Getac

Getac BIOS Configuration with Windows Management Instrumentation for AlderLake Platform

Rev 1.02

May 27, 2024

Revision History

Rev	Date	Description
R1.00	2022/12/30	First version
R1.01	2023/03/20	Add LoadMSFTUEFICA item.
R1.02	2024/05/27	Change Asset Tag field to Advanced page. Revised wording and format for p5~9, 12, 15~23

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 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

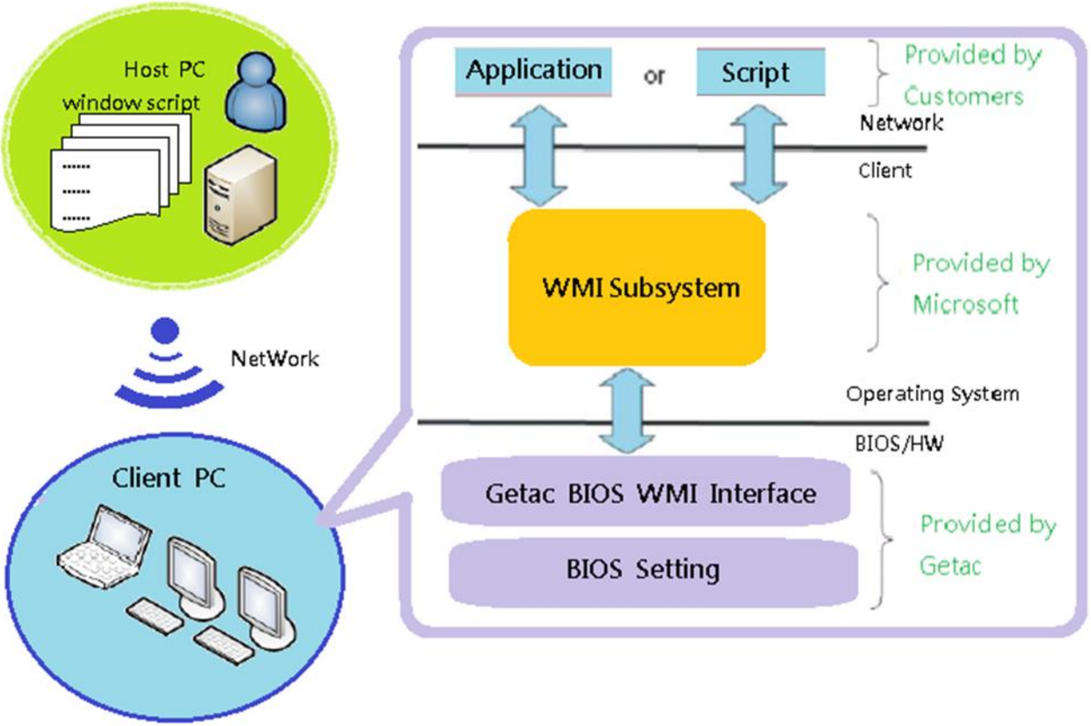
E.4. Network Access 22

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). 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 settings 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, 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: “SUVPW”
Item table:

Page	Item	WMI Item	Attr.
Security	Set Supervisor password	**SUVPW**	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: “SUVPW,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	Def.
Information	Virtual MAC Address **(*Note1)**	**VirtualMAC**	R	**XX-XX-XX-XX-XX-XX**	
	EC Version	**ECVersion**	R	**R1.00.070520**	
Main	Internal Numlock	**InternalNumlock**	R/W	**“Disabled”,”Enabled”**	Y
	FN and Ctrl Key Placement	**FNCtrlKeyPlacement**	R/W	**“CtrlFN”,” FNCtrl”**	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

Page	Item	WMI Item/ Return Item	Attr.	Return/AcceptValues	Def.
		Bluetooth	R/W	**“Disabled”, ”Enabled”**	Y
		MediaCardReader	R/W	**“Disabled”, ”Enabled”**	Y
		SmartCardReader	R/W	**“Disabled”, ”Enabled”**	Y
		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
	Asset Tag	**AssetTag**	R/W	**32 characters maximum**	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 **(*Note3)**	**LoadMSFTUEFICA**	R/W	**“Disabled”, ”Enabled”**	Y
	Security Freeze Lock	**SecurityFreezeLock**	R/W	**“Disabled”, ”Enabled”**	Y
	Intel Trusted Execution Technology **(*Note2)**	**IntelTrustedExeTech**	R/W	**“Disabled”, ”Enabled”**	Y
Boot	Boot Type Order **(*Note6)**	**BootTypeOrder**	R/W	**“HardDisk”,**	Y

Page	Item	WMI Item/ Return Item	Attr.	Return/AcceptValues	Def.
				”USBDisk”, “Network”, “USBCD”, ”CDROM”	
	Boot Device	**HardDiskDrive**	R/W	**“Off”, ”On”**	Y
		USBDiskDrive	R/W	**“Off”, ”On”**	Y
		USBCDDVDDrive	R/W	**“Off”, ”On”**	Y
		NetworkDrive	R/W	**“Off”, ”On”**	Y
		CDDVDDrive	R/W	**“Off”, ”On”**	Y
	Fast Boot	**FastBoot**	R/W	**“Disabled”, ”Enabled”**	Y
	Alternative WBM option	**AlternativeWBM**	R/W	**“Disabled”, ”Enabled”**	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.

*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	
B360G2	**Others**
“HardDisk”, “USBDisk”, “Network”, “USBCD”, “CDROM”	**“HardDisk”, “USBDisk”, “Network”, “USBCD”**

O = Support
X = Not Support

Appendix A-1.Models Mapping Table

Page	Item	WMI Item/ Return Item	Attr.	B360 G2	UX10 G3	V110 G7						
Information	Virtual MAC Address	**VirtualMAC**	R	X	O	X						
	EC Version	**ECVersion**	R	O	O	O						
Main	Internal Numlock	**InternalNumlock**	R/W	O	X	O						
	FN and Ctrl Key Placement	**FNCtrlKeyPlacement**	R/W	O	O	O						
	WMI Version	**WMIVersion**	R	O	O	O						
	WakeUp Capability	**HomeButtonWakeup**	R/W	X	O	X						
	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	X	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	O	O	O						

Page	Item	WMI Item/ Return Item	Attr.	B360 G2	UX10 G3	V110 G7						
		FingerprintScanner	R/W	O	O	O						
		FrontWebcam	R/W	O	O	O						
		RearCamera	R/W	X	O	O						
		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						
	Asset Tag	**AssetTag**	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	**LoadMSFTUEFICA**	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						
		USBDiskDrive	R/W	O	O	O						
		USBCDDVDDrive	R/W	O	O	O						
		NetworkDrive	R/W	O	O	O						
		CDDVDDrive	R/W	O	X	X						
	Fast Boot	**FastBoot**	R/W	O	O	O						
	Alternative WBM option	**AlternativeWBM**	R/W	O	O	O						

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 objOutParamsis 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 specificto 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

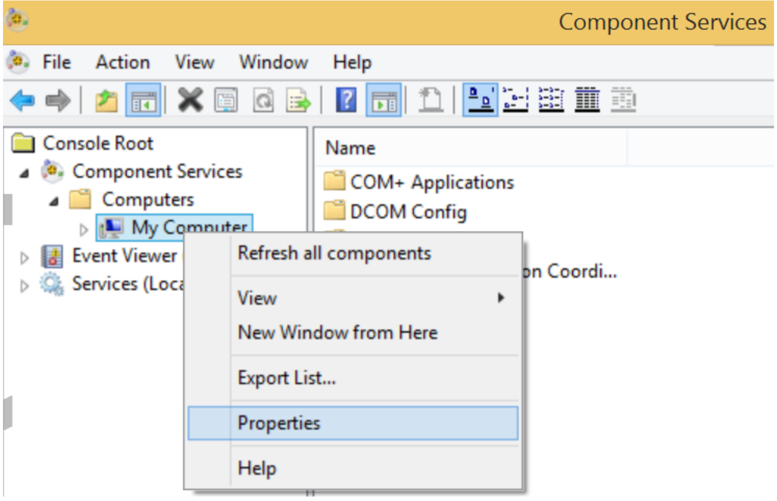
E.1. DCOM permissions

Step 1. Search -> **“Dcomcnfg”**

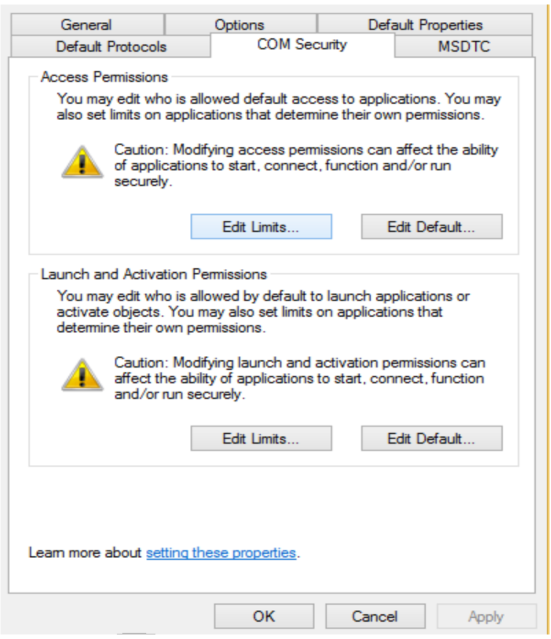
Step 2. Run **“Dcomcnfg”**

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

Step 4. Open **“My Computer Properties”**



Step 5. Go to “**COM Security”** tab



Access Permissions

You may edit who is allowed default access to applications. You may also set limits on applications that determine their own permissions.

Caution: Modifying access permissions can affect the ability of applications to start, connect, function and/or run securely.

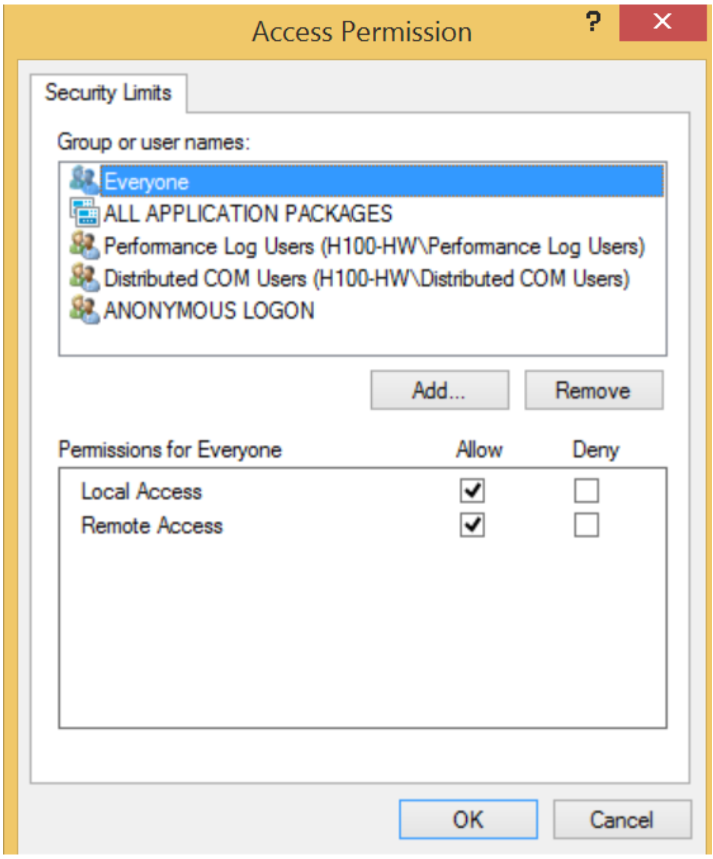
Launch and Activation Permissions

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.

Learn more about setting these properties.

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



Access Permission

Security Limits

Group or user names:

- Everyone
- ALL APPLICATION PACKAGES
- Performance Log Users (H100-HW\Performance Log Users)
- Distributed COM Users (H100-HW\Distributed COM Users)
- ANONYMOUS LOGON

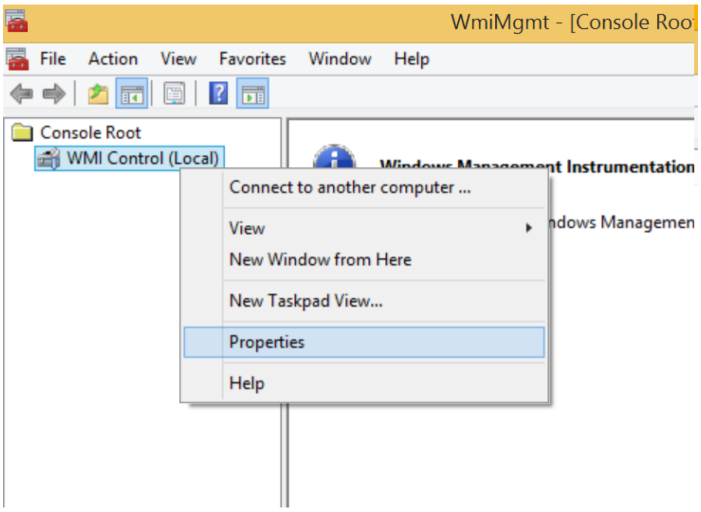
Permissions for Everyone	Allow	Deny
Local Access	☑	□
Remote Access	☑	□

E.2. WMI permissions

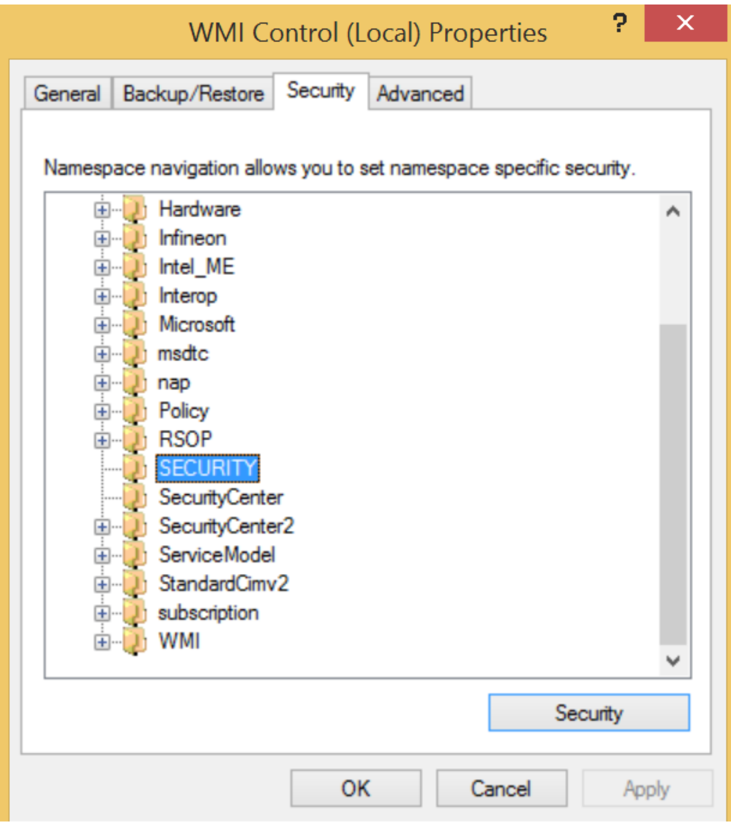
Step 1. Search -> **"WMImgmt.msc"**

Step 2. Run **"WMImgmt.msc"**

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



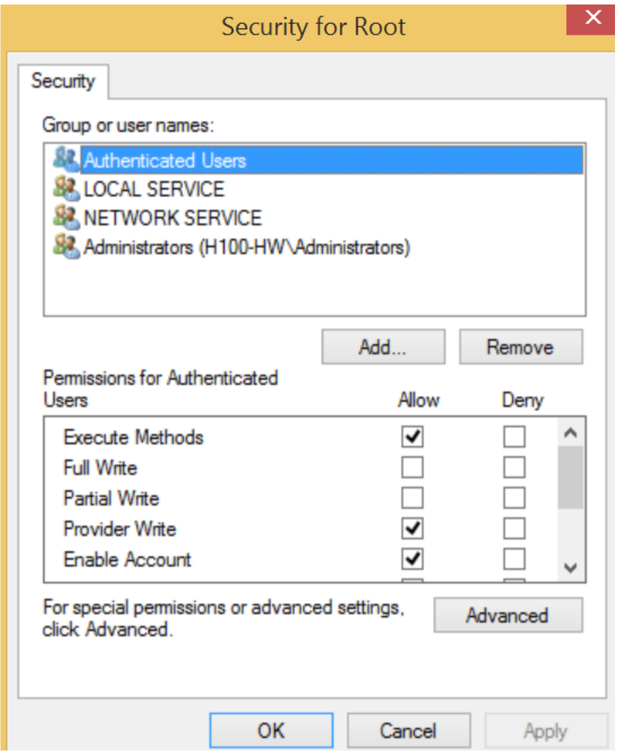
Step 4. Select **"Security"** tab in WMI Control Properties and open **"SECURITY"**


WMI Control (Local) Properties

Namespace navigation allows you to set namespace specific security.

- Hardware
- Infineon
- Intel_ME
- Interop
- Microsoft
- msdtc
- nap
- Policy
- RSOP
- SECURITY
- SecurityCenter
- SecurityCenter2
- ServiceModel
- StandardCimv2
- subscription
- WMI

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


Security for Root

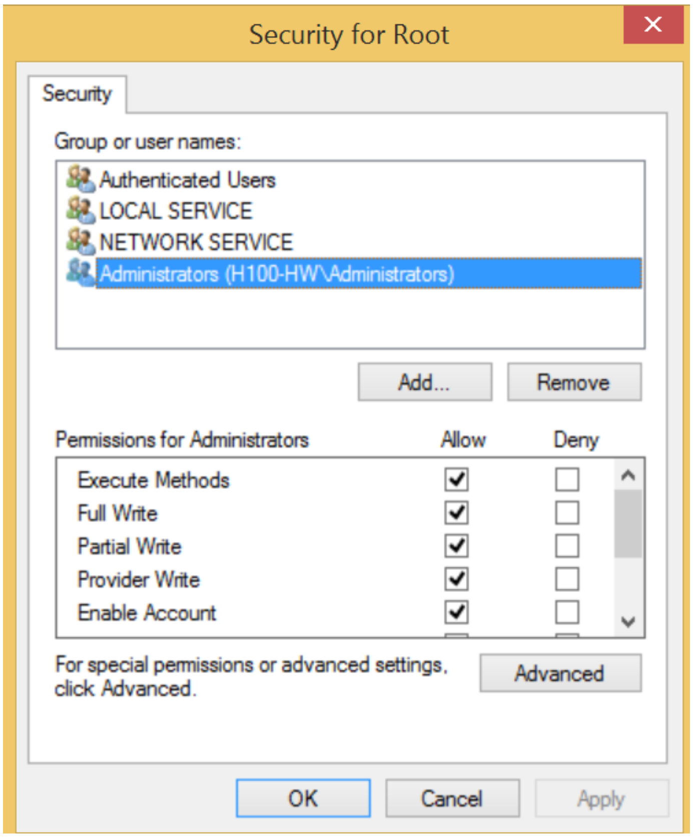
Group or user names:

- Authenticated Users
- LOCAL SERVICE
- NETWORK SERVICE
- Administrators (H100-HW\Administrators)

Permissions for Authenticated Users	Allow	Deny
Execute Methods	☑	□
Full Write	□	□
Partial Write	□	□
Provider Write	☑	□
Enable Account	☑	□

For special permissions or advanced settings, click Advanced.

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



Group or user names:

- Authenticated Users
- LOCAL SERVICE
- NETWORK SERVICE
- Administrators (H100-HW\Administrators)

Permissions for Administrators	Allow	Deny
Execute Methods	☑	□
Full Write	☑	□
Partial Write	☑	□
Provider Write	☑	□
Enable Account	☑	□

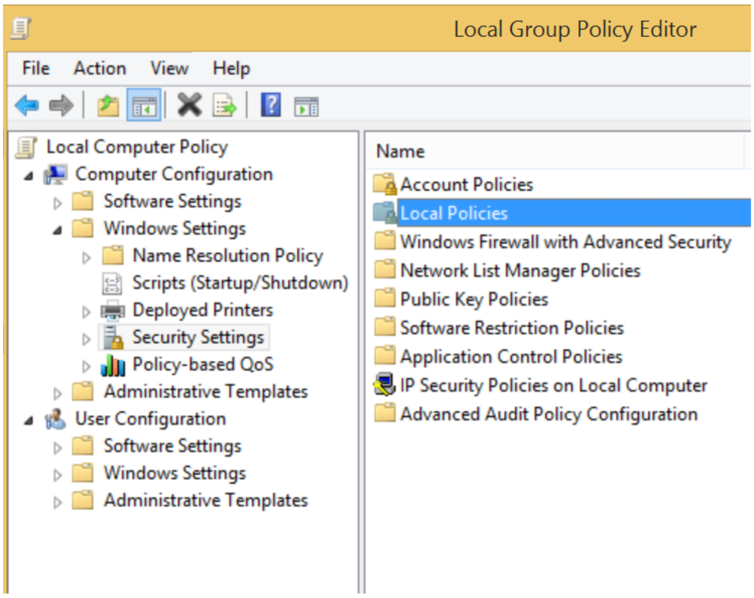
For special permissions or advanced settings, click Advanced.

E.3. WMI impersonation Rights

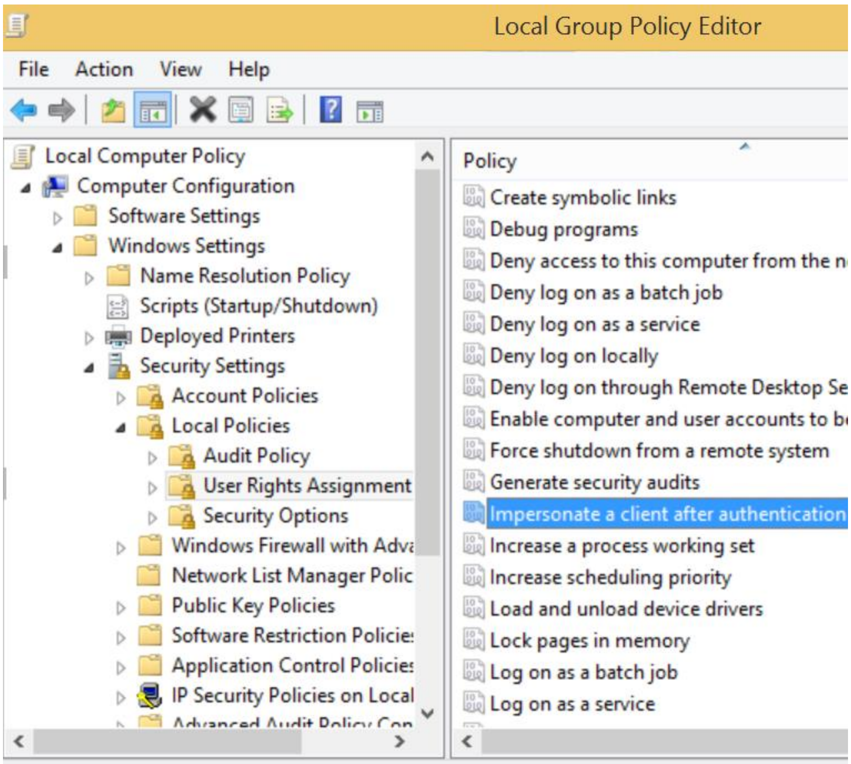
Step 1. Search -> **“gpedit.msc”**

Step 2. Run **“gpedit.msc”**

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



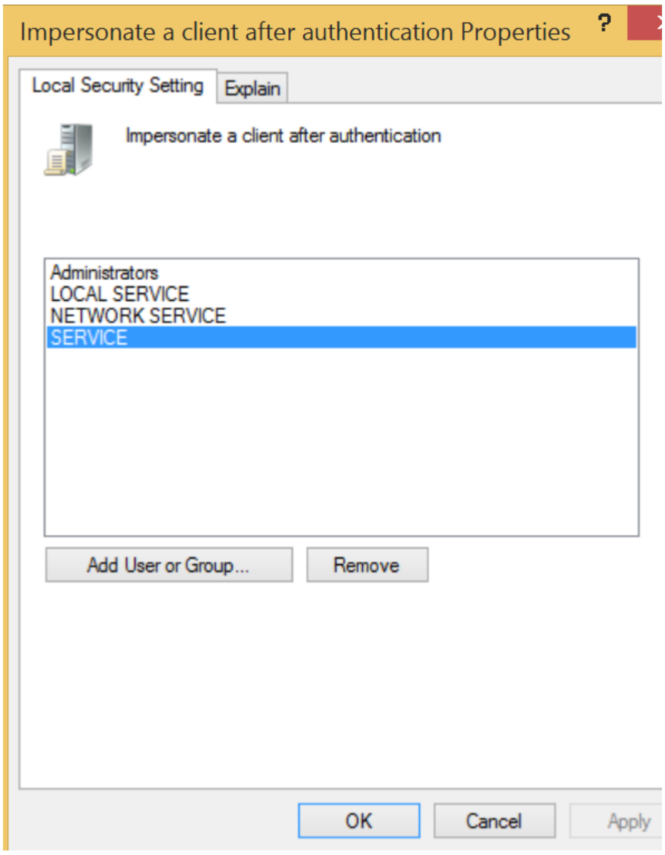
Step 4. Open **“Impersonate a client after authentication”** from **“User Rights Assignment”** in **“Local Policies”**.



Local Computer Policy
- Computer Configuration
  - Software Settings
  - Windows Settings
    - Name Resolution Policy
    - Scripts (Startup/Shutdown)
    - Deployed Printers
    - Security Settings
      - Account Policies
      - Local Policies
        - Audit Policy
        - User Rights Assignment
        - Security Options
      - Windows Firewall with Adva
      - Network List Manager Polic
      - Public Key Policies
      - Software Restriction Policie
      - Application Control Policies
      - IP Security Policies on Local
      - Advanced Audit Policy Con

Policy
- Create symbolic links
- Debug programs
- Deny access to this computer from the n
- Deny log on as a batch job
- Deny log on as a service
- Deny log on locally
- Deny log on through Remote Desktop Se
- Enable computer and user accounts to b
- Force shutdown from a remote system
- Generate security audits
- Impersonate a client after authentication
- Increase a process working set
- Increase scheduling priority
- Load and unload device drivers
- Lock pages in memory
- Log on as a batch job
- Log on as a service

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



Impersonate a client after authentication

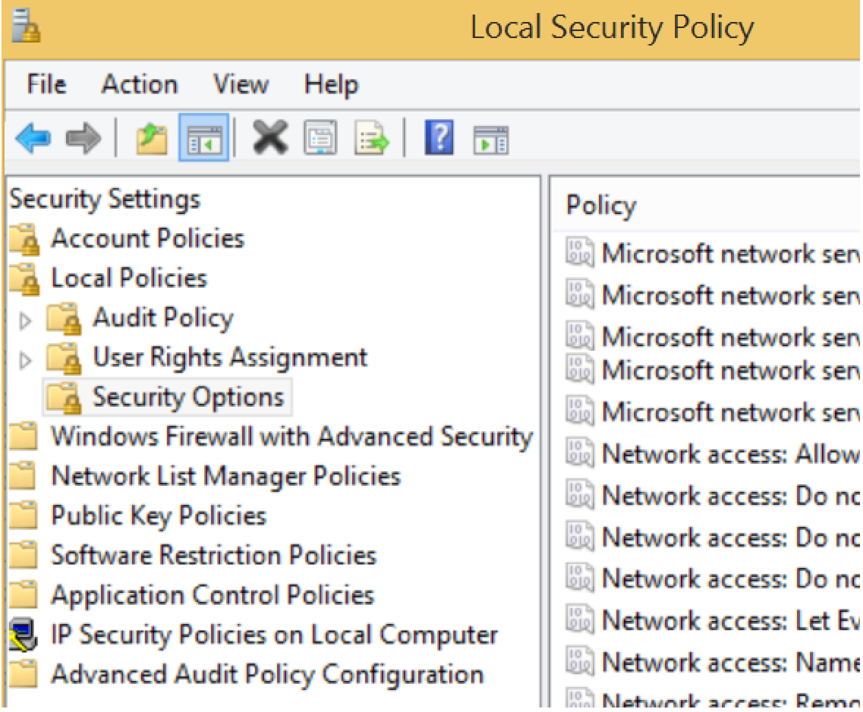
Administrators
LOCAL SERVICE
NETWORK SERVICE
SERVICE

E.4. Network Access

Step 1. Search -> **“secpol.msc”**

Step 2. Run **“secpol.msc”**

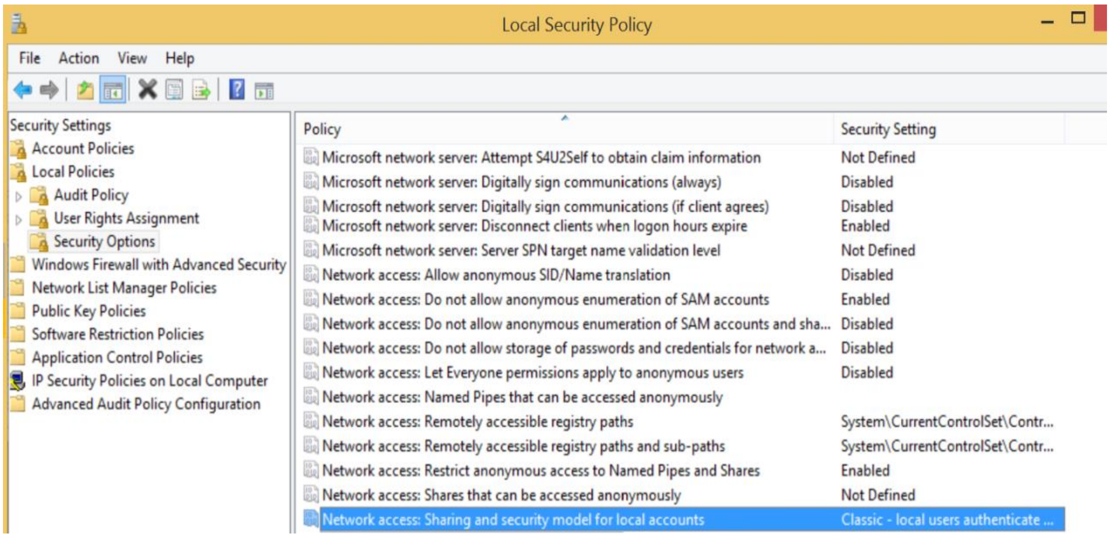
Step 3. Open **“Security Options”** from **“Local Policies”** in **“Security Settings”**



- Security Settings
  - Account Policies
  - Local Policies
    - Audit Policy
    - User Rights Assignment
    - Security Options
  - Windows Firewall with Advanced Security
  - Network List Manager Policies
  - Public Key Policies
  - Software Restriction Policies
  - Application Control Policies
  - IP Security Policies on Local Computer
  - Advanced Audit Policy Configuration

Policy
Microsoft network serv
Microsoft network serv
Microsoft network serv
Microsoft network serv
Microsoft network serv
Network access: Allow
Network access: Do nc
Network access: Do nc
Network access: Do nc
Network access: Let Ev
Network access: Name
Network access: Remo

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



- Security Settings
  - Account Policies
  - Local Policies
    - Audit Policy
    - User Rights Assignment
    - Security Options
  - Windows Firewall with Advanced Security
  - Network List Manager Policies
  - Public Key Policies
  - Software Restriction Policies
  - Application Control Policies
  - IP Security Policies on Local Computer
  - Advanced Audit Policy Configuration

Policy	Security Setting
Microsoft network server: Attempt S4U2Self to obtain claim information	Not Defined
Microsoft network server: Digitally sign communications (always)	Disabled
Microsoft network server: Digitally sign communications (if client agrees)	Disabled
Microsoft network server: Disconnect clients when logon hours expire	Enabled
Microsoft network server: Server SPN target name validation level	Not Defined
Network access: Allow anonymous SID/Name translation	Disabled
Network access: Do not allow anonymous enumeration of SAM accounts	Enabled
Network access: Do not allow anonymous enumeration of SAM accounts and sha...	Disabled
Network access: Do not allow storage of passwords and credentials for network a...	Disabled
Network access: Let Everyone permissions apply to anonymous users	Disabled
Network access: Named Pipes that can be accessed anonymously	
Network access: Remotely accessible registry paths	System\CurrentControlSet\Contr...
Network access: Remotely accessible registry paths and sub-paths	System\CurrentControlSet\Contr...
Network access: Restrict anonymous access to Named Pipes and Shares	Enabled
Network access: Shares that can be accessed anonymously	Not Defined
Network access: Sharing and security model for local accounts	Classic - local users authenticate ...