled", "Enabled"
		FrontWebcam	R/W	"Disabled", "Enabled"
		RearCamera	R/W	"Disabled", "Enabled"
		BarcodePM	R/W	"PowerSaving", "QuickStart"
		Thunderbolt	R/W	"Disabled", "Enabled"
		SystemUSBPort	R/W	"Disabled", "Enabled"
		DockingUSBPortSetting	R/W	"USB2.0", "USB3.0"
		InternalMicrophone	R/W	"Disabled", "Enabled"
		InternalSpeaker	R/W	"Disabled", "Enabled"
		SerialPort	R/W	"Disabled", "Enabled"
	Asset Tag	AssetTag	R/W	32 characters maximum
Security	StrongPassword	StrongPassword	R/W	"Disabled", "Enabled"
	Password on Boot	PasswordonBoot	R/W	"Disabled", "Enabled"
	PasswordConfig	PasswordConfig	R/W	"04"-"64"
	Secure Boot Configuration (*Note3)	LoadMSFTUEFICA	R/W	"Disabled", "Enabled"
	Security Freeze Lock	SecurityFreezeLock	R/W	"Disabled", "Enabled"
	Intel Trusted Execution Technology	IntelTrustedExeTech	R/W	"Disabled", "Enabled"

Page	Item	WMI Item/ Return Item	Attr.	Return/AcceptValues
	(*Note2)			
Boot	Boot Type Order (*Note4)	BootTypeOrder	R/W	"HardDisk", "USBDrive", "USBBD", "Network", "CDROM"
	Boot Device	HardDiskDrive	R/W	"Off", "On"
		USBDrive	R/W	"Off", "On"
		USBBDVDDrive	R/W	"Off", "On"
		NetworkDrive	R/W	"Off", "On"
		CDDVDDrive	R/W	"Off", "On"
	Fast Boot	FastBoot	R/W	"Disabled", "Enabled"
Alternative WBM option	AlternativeWBM	R/W	"Disabled", "Enabled"	

*Note1: It will return virtual MAC address when there is no physical network card in this system.

*Note2: Only AMT SKU systems are supported.

*Note3: Supervisor password is needed. Otherwise, system will return value as "fail".

"Disable" option won't delete MSFT CA Key.

To delete it, please restore to Factory Defaults manually.

Disable bitlocker function before executing LoadMSFTUEFICA. Otherwise, input bitlocker recovery key will be required after LoadMSFTUEFICA.

*Note4:

"BootTypeOrder" Individual model return/accept values case	
S510	Others
"HardDisk", "USBDrive", "Network", "USBBD", "CDROM"	"HardDisk", "USBDrive", "Network", "USBBD"

O = Support
X = Not Support

Appendix A-1.Models Mapping Table

Page	Item	WMI Item/ Return Item	Attr.	S510	VR- XG20G3				
Information	EC Version	ECVersion	R	O	O				
	Virtual MAC Address	VirtualMAC	R	X	X				
Main	Internal Numlock	InternalNumlock	R/W	O	X				
	FN and Ctrl Key Placement	FNCtrlKeyPlacement	R/W	O	X				
	WMI Version	WMIVersion	R	O	O				
Advanced	WakeUp Capability	HomeButtonWakeup	R/W	X	X				
	Power Button Delay	PowerButtonDelay	R/W	O	X				
	AC Initiation	ACInitiation	R/W	O	O				
	Hybrid Power	HybridPower	R/W	O	X				
	Magnetic Sensor	MagneticSensor	R/W	O	X				
	USB Power-off Charging	USBPowerOffCharging	R/W	O	X				
	Screen Tapping for Boot Options	ScreenTappingforBootOp	R/W	X	O				
	MAC Address Pass Through	MACAddressPassThrough	R/W	O	X				
	Active Management Tech. Support	IntelAMTSupport	R/W	O	X				
		IntelAMTSetupPrompt	R/W	O	X				
		IntelAMTUSBProvision	R/W	O	X				
		IntelTME	R/W	O	X				
	Virtualization Tech. Setup	IntelVT	R/W	O	O				
		VTd	R/W	O	O				
	Device Configuration	WirelessLAN	R/W	O	O				
		WWAN	R/W	O	O				
		Bluetooth	R/W	O	O				
		MediaCardReader	R/W	O	X				
		SmartCardReader	R/W	O	X				
		RFID	R/W	O	X				
FingerprintScanner		R/W	O	X					
FrontWebcam	R/W	O	X						

Page	Item	WMI Item/ Return Item	Attr.	S510	VR- XG20G3			
		RearCamera	R/W	X	X			
		BarcodePM	R/W	O	X			
		Thunderbolt	R/W	O	X			
		SystemUSBPort	R/W	O	X			
		DockingUSBPortSetting	R/W	O	X			
		InternalMicrophone	R/W	O	X			
		InternalSpeaker	R/W	O	X			
		SerialPort	R/W	O	O			
	Asset Tag	AssetTag	R/W	O	X			
Security	Password on Boot	PasswordonBoot	R/W	O	O			
	StrongPassword	StrongPassword	R/W	O	O			
	PasswordConfig	PasswordConfig	R/W	O	O			
	Secure Boot Configuration	LoadMSFTUEFICA	R/W	O	X			
	SecurityFreezeLock	SecurityFreezeLock	R/W	O	X			
	Intel Trusted Execution Technology	IntelTrustedExeTech	R/W	O	O			
Boot	Boot Type Order	BootTypeOrder	R/W	O	O			
	Boot Device	HardDiskDrive	R/W	O	O			
		USBDrive	R/W	O	O			
		USBCDDVDDrive	R/W	O	O			
		NetworkDrive	R/W	O	O			
		CDDVDDrive	R/W	O	X			
Fast Boot	FastBoot	R/W	O	X				
	Alternative WBM option	AlternativeWBM	R/W	O	X			

Appendix B.VB Script to set the supervisor password

User can set the Supervisor Password with below VB Script when the Supervisor Password is not registered and "1" is set.

```
strComputer = "."
Set objWMIService = GetObject("winmgmts:\\." & strComputer & "\root\WMI")

'-----
' Obtain an instance of the class
' using a key property value.
'-----
Set objShare = objWMIService.Get("Set_GetacBIOSPassWord.InstanceName='ACPI\PNP0C14\0_0'")

'-----
' Obtain an InParameters object specific to the method.
'-----
Set objInParam = objShare.Methods_("Set_GetacBIOSPassWord").inParameters.SpawnInstance_()

'-----
' Add the input parameters.
'-----
objInParam.Properties_.Item("DataIn") = "SUIPW,,1"

'-----
' Execute the method and obtain the return status.
' TheOutParameters object in objOutParams is created by the provider.
'-----
Set objOutParams = objWMIService.ExecMethod("Set_GetacBIOSPassWord.InstanceName='ACPI\PNP0C14\0_0'",
"Set_GetacBIOSPassWord", objInParam)

'-----
' ListOutParams
'-----
Wscript.Echo "Out Parameters: " & objInParam.Properties_.Item("DataIn")
Wscript.Echo "DataOut: " & objOutParams.DataOut
```

Appendix C.VB Script to Query the OS Select

Users can query OS select with below VBScript.

```
strComputer = "."
Set objWMIService = GetObject("winmgmts:\\." & strComputer & "\root\WMI")

'-----
' Obtain an instance of the class
' using a key property value.
'-----

Set objShare = objWMIService.Get("Query_GetacBIOSSettings.InstanceName='ACPI\PNP0C14\0_0'")

'-----
' Obtain an InParameters object specific to the method.
'-----

Set objInParam = objShare.Methods_("Query_GetacBIOSSettings").inParameters.SpawnInstance_()

'-----
' Add the input parameters.
'-----

objInParam.Properties_.Item("DataIn") = "OSSelect"

'-----
' Execute the method and obtain the return status.
' The OutParameters object in objOutParams is created by the provider.
'-----

Set objOutParams = objWMIService.ExecMethod("Query_GetacBIOSSettings.InstanceName='ACPI\PNP0C14\0_0'",
"Query_GetacBIOSSettings", objInParam)

'-----
' List OutParams
'-----

Wscript.Echo "Out Parameters: " & objInParam.Properties_.Item("DataIn")
Wscript.Echo "DataOut: " & objOutParams.DataOut
```


Appendix D. Check Procedure for Remote Access

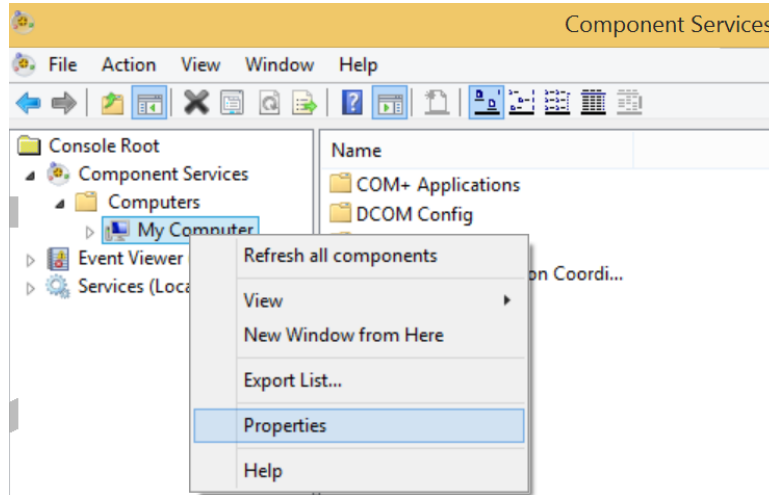
E.1. DCOM permissions

Step 1. Search -> “Dcomcnfg”

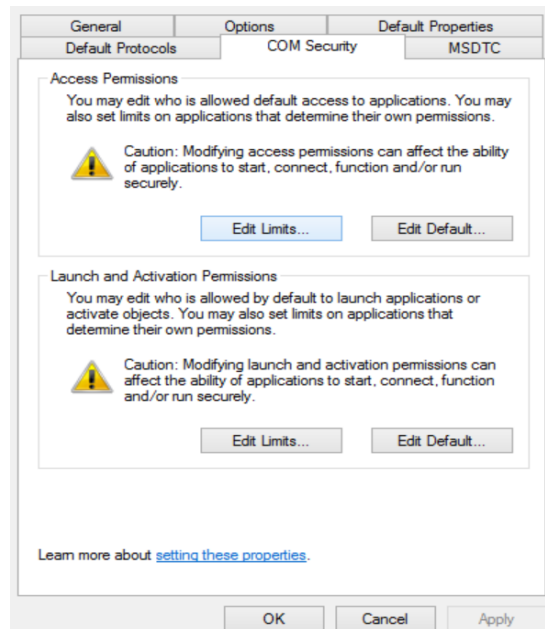
Step 2. Run “Dcomcnfg”

Step 3. Expand “Component Services” -> “Computers” -> “My Computer”

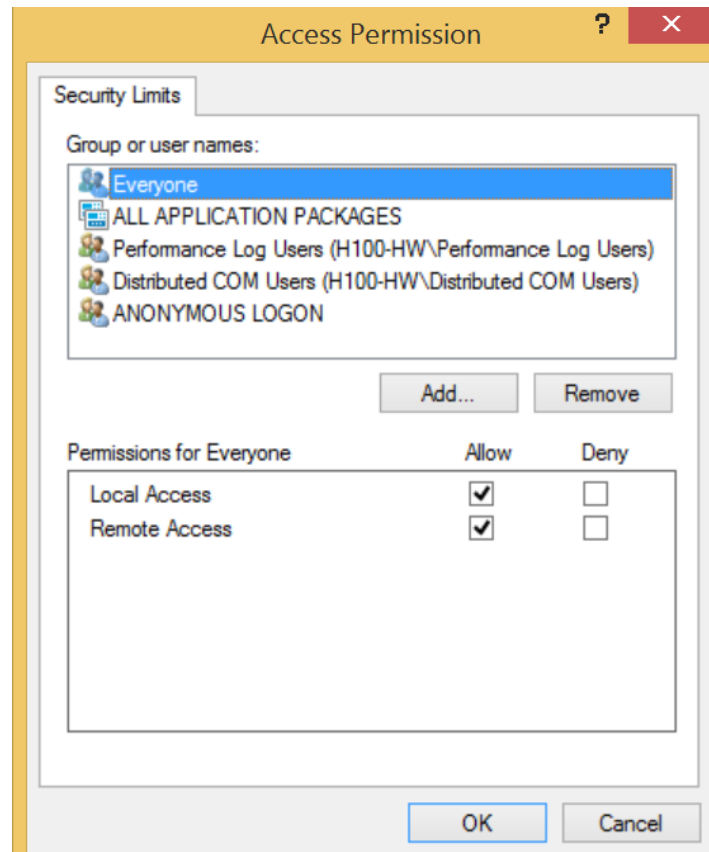
Step 4. Open “My Computer Properties”



Step 5. Go to “COM Security” tab



Step 6. Enter “Access Permissions” by clicking “Edit Limits”, and set “Local Activation” and “Local Launch” to Allow for “Everyone”.

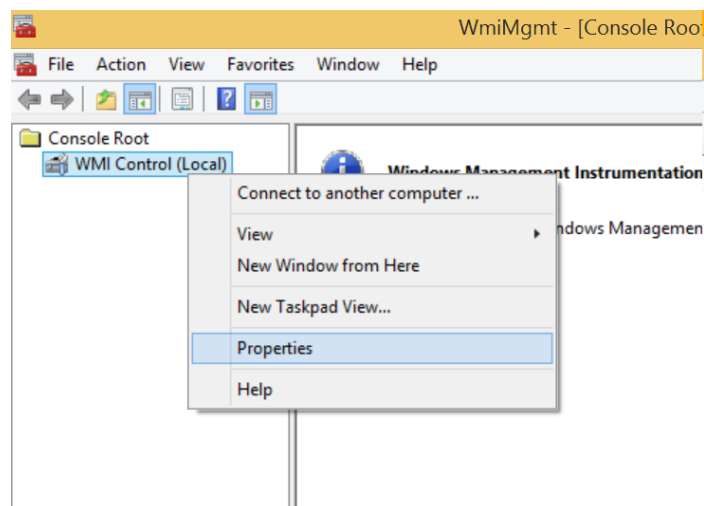


E.2. WMI permissions

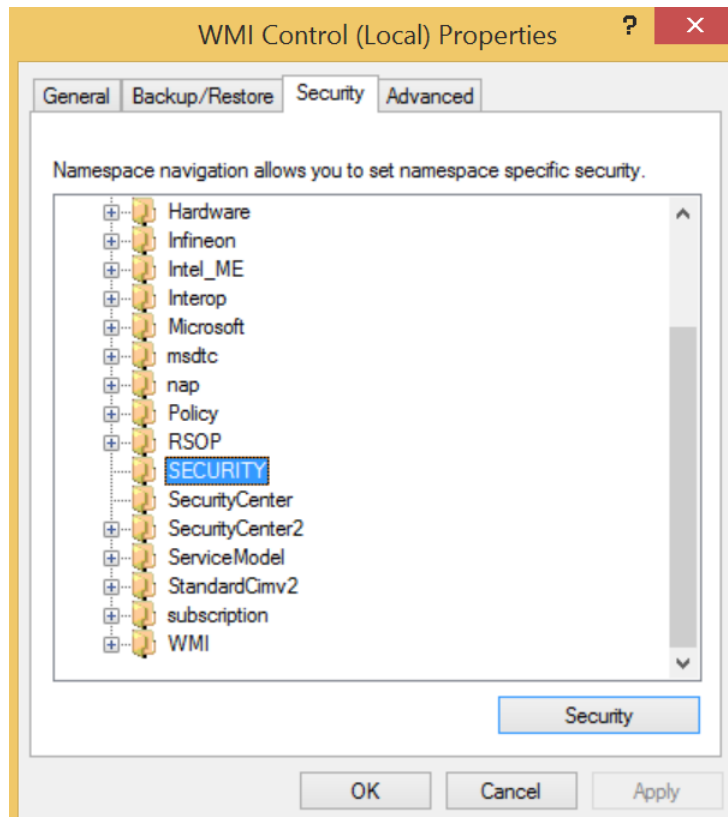
Step 1. Search -> **“WMIgmt.msc”**

Step 2. Run **“WMIgmt.msc”**

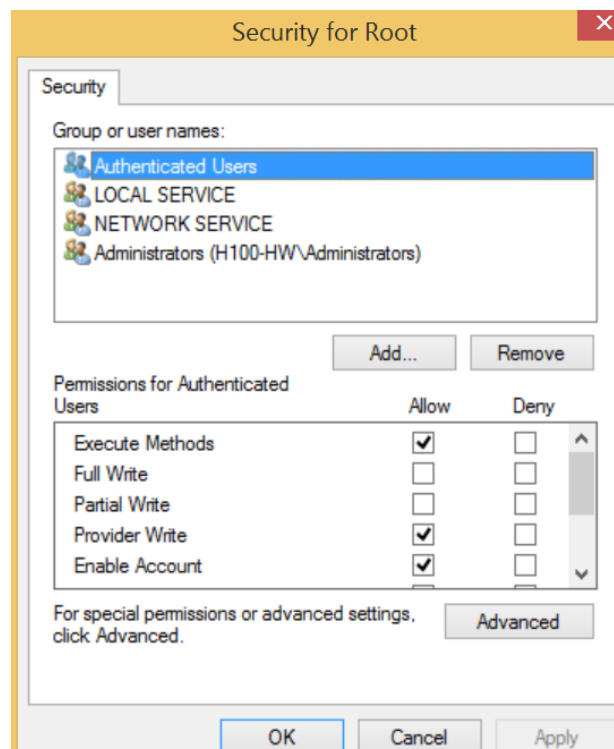
Step 3. Right click on WMI Control and open **“Properties”**



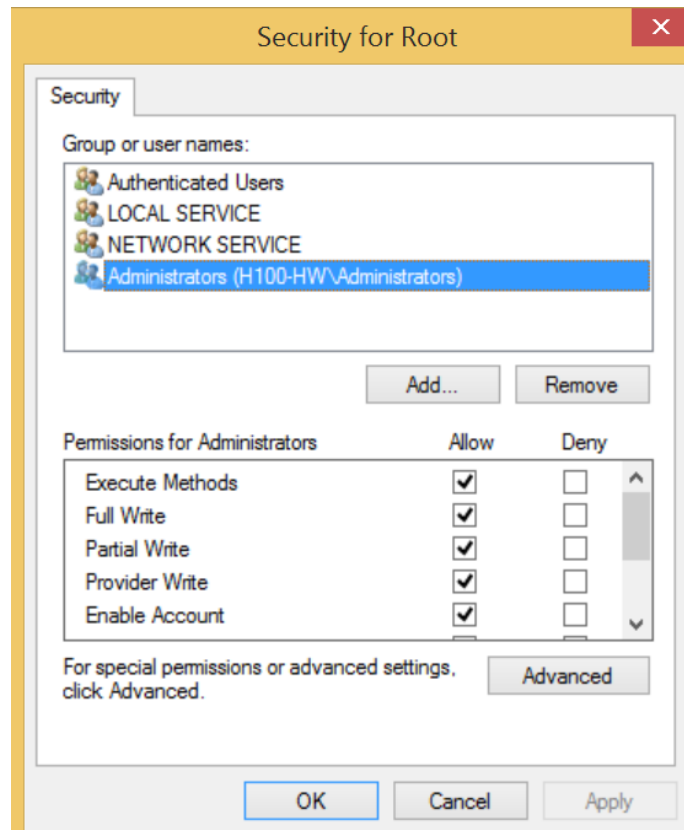
Step 4. Select **“Security”** tab in WMI Control Properties and open **“SECURITY”**



Step 5. Ensure “Execute Methods”, “Provider Write” and “Enable Account” are set to Allow in Permission for Authenticated Users



Step 6. Ensure all permissions are set to Allow in Permissions for Administrators

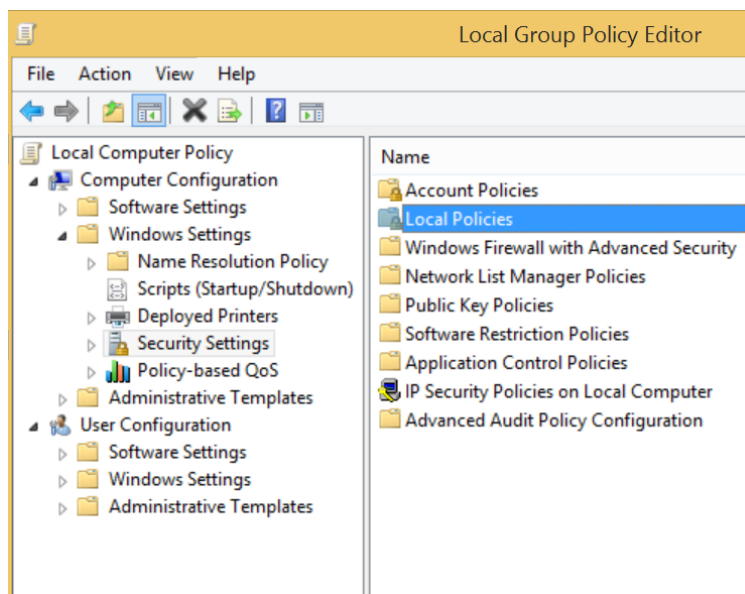


E.3. WMI impersonation Rights

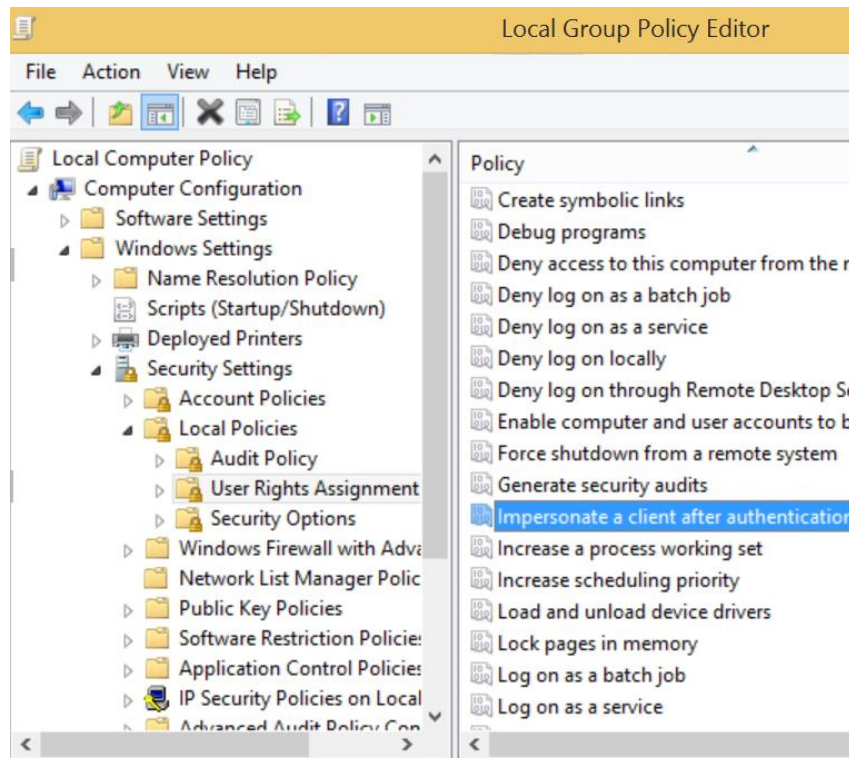
Step 1. Search -> **“gpedit.msc”**

Step 2. Run **“gpedit.msc”**

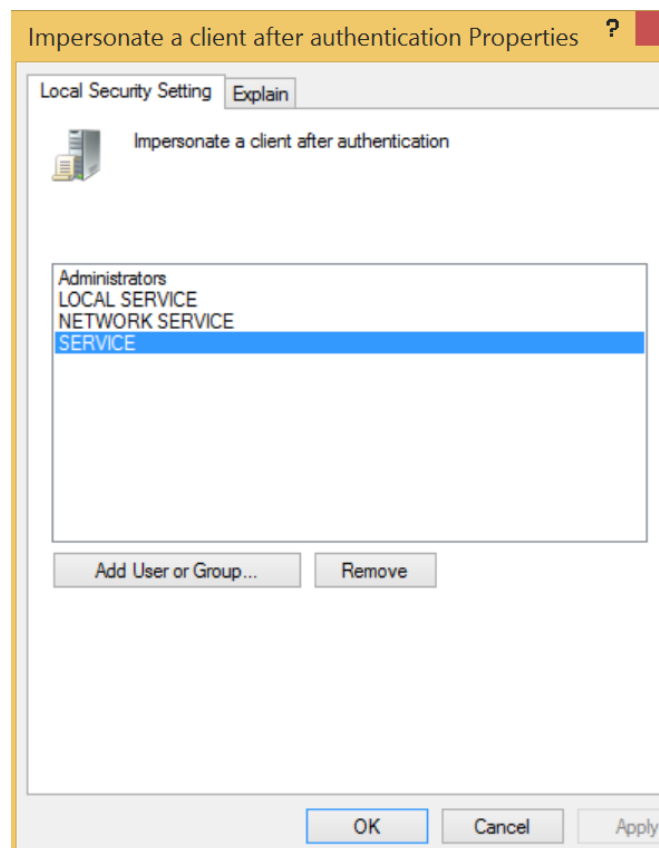
Step 3. Open **“Local Policies”** from **“Security Settings”** in **“Windows Settings”**



Step 4. Open **“Impersonate a client after authentication”** from **“User Rights Assignment”** in **“Local Policies”**.



Step 5. Verify “SERVICE” is granted for “Impersonate a client after authentication” in “Local Security Setting”

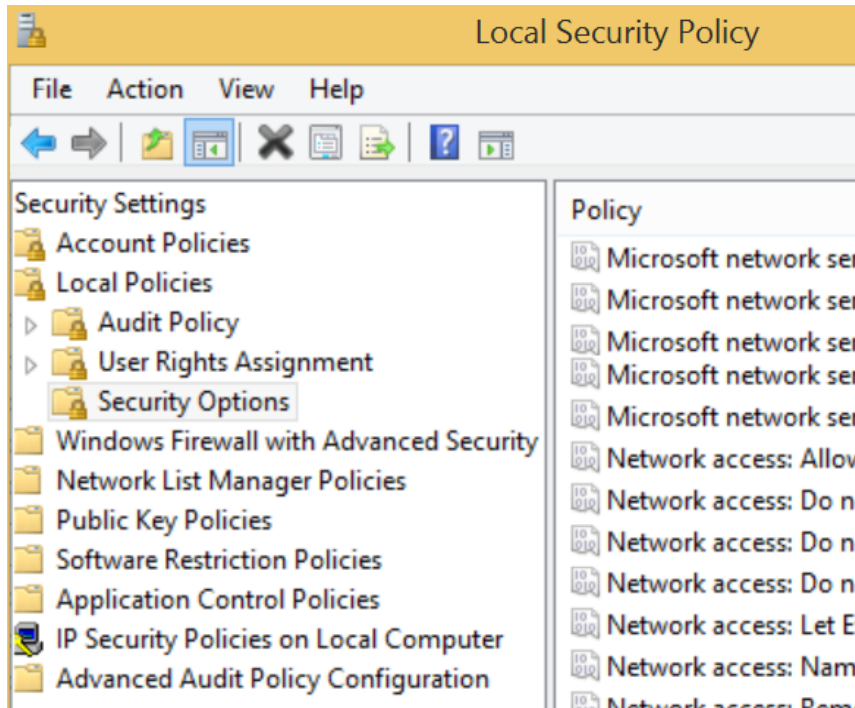


E.4. Network Access

Step 1. Search -> “secpol.msc”

Step 2. Run “secpol.msc”

Step 3. Open “Security Options” from “Local Policies” in “Security Settings”



Step 4. Check that the Security Setting of “Network Access: Sharing and security model for local accounts” is set to “Classic”.

