## Getac

# Getac BIOS Configuration with Windows Management Instrumentation for Raptor Lake Platform

Rev 1.02 Jul 01, 2024

### **Revision History**

Rev	Date	Description
R1.00	2023/10/17	First version
		1. Modify 2.4.2 Item table & Appendix A-1.Models Mapping Table.
		2. Add B360G2 project WMI record.
R1.01	2024/05/27	Change Asset Tag field to Advanced page.
		Revised wording and format for p5~9, 12, 15~22
R1.02	2024/07/01	Modify 2.4.2 Item table & Appendix A-1. Models Mapping Table.

#### **Table of Contents**

Revision History
Chapter 1.Introduction
1.1. Overview
1.2. Disclaimer
Chapter 2.Getac WMI Interface
2.1. Configure the BIOS Settings
2.2. Query BIOS User Password Status
2.3.Set BIOS User Password7
2.4.Switch to the BIOS Configure Mode
2.4.1.Load the default BIOS settings9
2.4.2.Query/Change the Getac BIOS Settings
Appendix A-1.Models Mapping Table
Appendix B.VB Script to set the supervisor password15
Appendix C.VB Script to Query the OS Select
Appendix D.Check Procedure for Remote Access
E.1. DCOM permissions
E.2. WMI permissions
E.3. WMI impersonation Rights
Getac Convright © Getac Techr

E.4. Network Access	22
---------------------	----



Page 4 of 22

#### **Chapter 1.Introduction**

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

#### 1.1. Overview

Most of Windows<sup>®</sup> 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.



## Getac

Page 5 of 22

#### 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.



Page 6 of 22

#### **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"



Page 7 of 22

#### 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 <u>10</u>. For models supporting "StrongPassword", the maximum length of a password can be up to <u>64</u> and the minimum length as <u>4</u>.

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 <u>10</u>. For models supporting "StrongPassword", the maximum length of a password can be up to <u>64</u> and the minimum length as <u>4</u>.

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

Getac

Page 8 of 22

#### 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"



Page 9 of 22

#### Item table:

Page	ltem	WMI Item/ Return Item	Attr.	Return/AcceptValues
	EC Version	ECVersion	R	R1.00.070520
Information	Virtual MAC Address (*Note1)	VirtualMAC	R	XX-XX-XX-XX-XX
	Internal Numlock	InternalNumlock	R/W	"Disabled","Enabled"
Main	FN and Ctrl Key Placement	FNCtrlKeyPlacement	R/W	"CtrlFN"," FNCtrl"
	WMI Version	WMIVersion	R	"0.00"-"9.99"
	Wake Up Capability	HomeButtonWakeup	R/W	"Disabled", "Enabled"
	Power Button Delay	PowerButtonDelay	R/W	"NoDelay", "1sec", "2sec"
	AC Initiation	ACInitiation	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"
Advanced	MAC Address Pass Through	MACAddressPassThrough	R/W	"Disabled", "Enabled"
	Secondary Boot Block Backup	SBBBackup	R/W	"Disabled", "Enabled"
	Active	IntelAMTSupport	R/W	"Disabled", "Enabled"
	Management Tech.	IntelAMTSetupPrompt	R/W	"Disabled", "Enabled"
	Support (*Note2)	IntelAMTUSBProvision	R/W	"Disabled", "Enabled"
	Virtualization Tech	IntelVT	R/W	"Disabled", "Enabled"
		VTd	R/W	"Disabled", "Enabled"

**Getac** 

Page 10 of 22

Page	Item	WMI Item/ Return Item	Attr.	Return/AcceptValues
		WirelessLAN	R/W	"Disabled", "Enabled"
		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"
	Device	FrontWebcam	R/W	"Disabled", "Enabled"
	Configuration	RearCamera	R/W	"Disabled", "Enabled"
		Revende DN4		"PowerSaving",
		BarcodePivi	K/ VV	"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"
	Asset Tag	AssetTag	R/W	32 characters maximum
	StrongPassword	StrongPassword	R/W	"Disabled", "Enabled"
	Password on Boot	PasswordonBoot	R/W	"Disabled", "Enabled"
	PasswordConfig	PasswordConfig	R/W	"04"-"64"
	Secure Boot			
	Configuration	LoadMSFTUEFICA	R/W	"Disabled", "Enabled"
Security	(*Note3)			
	Security Freeze	SocurityFroozol ock	D/\\/	"Disabled" "Enabled"
	Lock	JecuiltyFleezeLOCK		Disabieu , Lilabieu
	Intel Trusted			
	Execution	IntelTrustedExeTech	R/W	"Disabled", "Enabled"
	Technology			

Getac

Page 11 of 22

Page	ltem	WMI Item/ Return Item	Attr.	Return/AcceptValues
	(*Note2)			
	Boot Type Order <b>(*Note4)</b>	BootTypeOrder	R/W	"HardDisk", "USBDisk", "USBCD", "Network", "CDROM"
		HardDiskDrive	R/W	"Off", "On"
Boot		USBDiskDrive	R/W	"Off", "On"
	Boot Device	USBCDDVDDrive	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				
\$410G5	Others			
"HardDisk",	"HardDisk",			
"USBDisk",	"USBDisk",			
"Network",	"Network",			
"USBCD",	"USBCD"			
"CDROM"				

Getac

Page 12 of 22

O = Support

X = Not Support

#### Appendix A-1. Models Mapping Table

Page	Item	WMI Item/ Return Item	Attr.	S410G5	B360G2	F110G7	
Information	EC Version	ECVersion	R	0	0	0	
	Virtual MAC Address	VirtualMAC	R	Х	Х	Х	
Main	Internal Numlock	InternalNumlock	R/W	0	0	Х	
	FN and Ctrl Key Placement	FNCtrlKeyPlacement	R/W	0	0	0	
	WMI Version	WMIVersion	R	0	0	0	
	WakeUp Capability	HomeButtonWakeup	R/W	х	х	0	
	Power Button Delay	PowerButtonDelay	R/W	0	0	0	
	AC Initiation	ACInitiation	R/W	0	0	0	
	Magnetic Sensor	MagneticSensor	R/W	0	0	0	
	USB Power-off Charging	USBPowerOffCharging	R/W	0	0	0	
	Screen Tapping for Boot Options	ScreenTappingforBootOp	R/W	Х	Х	0	
	MAC Address Pass Through	MACAddressPassThrough	R/W	0	0	0	
	Secondary Boot Block Backup	SBBBackup	R/W	0	Х	0	
	Active Management Tech. Support	IntelAMTSupport	R/W	0	0	0	
		IntelAMTSetupPrompt	R/W	0	0	0	
Advanced		IntelAMTUSBProvision	R/W	0	0	0	
	Virtualization Tech. Setup	IntelVT	R/W	0	0	0	
		VTd	R/W	0	0	0	
		WirelessLAN	R/W	0	0	0	
		WWAN	R/W	0	0	0	
		Bluetooth	R/W	0	0	0	
		MediaCardReader	R/W	0	0	0	
	Device Configuration	SmartCardReader	R/W	0	0	0	
		RFID	R/W	0	0	0	
		FingerprintScanner	R/W	0	0	0	
		FrontWebcam	R/W	0	0	0	
		RearCamera	R/W	Х	Х	0	

Getac

Page 13 of 22

Page	Item	WMI Item/ Return Item	Attr.	S410G5	B360G2	F110G7		
		BarcodePM	R/W	0	0	0		
		Thunderbolt	R/W	0	0	0		
		SystemUSBPort	R/W	0	0	0		
		DockingUSBPortSetting	R/W	0	0	0		
		InternalMicrophone	R/W	0	0	0		
		InternalSpeaker	R/W	0	0	0		
		SerialPort	R/W	Х	Х	0		
	Asset Tag	AssetTag	R/W	0	0	0		
	Password on Boot	PasswordonBoot	R/W	0	0	0		
	StrongPassword	StrongPassword	R/W	0	0	0		
Constitut	PasswordConfig	PasswordConfig	R/W	0	0	0		
Security	Secure Boot Configuration	LoadMSFTUEFICA	R/W	0	0	0		
	SecurityFreezeLock	SecurityFreezeLock	R/W	0	0	Х		
	Intel Trusted Execution Technology	IntelTrustedExeTech	R/W	0	0	0		
	Boot Type Order	BootTypeOrder	R/W	0	0	0		
		HardDiskDrive	R/W	0	0	0		
Deet		USBDiskDrive	R/W	0	0	0		
BOOT	Boot Device	USBCDDVDDrive	R/W	0	0	0		
		NetworkDrive	R/W	0	0	0		
		CDDVDDrive	R/W	0	0	Х		
	Fast Boot	FastBoot	R/W	0	0	0	1	
	Alternative WBM option	AlternativeWBM	R/W	0	0	0		

Getac

Page 14 of 22

#### 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.

l\_\_\_\_\_

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\_()

I\_\_\_\_\_

' 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)

I\_\_\_\_\_

'ListOutParams

Wscript.Echo "Out Parameters: "&objInParam.Properties\_.Item("DataIn") Wscript.echo "DataOut: " &objOutParams.DataOut

Getac

Page 15 of 22

Appendix C.VB Script to Query the OS Select Users can query OS select with below VBScript.
<pre>strComputer = "." Set objWMIService = GetObject("winmgmts:\\" &amp;strComputer&amp; "\root\WMI")</pre>
' 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.PropertiesItem("DataIn") = "OSSelect"
' Execute the method and obtain the return status. ' TheOutParameters object in objOutParams is created by the provider.
' ' ListOutParams

Wscript.Echo "Out Parameters: "&objInParam.Properties\_.Item("DataIn") Wscript.echo "DataOut: " &objOutParams.DataOut



Page 16 of 22

Copyright © Getac Technology Corporation 2024. All Rights Reserved

\_\_\_\_\_

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



Page 17 of 22

Access	Permission	? ×
Security Limits		
Group or user names:		
ALL APPLICATION PACK     ALL APPLICATION     ALL     ALL APPLICATION     ALL     ALL	(AGES H100-HW\Performanc I100-HW\Distributed (	ee Log Users) COM Users)
	Add	Remove
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"



Copyright © Getac Technology Corporation 2024. All Rights Reserved

Page 18 of 22

WMI Control (Local) Properties ?	×
General Backup/Restore Security Advanced	
Namespace navigation allows you to set namespace specific security.	^
Security	
OK Cancel Apply	/

Step 5. Ensure "Execute Methods", "Provider Write" and "Enable Account" are set to Allow in

#### Permission for Authenticated Users

	Security	for Root	
Security			
Group or user nam	ies:		
Authenticate	d Users		
& LOCAL SER	VICE		
NETWORK S	SERVICE		
Administrators	s (H 100-H VV VAO	ministrators)	
		Add	Remove
Permissions for Au	thenticated		
Users		Allow	Deny
Execute Method	ds	✓	
Full Write			
Partial Write			
Enable Account	•	<ul> <li>✓</li> </ul>	
Ear appealal porming	sions or advance	ed settings,	Advanced
click Advanced			
click Advanced.			
click Advanced.			

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



Copyright © Getac Technology Corporation 2024. All Rights Reserved

Page 19 of 22

Security	/ Tor Root	
curity		
aroup or user names:		
& Authenticated Users		
& LOCAL SERVICE		
RETWORK SERVICE		
💐 Administrators (H100-HW\A	dministrators)	
	Add	Remove
emissions for Administrators	Allow	Denv
ermissions for Administrators	Allow	Deny
Execute Methods	Allow	Deny
ermissions for Administrators Execute Methods Full Write		Deny
ermissions for Administrators Execute Methods Full Write Partial Write		Deny
ermissions for Administrators Execute Methods Full Write Partial Write Provider Write	Allow V V	Deny
Permissions for Administrators Execute Methods Full Write Partial Write Provider Write Enable Account	Allow V V V	Deny
ermissions for Administrators Execute Methods Full Write Partial Write Provider Write Enable Account or special permissions or advanc lick Advanced.	Allow V V Ced settings,	Deny
Permissions for Administrators Execute Methods Full Write Partial Write Provider Write Enable Account or special permissions or advance lick Advanced.	Allow	Deny
emissions for Administrators Execute Methods Full Write Partial Write Provider Write Enable Account or special permissions or advance lick Advanced.	Allow	Deny

#### 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"**.



Copyright © Getac Technology Corporation 2024. All Rights Reserved

Page 20 of 22



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

Impersonate a client after authentication Properties	2
Local Security Setting Explain	
Impersonate a client after authentication	
Administrators LOCAL SERVICE NETWORK SERVICE	
SERVICE	
Add User or Group Remove	
	Angle

Getac

Copyright © Getac Technology Corporation 2024. All Rights Reserved

Page 21 of 22

#### 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"

🚡 Local	Local Security Policy		
File     Action     View     Help       Image: Second state     Image: Second state     Image: Second state     Image: Second state			
<ul> <li>Account Policies</li> <li>Account Policies</li> <li>Local Policies</li> <li>Audit Policy</li> <li>Buser Rights Assignment</li> <li>Security Options</li> <li>Windows Firewall with Advanced Security</li> <li>Network List Manager Policies</li> <li>Public Key Policies</li> <li>Software Restriction Policies</li> <li>Application Control Policies</li> <li>IP Security Policies on Local Computer</li> <li>Advanced Audit Policy Configuration</li> </ul>	Policy Microsoft network sen Microsoft network sen Microsoft network sen Microsoft network sen Microsoft network sen Network access: Allow Network access: Do nc Network access: Do nc Network access: Do nc Network access: Let Ev Network access: Name Network access: Name		

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

accounts" is set to "Classic".

Getac

3	Local Security Policy	-
File Action View Help		
Account Policies  Count Policies  Count Policies  Count Policy  Count Policy  Count Policy  Count Policy  Network List Manager Policies  Public Key Policies  Software Restriction Policies  Application Control Policies  Application Control Policies  Advanced Audit Policy Configuration	Policy         Image: Server Server: Attempt S4U2Self to obtain claim information         Image: Server: Digitally sign communications (always)         Image: Microsoft network server: Digitally sign communications (ff client agrees)         Image: Microsoft network server: Disconnect clients when logon hours expire         Image: Microsoft network server: Server SPN target name validation level         Image: Microsoft network server: Server SPN target name validation level         Image: Network access: Do not allow anonymous enumeration of SAM accounts         Image: Network access: Do not allow anonymous enumeration of SAM accounts and sha         Image: Network access: Do not allow storage of passwords and credentials for network a         Image: Network access: Let Everyone permissions apply to anonymous users         Image: Network access: Remotely accessible registry paths         Image: Network access: Remotely accessible registry paths         Image: Network access: Restrict anonymous access to Named Pipes and Shares         Image: Network access: Shares that can be accessed anonymously	Security Setting Not Defined Disabled Disabled Enabled Not Defined Disabled Enabled Disabled Disabled Disabled Disabled System\CurrentControlSet\Contr System\CurrentControlSet\Contr Enabled Not Defined

Copyright © Getac Technology Corporation 2024. All Rights Reserved

Page 22 of 22