



Getac BIOS Configuration with Windows Management Instrumentation for Tiger Lake Platform

Rev 1.00B

JULY 16, 2021

Revision History

Rev	Date	Description
R1.00	2020/10/08	First version
R1.00A	2021/06/08	- Add Product K120G2 - Modify TPMSetupMenu
R1.00B	2021/07/16	- Add Product F110G6
R1.01	2021/11/24	- Modify system policy - Modify F110G6 Device configuration

Table of Contents

Revision History	2
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	8
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.....	14
Appendix B.VB Script to set the supervisor password.....	16
Appendix C.VB Script to Query the OS Select	17
Appendix D.Check Procedure for Remote Access	18
E.1. DCOM permissions	18
E.2. WMI permissions	19
E.3. WMI impersonation Rights	21

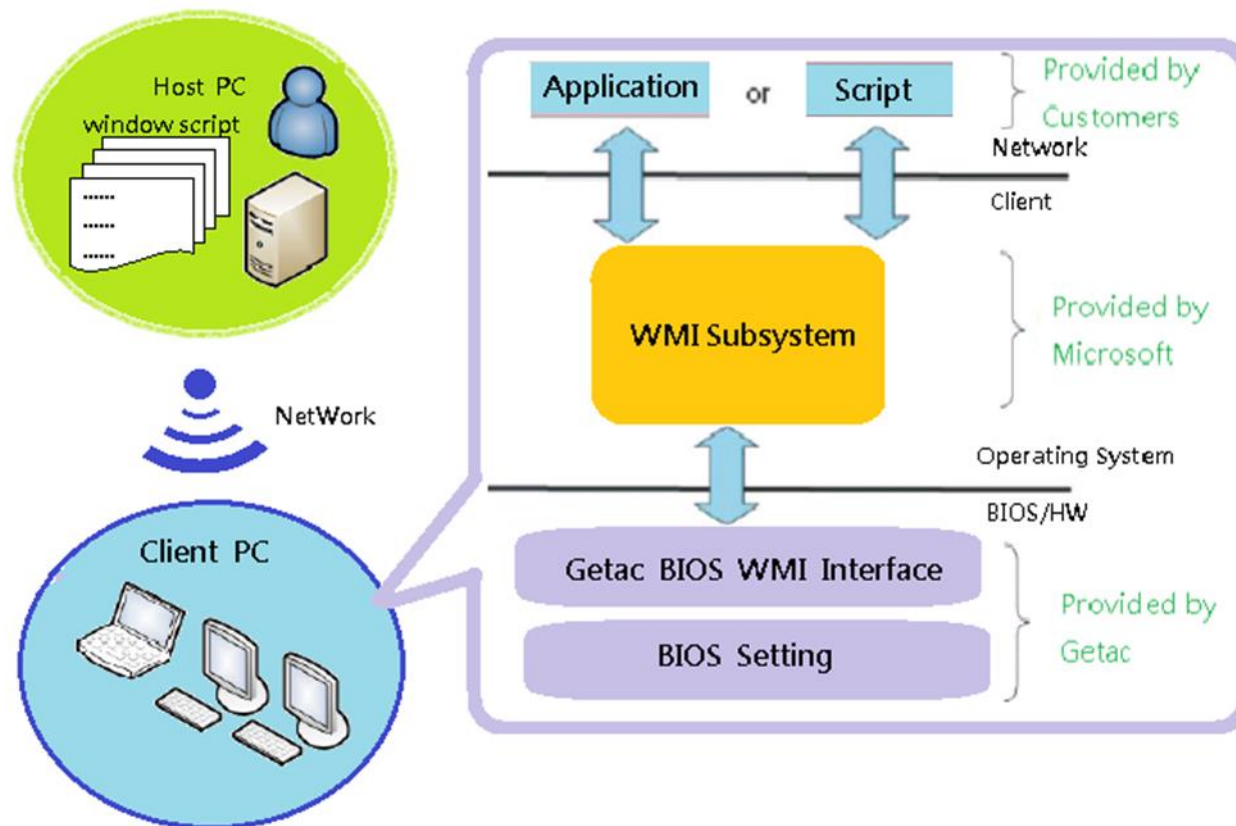
E.4. Network Access	23
---------------------------	----

Chapter 1.Introduction

This chapter will introduce the Getac WMI that will provide users the overview.

1.1. Overview

The most of Windows® operating systems provide Windows Management Instrumentation (WMI). Getac BIOS WMI interface can receive the instruction from Operating system and access the BIOS settings. IT administrator can query and set all the BIOS settings (except read only item), recover the BIOS to factory settings, set and change passwords, and modify the boot order in the remote PCs.



1.2. Disclaimer

BIOS setting are related to the WMI instruction and 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, describes details of how to operate the Getac WMI Interface to access the BIOS settings in remote PCs.

2.1. Configure the BIOS Settings

The following interface accesses the Getac BIOS settings.

Namespace: “\root\WMI”

2.2. Query BIOS User Password Status

User can check if the password is registered by 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

To set Password include Supervisor password and User password by this class. If user wants to set user password, the supervisor password must set before. If the supervisor password is clean, the user password will be clean at the same time.

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	SUIPW	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, maximum length of password is **10**, except models support "StrongPassword" the maximum length of password can be up to **64** and the minimum length of password is **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

As the BIOS security, users must switch to the BIOS configure mode before access the Getac WMI Interface. If Getac WMI interface receives wrong Supervisor password 3 times, Getac WMI interface will lock itself for security. If the Getac WMI interface is locked, any access will return "Locked". Users can entry BIOS setup utility to unlock.

Class name/Method name: Set_GetacBIOSConfigMode

Type: Method

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

Item table:

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

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

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

[2.4.1.Load the default BIOS settings](#)

This class name can recover the 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 the “load default” is requested.

[2.4.2.Query/Change the Getac BIOS Settings](#)

This section contains details on the WMI implementation for Query/Change the 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	Def.
Information	Virtual MAC Address (*Note1)	VirtualMAC	R	XX-XX-XX-XX-XX-XX	
Main	Internal Numlock	InternalNumlock	R/W	"Disabled","Enabled"	Y
	WMI Version	WMIVersion	R	"0.00"- "9.99"	Y
Advanced	Wake Up Capability	HomeButtonWakeup	R/W	"Disabled", "Enabled"	Y
	Power Button Delay	PowerButtonDelay	R/W	"NoDelay", "1sec", "2sec"	Y
	AC Initiation	ACInitiation	R/W	"Disabled", "Enabled"	Y
	Magnetic Sensor	MagneticSensor	R/W	"Enabled", "Disabled"	Y
	USB Power-off Charging	USBPowerOffCharging	R/W	"Disabled", "Enabled"	Y
	Screen Tapping for Boot Options	ScreenTappingforBootOp	R/W	"Disabled", "Enabled"	Y
	MAC Address Pass Through	MACAddressPassThrough	R/W	"Disabled", "Enabled"	Y
	Active Management Tech. Support (*Note2)	IntelAMTSupport	R/W	"Disabled", "Enabled"	Y
		IntelAMTSetupPrompt	R/W	"Disabled", "Enabled"	Y
		IntelAMTUSBProvision	R/W	"Disabled", "Enabled"	Y
	Virtualization Tech.	IntelVT	R/W	"Disabled", "Enabled"	Y
		VTd	R/W	"Disabled", "Enabled"	Y
	Device Configuration	WirelessLAN	R/W	"Disabled", "Enabled"	Y
		WWAN	R/W	"Disabled", "Enabled"	Y
		Bluetooth	R/W	"Disabled", "Enabled"	Y
		MediaCardReader	R/W	"Disabled", "Enabled"	Y
		SmartCardReader	R/W	"Disabled", "Enabled"	Y

Page	Item	WMI Item/ Return Item	Attr.	Return/AcceptValues	Def.
		RFID	R/W	"Disabled", "Enabled"	Y
		FingerprintScanner	R/W	"Disabled", "Enabled"	Y
		FrontWebcam	R/W	"Disabled", "Enabled"	Y
		RearCamera	R/W	"Disabled", "Enabled"	Y
		BarcodePM	R/W	"PowerSaving", "QuickStart"	Y
		Thunderbolt	R/W	"Disabled", "Enabled"	Y
		SystemUSBPort	R/W	"Disabled", "Enabled"	Y
		DockingUSBPortSetting	R/W	"USB2.0", "USB3.0"	Y
		InternalMicrophone	R/W	"Disabled", "Enabled"	Y
		InternalSpeaker	R/W	"Disabled", "Enabled"	Y
Security	Password on Boot	PasswordonBoot	R/W	"Disabled", "Enabled"	Y
	StrongPassword	StrongPassword	R/W	"Disabled", "Enabled"	Y
	PasswordConfig	PasswordConfig	R/W	"04"-"64"	Y
	Secure Boot Configuration (*Note2)	SecureBoot	R/W	"Disabled", "Enabled"	Y
	Security Freeze Lock	SecurityFreezeLock	R/W	"Disabled", "Enabled"	Y
	Intel Trusted Execution Technology (*Note2) (*Note5)	IntelTrustedExeTech	R/W	"Disabled", "Enabled"	Y
Boot	Boot Type Order (*Note6)	BootTypeOrder	R/W	"HardDisk", "USBDisk", "Network", "USB CD", "CDROM"	Y

Page	Item	WMI Item/ Return Item	Attr.	Return/AcceptValues	Def.
	Boot Device	HardDiskDrive	R/W	"Off", "On"	Y
		USBDrive	R/W	"Off", "On"	Y
		USBDDVDDrive	R/W	"Off", "On"	Y
		NetworkDrive	R/W	"Off", "On"	Y
		DDVDDrive	R/W	"Off", "On"	Y

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

*Note2 : Only AMT SKU systems are supported.

Note6 :

"BootTypeOrder" Individual model return/accept values case	
S410G4	Others
"HardDisk", "USBDrive", "Network", "USBCD", "CDROM"	"HardDisk", "USBDrive", "Network", "USBCD"

Appendix A-1.Models Mapping Table

Page	Item	WMI Item/ Return Item	Attr.	S410 G4	K120 G2	F110 G6						
Information	Virtual MAC Address	VirtualMAC	R	X	X	O						
Main	Internal Numlock	InternalNumlock	R/W	O	O	X						
	WMI Version	WMIVersion	R	O	O	O						
	WakeUp Capability	HomeButtonWakeup	R/W	X	O	O						
	Power Button Delay	PowerButtonDelay	R/W	O	O	O						
	AC Initiation	ACInitiation	R/W	O	O	O						
	Magnetic Sensor	MagneticSensor	R/W	O	O	O						
	USB Power-off Charging	USBPowerOffCharging	R/W	O	O	X						
	Screen Tapping for Boot Options	ScreenTappingforBootOp	R/W	X	O	O						
	MAC Address Pass Through	MACAddressPassThrough	R/W	O	O	O						
	Active Management Tech. Support	IntelAMTSupport	R/W	O	O	O						
		IntelAMTSetupPrompt	R/W	O	O	O						
		IntelAMTUSBProvision	R/W	O	O	O						
	Virtualization Tech. Setup	IntelVT	R/W	O	O	O						
		VTd	R/W	O	O	O						
	Device Configuration	WirelessLAN	R/W	O	O	O						
		WWAN	R/W	O	O	O						
		Bluetooth	R/W	O	O	O						
		MediaCardReader	R/W	O	O	O						
		SmartCardReader	R/W	O	O	O						
		RFID	R/W	X	O	O						
		FingerprintScanner	R/W	O	O	O						
		FrontWebcam	R/W	O	O	O						
		RearCamera	R/W	X	O	O						

Page	Item	WMI Item/ Return Item	Attr.	S410 G4	K120 G2	F110 G6						
		BarcodePM	R/W	O	O	O						
		Thunderbolt	R/W	O	O	O						
		SystemUSBPort	R/W	O	O	O						
		DockingUSBPortSetting	R/W	O	O	O						
		InternalMicrophone	R/W	O	O	O						
		InternalSpeaker	R/W	O	O	O						
Security	Password on Boot	PasswordonBoot	R/W	O	O	O						
	StrongPassword	StrongPassword	R/W	O	O	O						
	PasswordConfig	PasswordConfig	R/W	O	O	O						
	Secure Boot Configuration	SecureBoot	R/W	O	O	O						
	SecurityFreezeLock	SecurityFreezeLock	R/W	O	X	X						
	Intel Trusted Execution Technology	IntelTrustedExeTech	R/W	O	O	O						
Boot	Boot Type Order	BootTypeOrder	R/W	O	O	O						
	Boot Device	HardDiskDrive	R/W	O	O	O						
		USBDrive	R/W	O	O	O						
		USBCDDVDDrive	R/W	O	O	O						
		NetworkDrive	R/W	O	O	O						
		CDDVDDrive	R/W	O	X	X						

Appendix B.VB Script to set the supervisor password

User can set the supervisor password by 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") = "SUVPW,,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

User can query the OS select by 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.
' TheOutParameters object in objOutParams is created by the provider.
'-----

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

'-----
' ListOutParams
'-----

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

Appendix D.Check Procedure for Remote Access

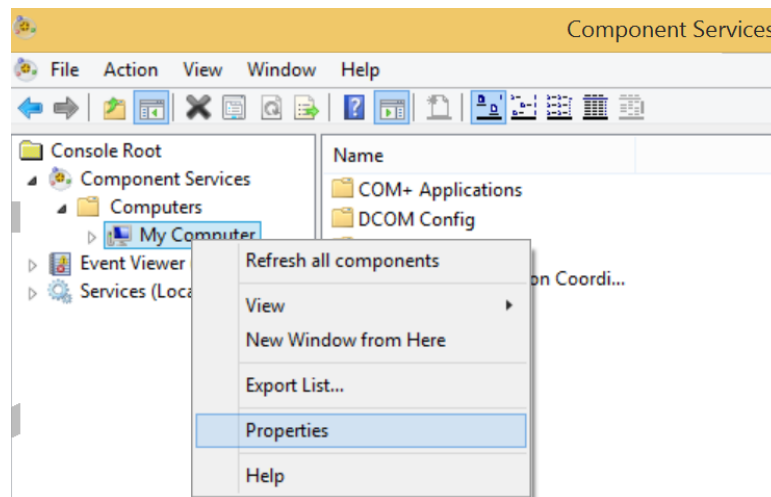
E.1. DCOM permissions

Step 1. Search->**Dcomcnfg**

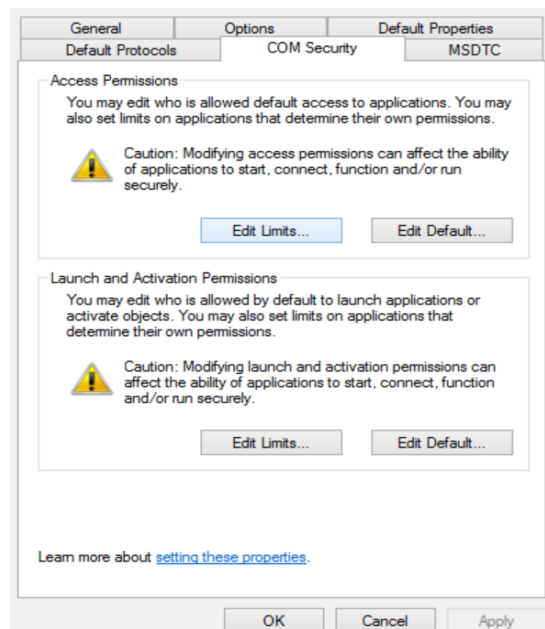
Step 2. Run **Dcomcnfg**

Step 3. Expand **Component Services** ->**Computers** ->**My computer**

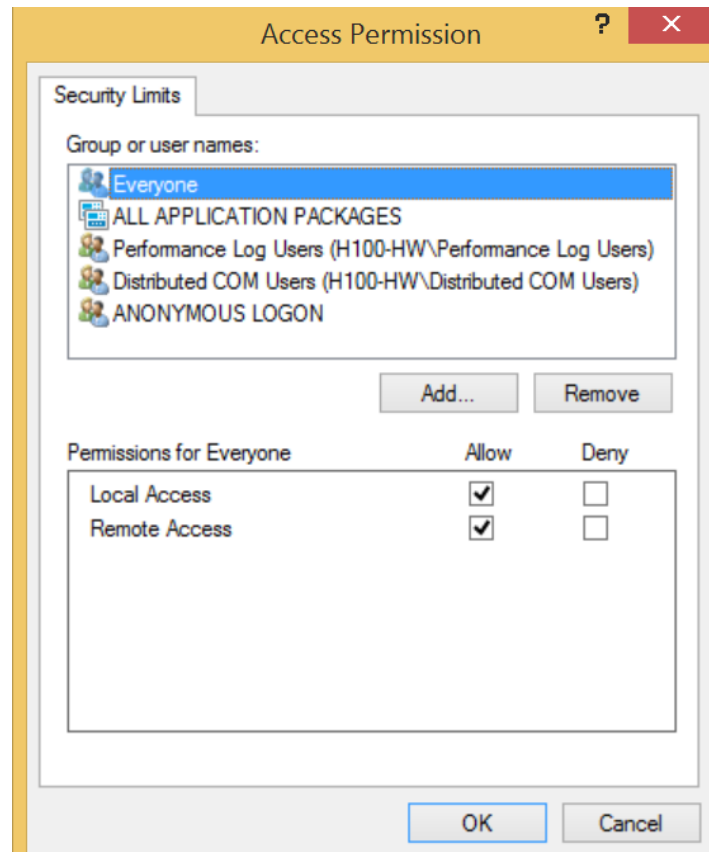
Step 4. Open **My Computer Properties**



Step 5. Go to **COM Security** page.



Step 6. Entry Access Permissions by click **Edit Limits**, and ensure **Everyone** has the **Local Activation** and **Local Launch** allow.

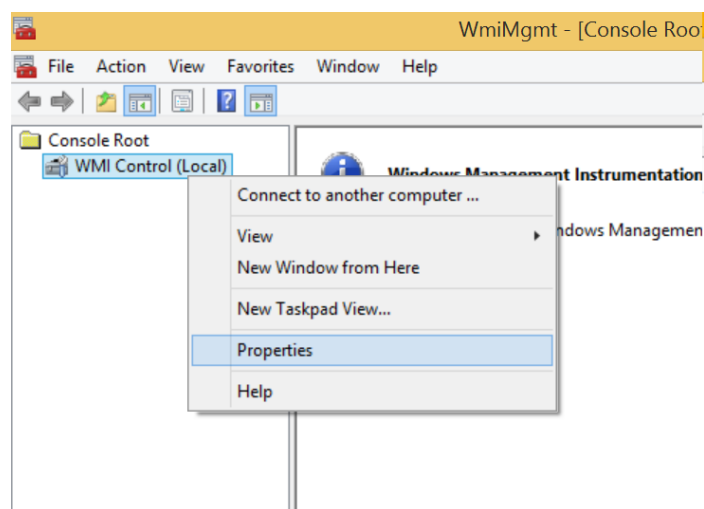


E.2. WMI permissions

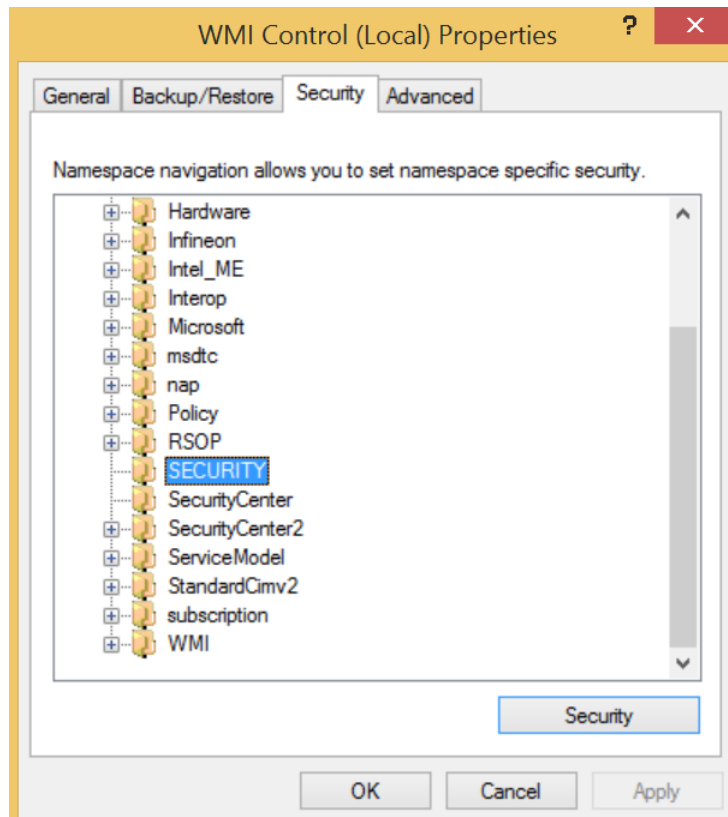
Step 1. Search->[WMIimgmt.msc](#)

Step 2. Run [WMIimgmt.msc](#)

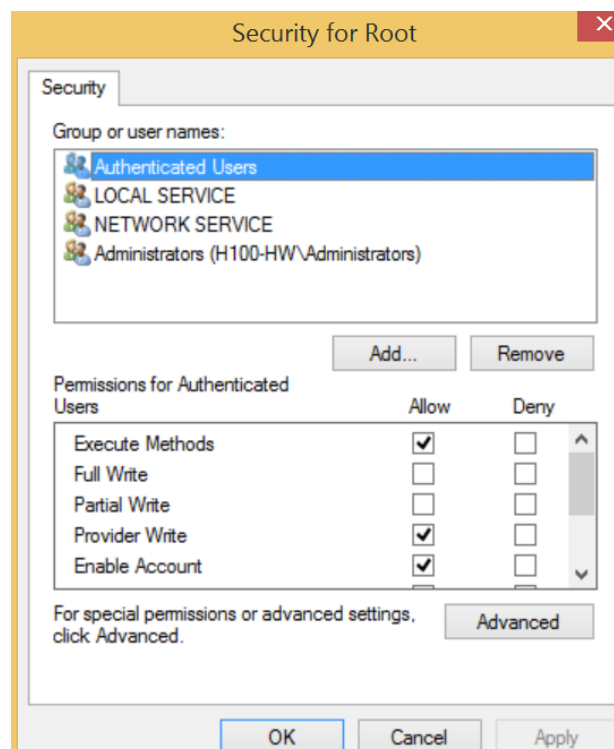
Step 3. Open the [Properties](#) of WMI control



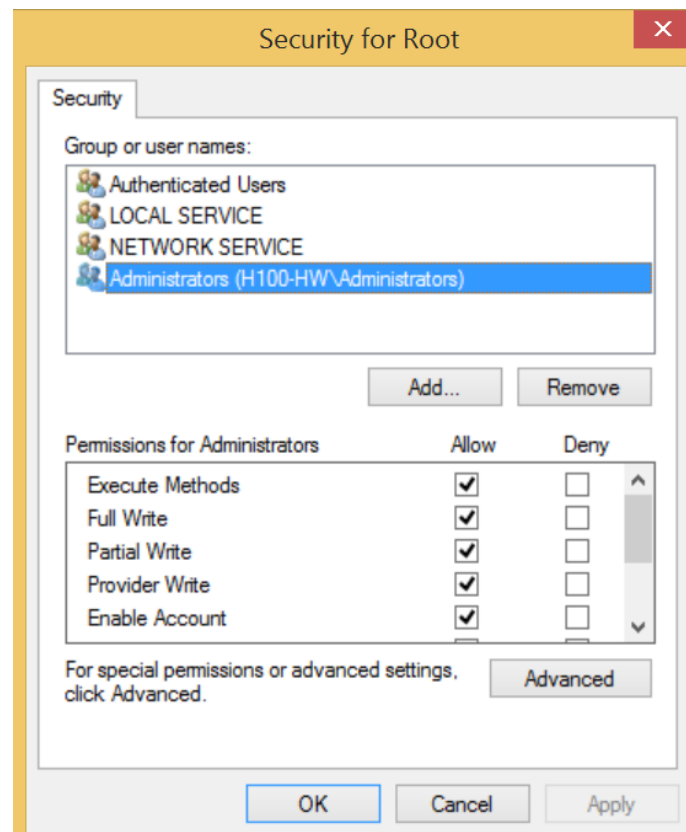
Step 4. Open SECURITY in [Security](#) page of [WMI Control Properties](#)



Step 5. Ensure the **Execute Methods**, **Provider Write** and **Enable Account** enabled in **Permission for Authenticated Users**.



Step 6. Ensure all permissions enabled in [Permissions for Administrators](#).

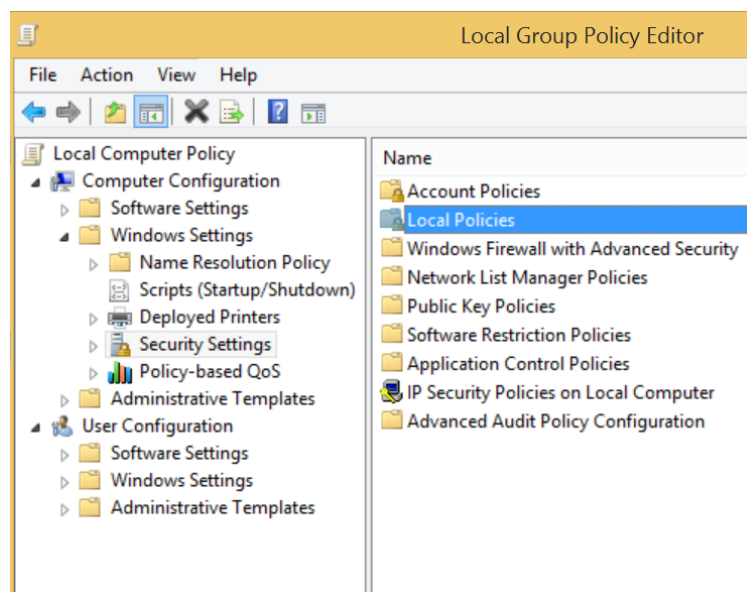


E.3. WMI impersonation Rights

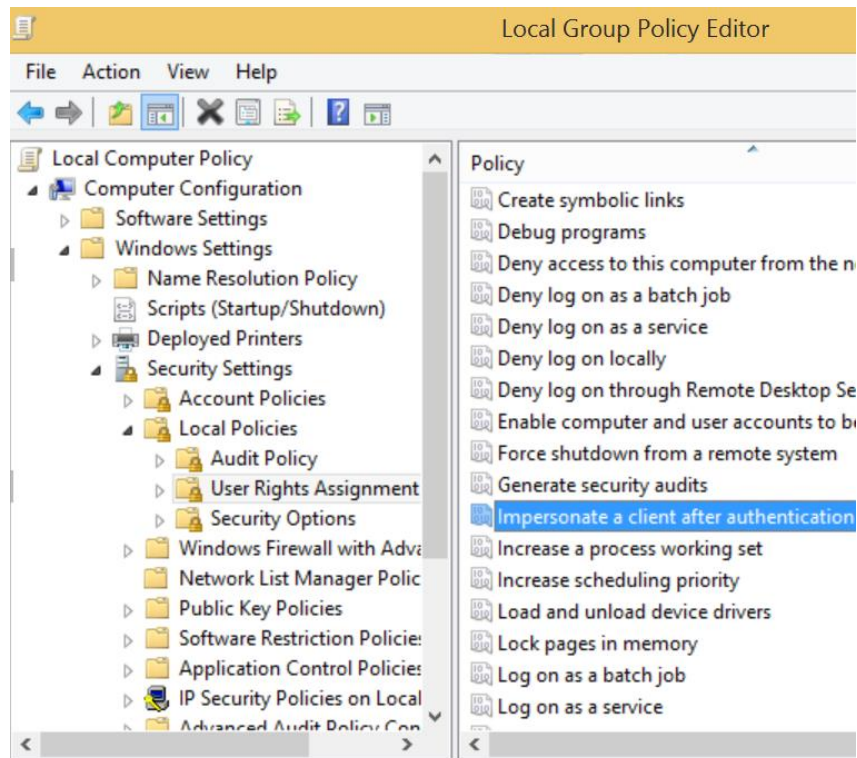
Step 1. Search->[gpedit.msc](#)

Step 2. Run [gpedit.msc](#)

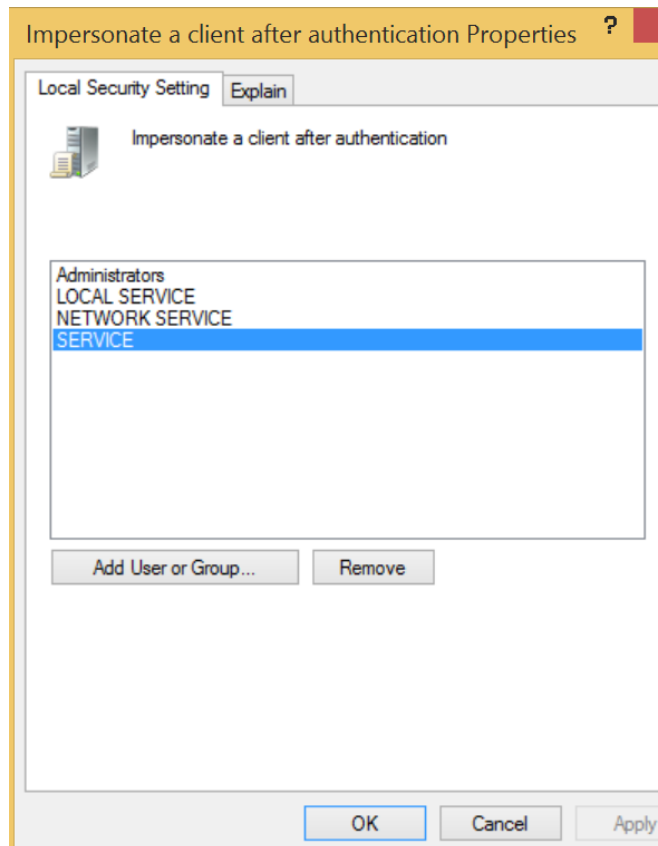
Step 3. Click the [Local Policies](#) of [Security Settings](#) in [windows Settings](#)



Step 4. Open the **Impersonate a client after authentication** in **User Rights Assignment of Local Policies**.



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

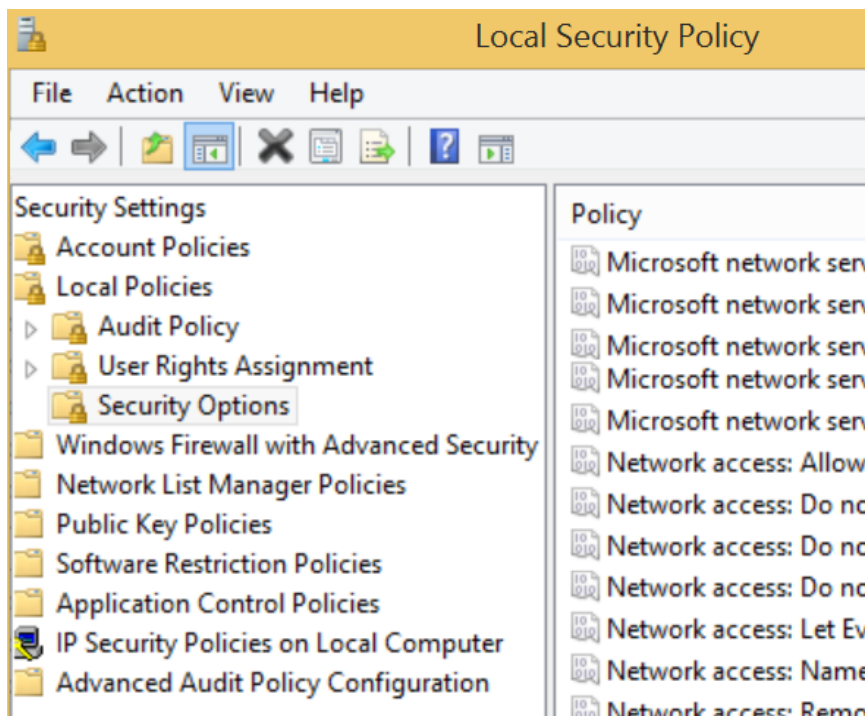


E.4. Network Access

Step 1. Search->[secpol.msc](#)

Step 2. Run [secpol.msc](#)

Step 3. Click the [Security Options](#) of [Local Policies](#) in [Security Settings](#)



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

