Getac

Getac BIOS Configuration with Windows Management Instrumentation for Comet Lake Platform

Rev 1.03

Apr 23, 2024

Revision History

Rev	Date	Description
R1.00	2019/10/22	Cometlake platform first release for B360 projects
	2020/06/01	Modify format for B360 and other projects formal release
R1.01	2020/09/26	Add UX10G2 and V110G6 Models Mapping Table
R1.02	2022/08/09	Add FN and Ctrl Key Placement item.
R1.03	2024/04/23	Add “IntergratedWebcam” and “Bottomcamera” items for UX10G2, A140G2 and V110G6. Revised wording and format for p5, 7~9, 13, 18~26

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 15

Appendix B.VB Script to set the supervisor password 18

Appendix C.VB Script to Query the OS Select 19

Appendix D.VB Script to enable the TPMSupport. 20

Appendix E.Check Procedure for Remote Access 21

E.1. DCOM permissions 21

E.2. WMI permissions 22

E.3. WMI impersonation Rights 24

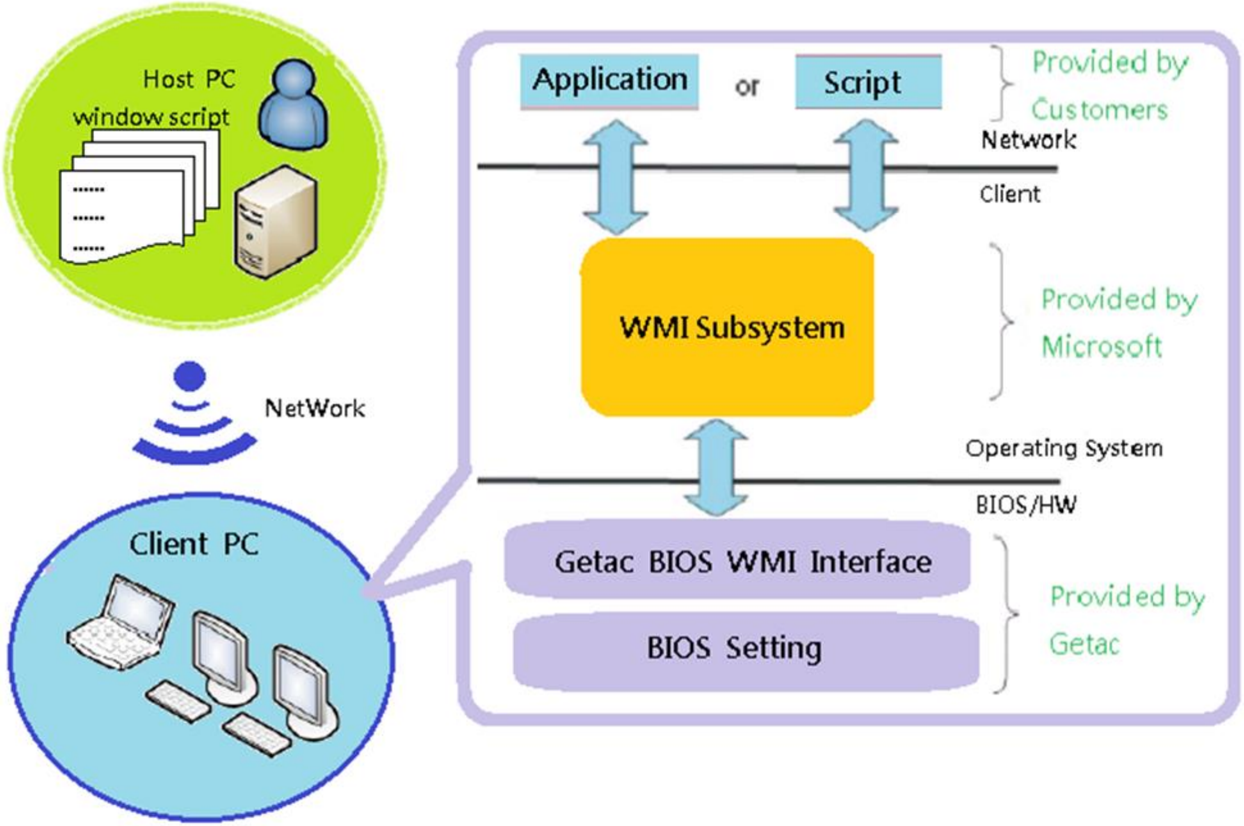
E.4. Network Access 26

Chapter 1.Introduction

This chapter will introduce the Getac WMI and provide users with an 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, 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 is set in this class. If users want to set User Password, the Supervisor Password must be set first. If the Supervisor Password is clean, the User Password will be clean 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, maximum length of a password is **10**, except models supporting “StrongPassword” the maximum length of the password can be up to **64** and the minimum length can be **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.

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

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

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**	
Main	Legacy USB Support	**LegacyUSBSupport**	R/W	**“Disabled”, ”Enabled”**	Y
	CSM Support **(*Note2)**	**CSMSupport**	R/W	**“Off”,”On”**	Y
	PXE Boot **(*Note3)**	**PXEBoot**	R/W	**“UEFI”,”Legacy”**	Y
	Internal Numlock	**InternalNumlock**	R/W	**“Disabled”,”Enabled”**	Y
	FN and Ctrl Key Placement	**FNCtrlKeyPlacement**	R/W	**“CtrlFN”,” FNCtrl”**	Y
	WMI Version	**WMIVersion**	R	**“0000”-“9999”**	Y
	Boot Priority **(*Note3)**	**BootPriority**	R/W	**“UEFI First”, “Legacy First”**	Y
Advanced	Wake Up Capability	**AnyKeyWakeup**	R/W	**“Disabled”, ”Enabled”**	Y
		DKBDWakeupS3	R/W	**“Disabled”, ”Enabled”**	Y
		USBWakeup	R/W	**“Disabled”, ”Enabled”**	Y
	System Policy	**SystemPolicy**	R/W	**“Performance”, ”Balance”**	Y
	AC Initiation	**ACInitiation**	R/W	**“Disabled”, ”Enabled”**	Y
	Magnetic Sensor	**HallSensor**	R/W	**”Enabled”, “Disabled”**	Y
	USB Power-off Charging	**PowerShareUSB**	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

Page	Item	WMI Item/ Return Item	Attr.	Return/AcceptValues	Def.
	Active Management Tech. Support **(*Note4)**	**IntelAMTSupport**	R/W	**“Disabled”, ”Enabled”**	Y
		IntelAMTSetupPrompt	R/W	**“Disabled”, ”Enabled”**	Y
		IntelAMTUSBProvision	R/W	**“Disabled”, ”Enabled”**	Y
	Virtualization Tech. Setup	**IntelVT**	R/W	**“Disabled”, ”Enabled”**	Y
		VTd	R/W	**“Disabled”, ”Enabled”**	Y
		SGX	R/W	**“Disabled”, ”Enabled”** **“Software Controlled”**	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
		RFID	R/W	**“Disabled”, ”Enabled”**	Y
		FingerprintScanner	R/W	**“Disabled”, ”Enabled”**	Y
		IntergratedWebcam	R/W	**“Disabled”, ”Enabled”**	Y
		Bottomcamera	R/W	**“Disabled”, ”Enabled”**	Y
		SystemUSBPort	R/W	**“Disabled”, ”Enabled”**	Y
		DockingUSBPortSetting	R/W	**“USB2.0”, “USB3.0”**	Y
		Microphone	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	**SecurityFreezeLock**	R/W	**“Disabled”, ”Enabled”**	Y

Page	Item	WMI Item/ Return Item	Attr.	Return/AcceptValues	Def.
	Lock				
	TPMSetupMenu **(*Note5)**	**TPMSupport**	R/W	**"Disabled", "Enabled"**	Y
	Intel Trusted Execution Technology **(*Note4) (*Note5)**	**IntelTrustedExeTech**	R/W	**"Disabled", "Enabled"**	Y
Boot	Boot Type Order **(*Note6)**	**BootTypeOrder**	R/W	**"HardDisk", "USBDisk", "Network", "USBCD", "CDROM"**	Y
	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

*note1: **It will return virtual MAC address when there is no physical network card in this system.**

***note2: "CSM Support" can be set only when "Secure Boot "is disabled.**

***note3: The default setting of "PXE Boot"' is "UEFI". And the default setting of "Boot Priority" is "UEFI First"**

"PXE Boot" and "Boot Priority" can be toggled only when "CSM Support" is on.

*note4: **Only AMT SKU systems are supported.**

*note5: **"Intel Trusted Execution Technology "item can be allowed to update only when "TPM Support" is enabled.**
In other cases, "FAIL" is returned as it is not supported.
"TPM Support" item can be updated just when "Intel Trusted Execution Technology" doesn't been enabled.

*note6：

“BootTypeOrder” Individual model return/accept values case	
S410G3/B360	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	A140 G2	UX10 G2	V110 G6				
Information	Virtual MAC Address	**VirtualMAC**	R	X	X	X	X				
Main	Legacy USB Support	**LegacyUSBSupport**	R/W	o	o	o	o				
	CSM Support	**CSMSupport**	R/W	o	o	o	o				
	PXE Boot	**PXEBoot**	R/W	o	o	o	o				
	Internal Numlock	**InternalNumlock**	R/W	o	X	X	o				
	FN and Ctrl Key Placement	**FNCtrlKeyPlacement**	R/W	o	X	o	o				
	WMI Version	**WMIVersion**	R	o	o	o	o				
	Boot Priority	**BootPriority**	R/W	o	o	o	o				
	WakeUp Capability	**AnyKeyWakeup**	R/W	o	X	X	o				
		USBWakeup	R/W	o	o	o	o				
		DKBDWakeupS3	R/W	X	X	X	X				
	System Policy	**SystemPolicy**	R/W	o	o	o	o				
	AC Initiation	**ACInitiation**	R/W	o	o	o	o				
	Magnetic Sensor	**HallSensor**	R/W	o	o	o	o				
	USB Power-off Charging	**PowerShareUSB**	R/W	o	X	X	o				
	Screen Tapping for Boot Options	**ScreenTappingforBootOp**	R/W	X	o	o	o				
	MAC Address Pass Through	**MACAddressPassThroug h**	R/W	o	o	o	o				
	Active Management Tech. Support	**IntelAMTSupport**	R/W	o	o	o	o				
		IntelAMTSetupPrompt	R/W	o	o	o	o				
		IntelAMTUSBProvision	R/W	o	o	o	o				
	Virtualization Tech. Setup	**IntelVT**	R/W	o	o	o	o				
		VTd	R/W	o	o	o	o				
		SGX	R/W	o	o	o	o				

Page	Item	WMI Item/ Return Item	Attr.	B360	A140 G2	UX10 G2	V110 G6				
	Device Configuration	**WirelessLAN**	R/W	○	○	○	o				
		WWAN	R/W	○	○	○	o				
		Bluetooth	R/W	○	○	○	o				
		MediaCardReader	R/W	○	X	X	o				
		SmartCardReader	R/W	○	X	X	x				
		RFID	R/W	X	X	X	x				
		FingerprintScanner	R/W	○	X	X	x				
		IntergratedWebcam	R/W	○	o	o	o				
		Bottomcamera	R/W	X	o	o	o				
		SystemUSBPort	R/W	○	○	○	o				
		DockingUSBPortSetting	R/W	○	○	○	o				
		Microphone	R/W	○	○	○	o				
		InternalSpeaker	R/W	○	○	○	o				
Security	Password on Boot	**PasswordonBoot**	R/W	○	○	○	o				
	StrongPassword	**StrongPassword**	R/W	○	○	○	o				
	PasswordConfig	**PasswordConfig**	R/W	○	○	○	o				
	Secure Boot Configuration	**SecureBoot**	R/W	○	○	○	o				
	SecurityFreezeLoc k	**SecurityFreezeLock**	R/W	○	○	○	o				
	TPMSetupMenu	**TPMSupport**	R/W	○	○	○	o				
	Intel Trusted Execution Technology	**IntelTrustedExeTech**	R/W	○	○	○	o				
Boot	Boot Type Order	**BootTypeOrder**	R/W	○	○	○	○				
	Boot Device	**HardDiskDrive**	R/W	○	○	○	○				
		USBDiskDrive	R/W	○	○	○	○				
		USBCDDVDDrive	R/W	○	○	○	○				
		NetworkDrive	R/W	○	○	○	○				

Page	Item	WMI Item/ Return Item	Attr.	B360	A140 G2	UX10 G2	V110 G6				
		CDDVDDrive	R/W	○	X	X	X				

Appendix B.VB Script to set the supervisor password

Users 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") =    "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

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 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.VB Script to enable the TPMSupport. Enable (TPMSupport)

Users can enable TPMSupport with below VBScript after configure mode set.

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

'------------------------------------------------------------------------------------------------------
'As the BIOS security, users must switch to the BIOS configure mode before access the Getac WMI Interface
'See this Spec 2.4. Switch to the BIOS Configure Mode
'------------------------------------------------------------------------------------------------------
Set objShare =objWMIService.Get("Set_GetacBIOSConfigMode.InstanceName='ACPI\PNP0C14\0_0'")
Set objInParam = objShare.Methods_("Set_GetacBIOSConfigMode").inParameters.SpawnInstance_()
objInParam.Properties_.Item("DataIn") = ",SetStart"
Set objOutParams =
objWMIService.ExecMethod("Set_GetacBIOSConfigMode.InstanceName='ACPI\PNP0C14\0_0'","Set_GetacBIOSConfigM
ode", objInParam)

Wscript.echo "Feature: " &objInParam.Properties_.Item("DataIn")
Wscript.echo "DataOut: " &objOutParams.DataOut

'------------------------------------------------------------------------------------------------------
'Add the input parameters, for this this example "TPMSupport,Enabled"
'------------------------------------------------------------------------------------------------------
Set objShare =objWMIService.Get("Set_GetacBIOSSettings.InstanceName='ACPI\PNP0C14\0_0'")
Set objInParam = objShare.Methods_("Set_GetacBIOSSettings").inParameters.SpawnInstance_()
objInParam.Properties_.Item("DataIn") = "TPMSupport,Enabled"
Set objOutParams =
objWMIService.ExecMethod("Set_GetacBIOSSettings.InstanceName='ACPI\PNP0C14\0_0'","Set_GetacBIOSSettings",
objInParam)

Wscript.echo "Feature: " &objInParam.Properties_.Item("DataIn")
Wscript.echo "DataOut: " &objOutParams.DataOut
```

Appendix E.Check Procedure for Remote Access

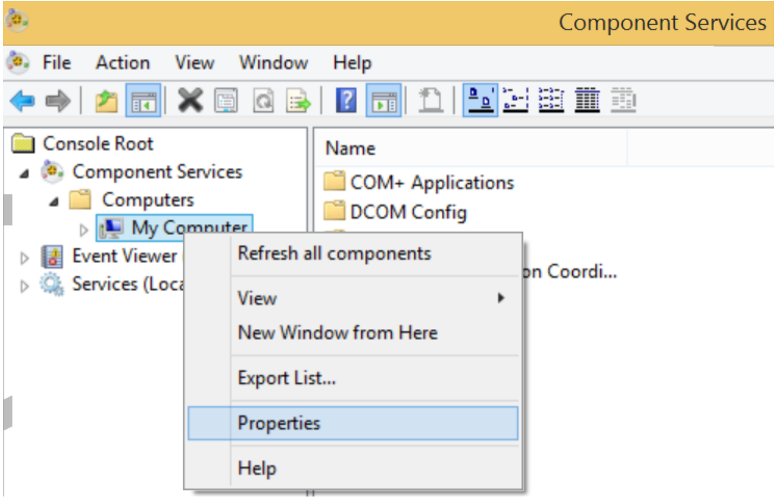
E.1. DCOM permissions

Step 1. Search -> **Dcomcnfg**

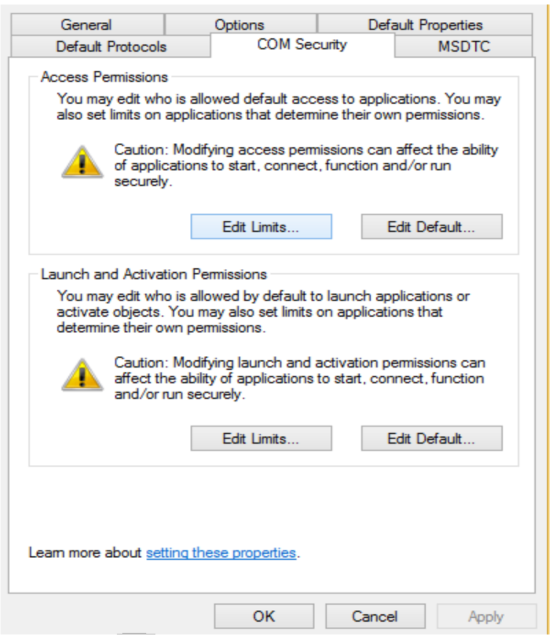
Step 2. Run **“Dcomcnfg”**

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.

Edit Limits... Edit Default...

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.

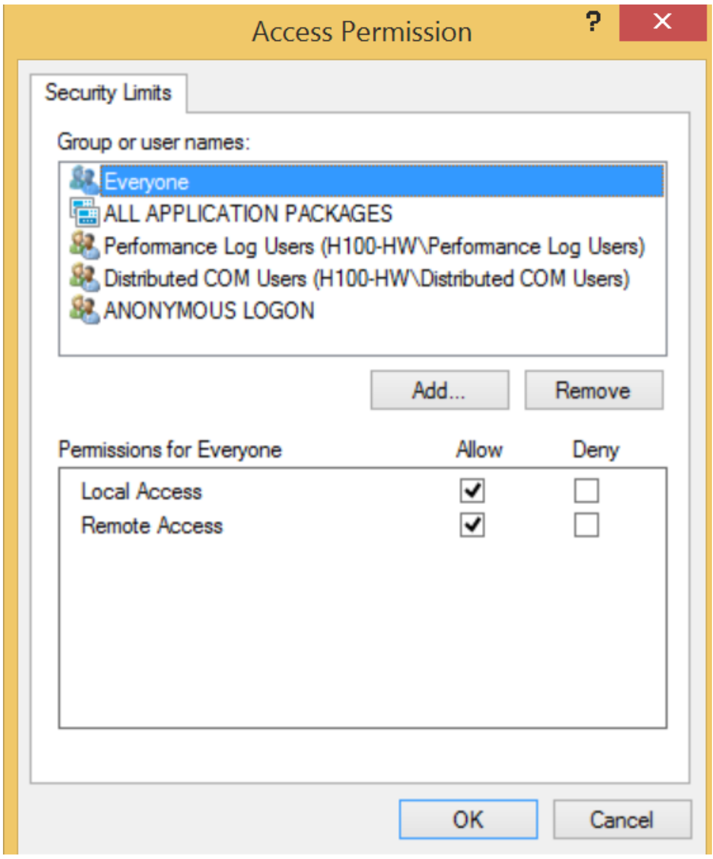
Caution: Modifying launch and activation permissions can affect the ability of applications to start, connect, function and/or run securely.

Edit Limits... Edit Default...

Learn more about setting these properties.

OK Cancel Apply

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



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

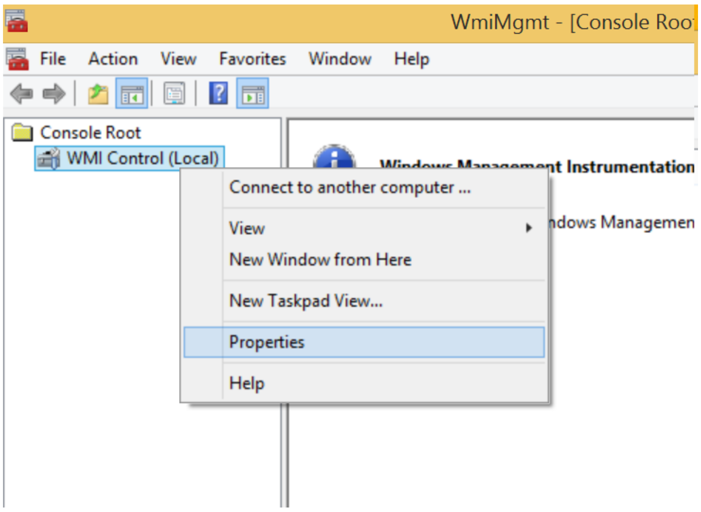
Permissions for Everyone	Allow	Deny
Local Access	☑	□
Remote Access	☑	□

E.2. WMI permissions

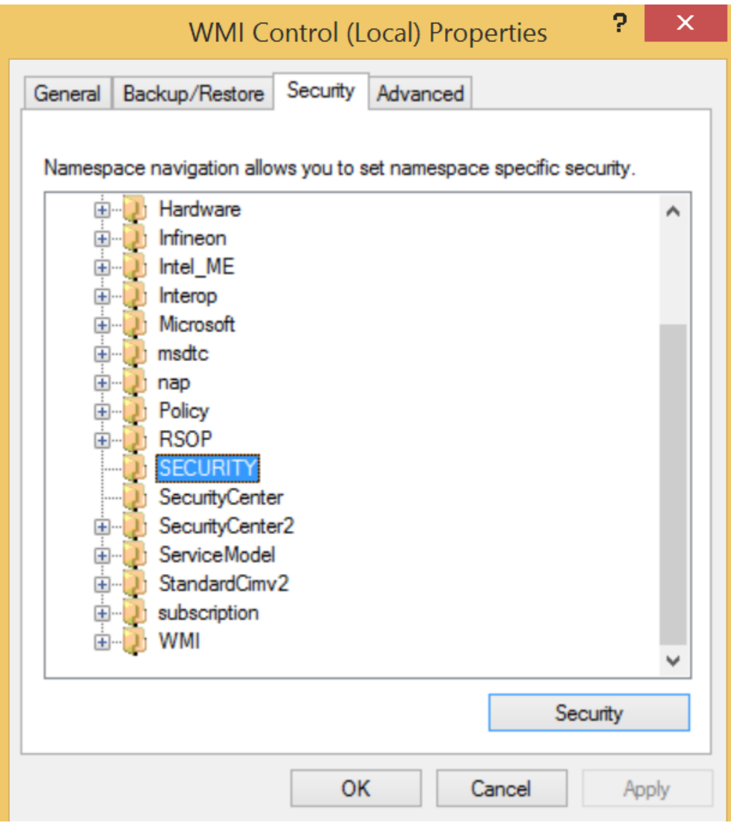
Step 1. Search -> **WMImgmt.msc**

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

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

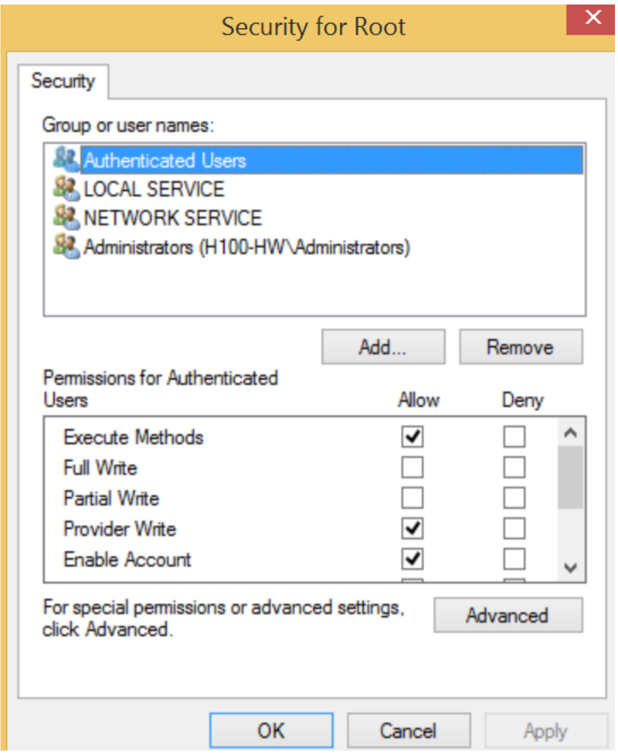


Step 4. Select **"Security"** tab in WMI Control Properties and open **"SECURITY"**



Namespace navigation allows you to set namespace specific security.

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



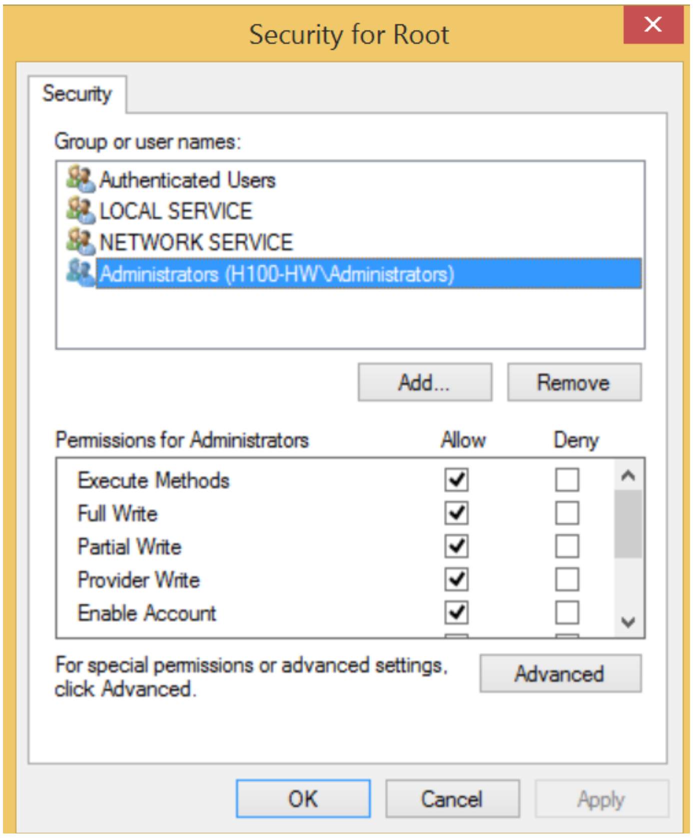
Group or user names:

- 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



Security for Root

Security

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	☑	□

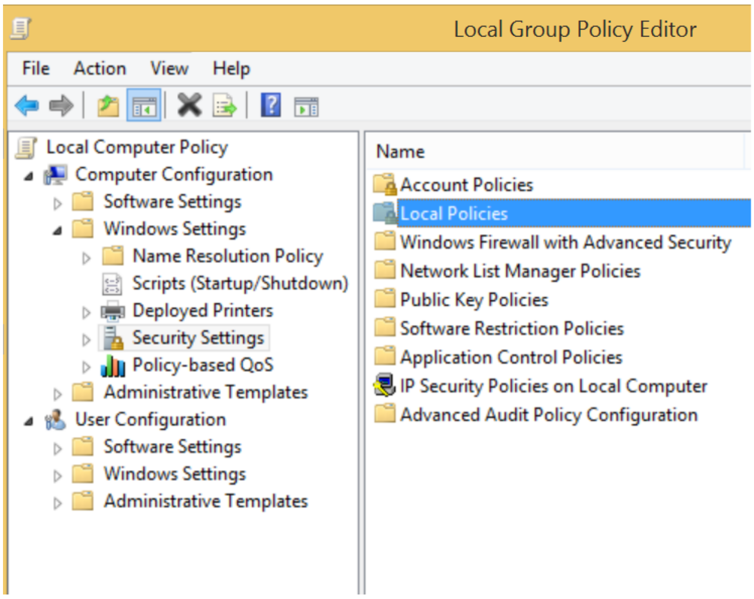
For special permissions or advanced settings, click Advanced.

E.3. WMI impersonation Rights

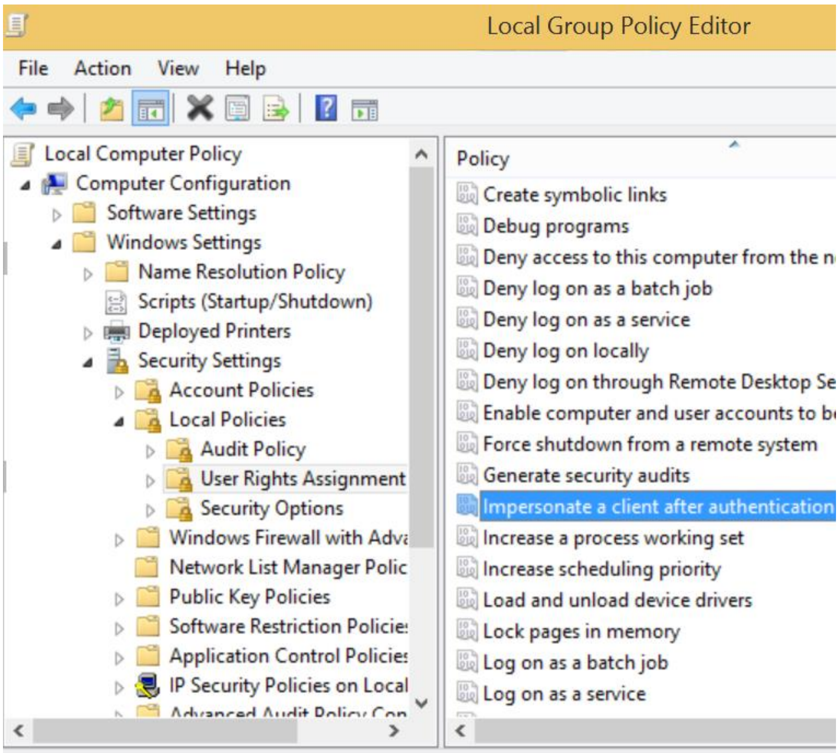
Step 1. Search -> **gpedit.msc**

Step 2. Run **“gpedit.msc”**

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



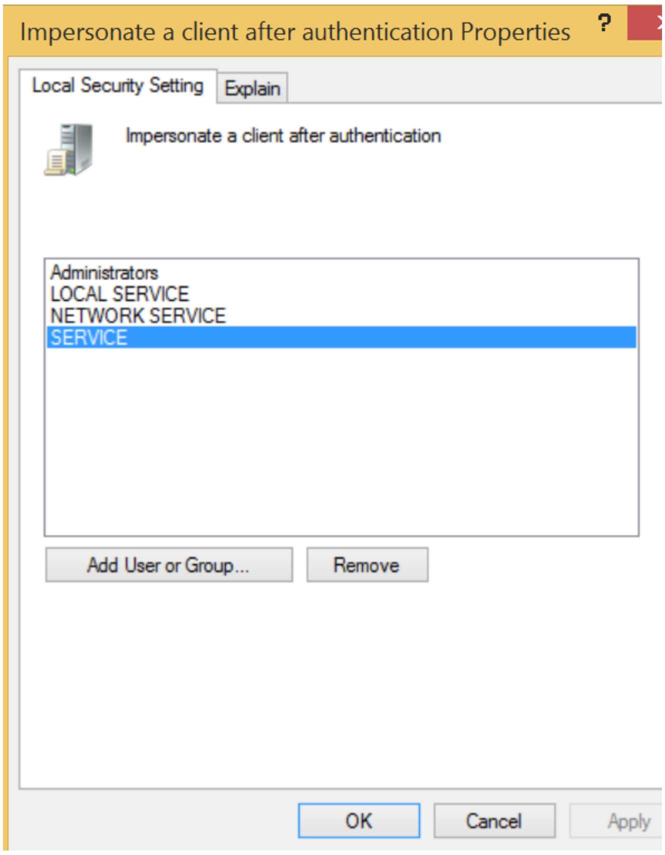
Step 4. Open **“Impersonate a client after authentication”** from **“User Rights Assignment”** in **“Local Policies”**



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 Policie
      - 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

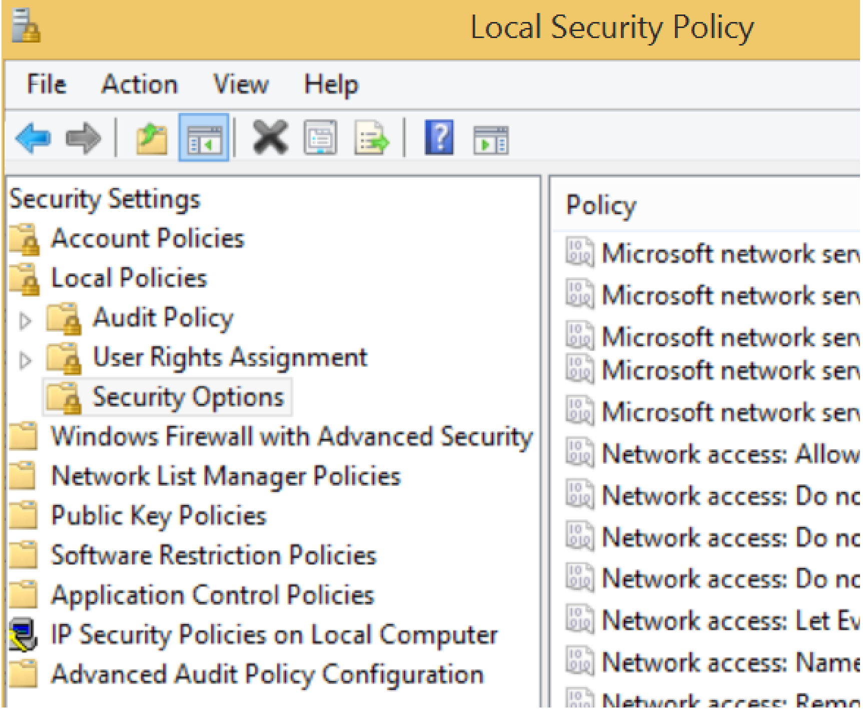
Administrators
LOCAL SERVICE
NETWORK SERVICE
SERVICE

E.4. Network Access

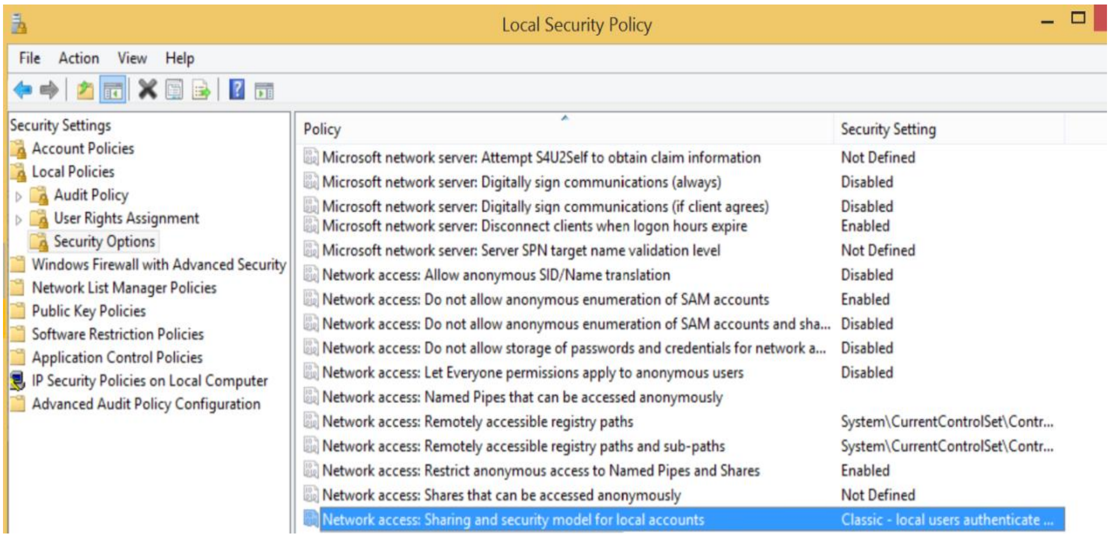
Step 1. Search -> **secpol.msc**

Step 2. Run **"secpol.msc"**

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



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


Local Security Policy
File
Action
View
Help
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 ...