Table 2-38. Additional MSRs Supported by Intel® Xeon® Processors with a CPUID Signature DisplayFamily_DisplayModel Value of 06_4FH

Regi Add		Register Name / Bit Fields	Scope	Bit Description
Hex	Dec			

See Table 2-20, Table 2-21, Table 2-29, and Table 2-30 for other MSR definitions applicable to processors with a CPUID Signature DisplayFamily_DisplayModel value of 06_45H.

NOTES:

1. An override configuration lower than the factory-set configuration is always supported. An override configuration higher than the factory-set configuration is dependent on features specific to the processor and the platform.

2.17 MSRS IN THE 6TH GENERATION, 7TH GENERATION, 8TH GENERATION, 9TH GENERATION, 10TH GENERATION, 11TH GENERATION, 12TH GENERATION, AND 13TH GENERATION INTEL® CORE™ PROCESSORS, INTEL® XEON® SCALABLE PROCESSOR FAMILY, 2ND, 3RD, AND 4TH GENERATION INTEL® XEON® SCALABLE PROCESSOR FAMILY, 8TH GENERATION INTEL® CORE™ I3 PROCESSORS, AND INTEL® XEON® E PROCESSORS

6th generation Intel[®] Core[™] processors are based on Skylake microarchitecture and have a CPUID Signature DisplayFamily DisplayModel value of 06 4EH or 06 5EH.

The Intel[®] Xeon[®] Scalable Processor Family based on the Skylake microarchitecture, the 2nd generation Intel[®] Xeon[®] Scalable Processor Family based on the Cascade Lake product, and the 3rd generation Intel[®] Xeon[®] Scalable Processor Family based on the Cooper Lake product all have a CPUID Signature DisplayFamily_DisplayModel value of 06_55H .

7th generation Intel[®] Core[™] processors are based on the Kaby Lake microarchitecture, 8th generation and 9th generation Intel[®] Core[™] processors, and Intel[®] Xeon[®] E processors are based on Coffee Lake microarchitecture; these processors have a CPUID Signature DisplayFamily_DisplayModel value of 06_8EH or 06_9EH .

8th generation Intel[®] Core™ i3 processors are based on Cannon Lake microarchitecture and have a CPUID Signature DisplayFamily DisplayModel value of 06 66H.

10th generation Intel[®] Core[™] processors are based on Comet Lake microarchitecture (with a CPUID Signature DisplayFamily_DisplayModel value of 06_A5H or 06_A6H) and Ice Lake microarchitecture (with a CPUID Signature DisplayFamily_DisplayModel value of 06_7DH or 06_7EH).

11th generation Intel $^{\mathbb{R}}$ Core $^{\mathsf{TM}}$ processors are based on Tiger Lake microarchitecture and have a CPUID Signature DisplayFamily DisplayModel value of 06 8CH or 06 8DH.

The 3rd generation Intel[®] Xeon[®] Scalable Processor Family is based on Ice Lake microarchitecture and has a CPUID Signature DisplayFamily_DisplayModel value of 06_6AH or 06_6CH.

12th generation Intel[®] Core[™] processors supporting the Alder Lake performance hybrid architecture have a CPUID Signature DisplayFamily_DisplayModel value of 06_97H or 06_9AH.

13th generation Intel[®] Core[™] processors supporting the Raptor Lake performance hybrid architecture have a CPUID Signature DisplayFamily_DisplayModel value of 06_BAH, 06_B7H, or 06_BFH.

The 4th generation Intel[®] Xeon[®] Scalable Processor Family is based on Sapphire Rapids microarchitecture and has a CPUID Signature DisplayFamily_DisplayModel value of 06_8FH.

These processors support the MSR interfaces listed in Table 2-20, Table 2-21, Table 2-25, Table 2-29, Table 2-35, and Table 2-39¹. For an MSR listed in Table 2-39 that also appears in the model-specific tables of prior generations, Table 2-39 supersede prior generation tables.

Tables 2-40 through 2-52 list additional supported MSR interfaces for specific processors; see each table for additional details.

The notation of "Platform" in the Scope column (with respect to MSR_PLATFORM_ENERGY_COUNTER and MSR_PLATFORM_POWER_LIMIT) is limited to the power-delivery domain and the specifics of the power delivery integration may vary by platform vendor's implementation.

Table 2-39. Additional MSRs Supported by 6th Generation, 7th Generation, 8th Generation, 9th Generation, 10th Generation, 11th Generation, 12th Generation, and 13th Generation Intel® Core™ Processors, Intel® Xeon® Scalable Processor Family, 2nd, 3rd, and 4th Generation Intel® Xeon® Scalable Processor Family, 8th Generation Intel® Core™ i3 Processors, and Intel® Xeon® E Processors

Regi Addı		Register Name / Bit Fields	Scope	Bit Description
Hex	Dec			
ЗАН	58	IA32_FEATURE_CONTROL	Thread	Control Features in Intel 64 Processor (R/W)
				See Table 2-2.
FEH	254	IA32_MTRRCAP	Thread	MTRR Capability (R/O, Architectural)
				See Table 2-2
19CH	412	IA32_THERM_STATUS	Соге	Thermal Monitor Status (R/W)
				See Table 2-2.
		0		Thermal Status (R/O)
				See Table 2-2.
		1		Thermal Status Log (R/WCO)
				See Table 2-2.
		2		PROTCHOT # or FORCEPR# Status (R/O)
				See Table 2-2.
		3		PROTCHOT # or FORCEPR# Log (R/WC0)
				See Table 2-2.
		4		Critical Temperature Status (R/O)
				See Table 2-2.
		5		Critical Temperature Status Log (R/WCO)
				See Table 2-2.
		6		Thermal threshold #1 Status (R/O)
				See Table 2-2.
		7		Thermal threshold #1 Log (R/WC0)
				See Table 2-2.
		8		Thermal Threshold #2 Status (R/O)
				See Table 2-2.
		9		Thermal Threshold #2 Log (R/WC0)
				See Table 2-2.
		10		Power Limitation Status (R/O)
				See Table 2-2.

^{1.} MSRs at the following addresses are not supported in the 12th generation Intel Core processor E-core: 3F7H. MSRs at the following addresses are not supported in the 12th generation Intel Core processor E-core or P-core: 652H, 653H, 655H, 656H, DB0H, DB1H, DB2H, and D90H.

Table 2-39. Additional MSRs Supported by 6th Generation, 7th Generation, 8th Generation, 9th Generation, 10th Generation, 11th Generation, 12th Generation, and 13th Generation Intel® Core™ Processors, Intel® Xeon® Scalable Processor Family, 2nd, 3rd, and 4th Generation Intel® Xeon® Scalable Processor Family, 8th Generation Intel® Core™ i3 Processors, and Intel® Xeon® E Processors

Regi Add		Register Name / Bit Fields	Scope	Bit Description
Hex	Dec			
		11		Power Limitation Log (R/WCO) See Table 2-2.
		12		Current Limit Status (R/O) See Table 2-2.
		13		Current Limit Log (R/WCO) See Table 2-2.
		14		Cross Domain Limit Status (R/O) See Table 2-2.
		15		Cross Domain Limit Log (R/WCO) See Table 2-2.
		22:16		Digital Readout (R/O) See Table 2-2.
		26:23		Reserved
		30:27		Resolution in Degrees Celsius (R/O) See Table 2-2.
		31		Reading Valid (R/O) See Table 2-2.
		63:32		Reserved
1ADH	429	MSR_TURBO_RATIO_LIMIT	Package	Maximum Ratio Limit of Turbo Mode R/O if MSR_PLATFORM_INFO.[28] = 0, R/W if MSR_PLATFORM_INFO.[28] = 1
		7:0	Package	Maximum Ratio Limit for 1C Maximum turbo ratio limit of 1 core active.
		15:8	Package	Maximum Ratio Limit for 2C Maximum turbo ratio limit of 2 core active.
		23:16	Package	Maximum Ratio Limit for 3C Maximum turbo ratio limit of 3 core active.
		31:24	Package	Maximum Ratio Limit for 4C Maximum turbo ratio limit of 4 core active.
		63:32		Reserved
1C9H	457	MSR_LASTBRANCH_TOS	Thread	Last Branch Record Stack TOS (R/W)
				Contains an index (bits 0-4) that points to the MSR containing the most recent branch record.
1FCH	508	MSR_POWER_CTL	Core	Power Control Register See http://biosbits.org.
		0		Reserved

Table 2-39. Additional MSRs Supported by 6th Generation, 7th Generation, 8th Generation, 9th Generation, 10th Generation, 11th Generation, 12th Generation, and 13th Generation Intel® Core™ Processors, Intel® Xeon® Scalable Processor Family, 2nd, 3rd, and 4th Generation Intel® Xeon® Scalable Processor Family, 8th Generation Intel® Core™ i3 Processors, and Intel® Xeon® E Processors

_	ister ress	Register Name / Bit Fields	Scope	Bit Description
Hex	Dec			
		1	Package	C1E Enable (R/W) When set to '1', will enable the CPU to switch to the Minimum Enhanced Intel SpeedStep Technology operating point when all execution cores enter MWAIT (C1).
		18:2		Reserved
		19		Disable Energy Efficiency Optimization (R/W) Setting this bit disables the P-States energy efficiency optimization. Default value is 0. Disable/enable the energy efficiency optimization in P-State legacy mode (when IA32_PM_ENABLE[HWP_ENABLE] = 0), has an effect only in the turbo range or into PERF_MIN_CTL value if it is not zero set. In HWP mode (IA32_PM_ENABLE[HWP_ENABLE] == 1), has an effect between the OS desired or OS maximize to the OS minimize performance setting.
		20		Disable Race to Halt Optimization (R/W) Setting this bit disables the Race to Halt optimization and avoids this optimization limitation to execute below the most efficient frequency ratio. Default value is 0 for processors that support Race to Halt optimization.
		63:21		Reserved
300H	768	MSR_SGXOWNEREPOCHO	Package	Lower 64 Bit CR_SGXOWNEREPOCH (W) Writes do not update CR_SGXOWNEREPOCH if CPUID.(EAX=12H, ECX=0):EAX.SGX1 is 1 on any thread in the package.
		63:0		Lower 64 bits of an 128-bit external entropy value for key derivation of an enclave.
301H	769	MSR_SGXOWNEREPOCH1	Package	Upper 64 Bit CR_SGXOWNEREPOCH (W) Writes do not update CR_SGXOWNEREPOCH if CPUID.(EAX=12H, ECX=0):EAX.SGX1 is 1 on any thread in the package.
		63:0		Upper 64 bits of an 128-bit external entropy value for key derivation of an enclave.
38EH	910	IA32_PERF_GLOBAL_STATUS		See Table 2-2. See Section 20.2.4, "Architectural Performance Monitoring Version 4."
		0	Thread	Ovf_PMC0
		1	Thread	Ovf_PMC1
		2	Thread	Ovf_PMC2
		3	Thread	Ovf_PMC3
		4	Thread	Ovf_PMC4 (if CPUID.0AH:EAX[15:8] > 4)

Table 2-39. Additional MSRs Supported by 6th Generation, 7th Generation, 8th Generation, 9th Generation, 10th Generation, 11th Generation, 12th Generation, and 13th Generation Intel® Core™ Processors, Intel® Xeon® Scalable Processor Family, 2nd, 3rd, and 4th Generation Intel® Xeon® Scalable Processor Family, 8th Generation Intel® Core™ i3 Processors, and Intel® Xeon® E Processors

	ister ress	Register Name / Bit Fields	Scope	Bit Description
Hex	Dec			
		5	Thread	Ovf_PMC5 (if CPUID.OAH:EAX[15:8] > 5)
		6	Thread	Ovf_PMC6 (if CPUID.OAH:EAX[15:8] > 6)
		7	Thread	Ovf_PMC7 (if CPUID.OAH:EAX[15:8] > 7)
		31:8		Reserved
		32	Thread	Ovf_FixedCtr0
		33	Thread	Ovf_FixedCtr1
		34	Thread	Ovf_FixedCtr2
		54:35		Reserved
		55	Thread	Trace_ToPA_PMI
		57:56		Reserved
		58	Thread	LBR_Frz
		59	Thread	CTR_Frz
		60	Thread	ASCI
		61	Thread	Ovf_Uncore
		62	Thread	Ovf_BufDSSAVE
		63	Thread	CondChgd
390H	912	IA32_PERF_GLOBAL_STATUS_RESET		See Table 2-2. See Section 20.2.4, "Architectural Performance Monitoring Version 4."
		0	Thread	Set 1 to clear Ovf_PMCO.
		1	Thread	Set 1 to clear Ovf_PMC1.
		2	Thread	Set 1 to clear Ovf_PMC2.
		3	Thread	Set 1 to clear Ovf_PMC3.
		4	Thread	Set 1 to clear Ovf_PMC4 (if CPUID.OAH:EAX[15:8] > 4).
		5	Thread	Set 1 to clear Ovf_PMC5 (if CPUID.OAH:EAX[15:8] > 5).
		6	Thread	Set 1 to clear Ovf_PMC6 (if CPUID.OAH:EAX[15:8] > 6).
		7	Thread	Set 1 to clear Ovf_PMC7 (if CPUID.OAH:EAX[15:8] > 7).
		31:8		Reserved
		32	Thread	Set 1 to clear Ovf_FixedCtrO.
		33	Thread	Set 1 to clear Ovf_FixedCtr1.
		34	Thread	Set 1 to clear Ovf_FixedCtr2.
		54:35		Reserved
		55	Thread	Set 1 to clear Trace_ToPA_PMI.
		57:56		Reserved
		58	Thread	Set 1 to clear LBR_Frz.
		59	Thread	Set 1 to clear CTR_Frz.

Table 2-39. Additional MSRs Supported by 6th Generation, 7th Generation, 8th Generation, 9th Generation, 10th Generation, 11th Generation, 12th Generation, and 13th Generation Intel® Core™ Processors, Intel® Xeon® Scalable Processor Family, 2nd, 3rd, and 4th Generation Intel® Xeon® Scalable Processor Family, 8th Generation Intel® Core™ i3 Processors, and Intel® Xeon® E Processors

Regi Add	ister ress	Register Name / Bit Fields	Scope	Bit Description
Hex	Dec			
		60	Thread	Set 1 to clear ASCI.
		61	Thread	Set 1 to clear Ovf_Uncore.
		62	Thread	Set 1 to clear Ovf_BufDSSAVE.
		63	Thread	Set 1 to clear CondChgd.
391H	913	IA32_PERF_GLOBAL_STATUS_SET		See Table 2-2. See Section 20.2.4, "Architectural Performance Monitoring Version 4."
		0	Thread	Set 1 to cause Ovf_PMC0 = 1.
		1	Thread	Set 1 to cause Ovf_PMC1 = 1.
		2	Thread	Set 1 to cause Ovf_PMC2 = 1.
		3	Thread	Set 1 to cause Ovf_PMC3 = 1.
		4	Thread	Set 1 to cause Ovf_PMC4=1 (if CPUID.0AH:EAX[15:8] > 4).
		5	Thread	Set 1 to cause Ovf_PMC5=1 (if CPUID.0AH:EAX[15:8] > 5).
		6	Thread	Set 1 to cause Ovf_PMC6=1 (if CPUID.0AH:EAX[15:8] > 6).
		7	Thread	Set 1 to cause Ovf_PMC7=1 (if CPUID.0AH:EAX[15:8] > 7).
		31:8		Reserved
		32	Thread	Set 1 to cause Ovf_FixedCtr0 = 1.
		33	Thread	Set 1 to cause Ovf_FixedCtr1 = 1.
		34	Thread	Set 1 to cause Ovf_FixedCtr2 = 1.
		54:35		Reserved
		55	Thread	Set 1 to cause Trace_ToPA_PMI = 1.
		57:56		Reserved
		58	Thread	Set 1 to cause LBR_Frz = 1.
		59	Thread	Set 1 to cause CTR_Frz = 1.
		60	Thread	Set 1 to cause ASCI = 1.
		61	Thread	Set 1 to cause Ovf_Uncore.
		62	Thread	Set 1 to cause Ovf_BufDSSAVE.
		63		Reserved
392H	914	IA32_PERF_GLOBAL_INUSE	Thread	See Table 2-2.
3F7H	1015	MSR_PEBS_FRONTEND	Thread	FrontEnd Precise Event Condition Select (R/W)
		2:0		Event Code Select
		3		Reserved
		4		Event Code Select High

Table 2-39. Additional MSRs Supported by 6th Generation, 7th Generation, 8th Generation, 9th Generation, 10th Generation, 11th Generation, 12th Generation, and 13th Generation Intel® Core™ Processors, Intel® Xeon® Scalable Processor Family, 2nd, 3rd, and 4th Generation Intel® Xeon® Scalable Processor Family, 8th Generation Intel® Core™ i3 Processors, and Intel® Xeon® E Processors

	ister ress	Register Name / Bit Fields	Scope	Bit Description
Hex	Dec			
		7:5		Reserved
		19:8		IDQ_Bubble_Length Specifier
		22:20		IDQ_Bubble_Width Specifier
		63:23		Reserved
500H	1280	IA32_SGX_SVN_STATUS	Thread	Status and SVN Threshold of SGX Support for ACM (R/O)
		0		Lock
				See Section 39.11.3, "Interactions with Authenticated Code Modules (ACMs)."
		15:1		Reserved
		23:16		SGX_SVN_SINIT
				See Section 39.11.3, "Interactions with Authenticated Code Modules (ACMs)."
		63:24		Reserved
560H	1376	IA32_RTIT_OUTPUT_BASE	Thread	Trace Output Base Register (R/W)
				See Table 2-2.
561H	1377	IA32_RTIT_OUTPUT_MASK_PTRS	Thread	Trace Output Mask Pointers Register (R/W) See Table 2-2.
	1202	IA22 DTIT CTI	Theread	
570H	1392	IA32_RTIT_CTL 0	Thread	Trace Control Register (R/W) TraceEn
		1		CYCEn
		2		OS Llare
		3		User
		6:4		Reserved, must be zero.
		7		CR3Filter
		8		ToPA Writing 0 will #GP if also setting TraceEn.
		9		MTCEn
		10		TSCEn
		11		DisRETC
		12		Reserved, must be zero.
		13		BranchEn
		17:14		
		18		MTCFreq
				Reserved, must be zero.
		22:19		CycThresh
		23		Reserved, must be zero.

Table 2-39. Additional MSRs Supported by 6th Generation, 7th Generation, 8th Generation, 9th Generation, 10th Generation, 11th Generation, 12th Generation, and 13th Generation Intel® Core™ Processors, Intel® Xeon® Scalable Processor Family, 2nd, 3rd, and 4th Generation Intel® Xeon® Scalable Processor Family, 8th Generation Intel® Core™ i3 Processors, and Intel® Xeon® E Processors

Register Address		Register Name / Bit Fields	Scope	Bit Description
Hex	Dec			
		27:24		PSBFreq
		31:28		Reserved, must be zero.
		35:32		ADDRO_CFG
		39:36		ADDR1_CFG
		63:40		Reserved, must be zero.
571H	1393	IA32_RTIT_STATUS	Thread	Tracing Status Register (R/W)
		0		FilterEn, writes ignored.
		1		ContexEn, writes ignored.
		2		TriggerEn, writes ignored.
		3		Reserved
		4		Error (R/W)
		5		Stopped
		31:6		Reserved, must be zero.
		48:32		PacketByteCnt
		63:49		Reserved, must be zero.
572H	1394	IA32_RTIT_CR3_MATCH	Thread	Trace Filter CR3 Match Register (R/W)
		4:0		Reserved
		63:5		CR3[63:5] value to match
580H	1408	IA32_RTIT_ADDRO_A	Thread	Region 0 Start Address (R/W)
		63:0		See Table 2-2.
581H	1409	IA32_RTIT_ADDRO_B	Thread	Region 0 End Address (R/W)
		63:0		See Table 2-2.
582H	1410	IA32_RTIT_ADDR1_A	Thread	Region 1 Start Address (R/W)
		63:0		See Table 2-2.
583H	1411	IA32_RTIT_ADDR1_B	Thread	Region 1 End Address (R/W)
		63:0		See Table 2-2.
639H	1593	MSR_PPO_ENERGY_STATUS	Package	PPO Energy Status (R/O)
				See Section 15.10.4, "PPO/PP1 RAPL Domains."
64DH	1613	MSR_PLATFORM_ENERGY_COUNTER	Platform	Platform Energy Counter (R/O)
				This MSR is valid only if both platform vendor hardware implementation and BIOS enablement support it. This MSR will read 0 if not valid.

Table 2-39. Additional MSRs Supported by 6th Generation, 7th Generation, 8th Generation, 9th Generation, 10th Generation, 11th Generation, 12th Generation, and 13th Generation Intel® Core™ Processors, Intel® Xeon® Scalable Processor Family, 2nd, 3rd, and 4th Generation Intel® Xeon® Scalable Processor Family, 8th Generation Intel® Core™ i3 Processors, and Intel® Xeon® E Processors

Regi Add		Register Name / Bit Fields	Scope	Bit Description
Hex	Dec			
		31:0		Total energy consumed by all devices in the platform that receive power from integrated power delivery mechanism, included platform devices are processor cores, SOC, memory, add-on or peripheral devices that get powered directly from the platform power delivery means. The energy units are specified in the MSR_RAPL_POWER_UNIT.Enery_Status_Unit.
		63:32		Reserved
64EH	1614	MSR_PPERF	Thread	Productive Performance Count (R/O)
		63:0		Hardware's view of workload scalability. See Section 15.4.5.1.
64FH	1615	MSR_CORE_PERF_LIMIT_REASONS	Package	Indicator of Frequency Clipping in Processor Cores (R/W)
				(Frequency refers to processor core frequency.)
		0		PROCHOT Status (R0)
				When set, frequency is reduced below the operating system request due to assertion of external PROCHOT.
		1		Thermal Status (R0)
				When set, frequency is reduced below the operating system request due to a thermal event.
		3:2		Reserved
		4		Residency State Regulation Status (R0)
				When set, frequency is reduced below the operating system request due to residency state regulation limit.
		5		Running Average Thermal Limit Status (R0)
				When set, frequency is reduced below the operating system request due to Running Average Thermal Limit (RATL).
		6		VR Therm Alert Status (R0)
				When set, frequency is reduced below the operating system request due to a thermal alert from a processor Voltage Regulator (VR).
		7		VR Therm Design Current Status (R0)
				When set, frequency is reduced below the operating system request due to VR thermal design current limit.
		8		Other Status (R0)
				When set, frequency is reduced below the operating system request due to electrical or other constraints.
		9		Reserved

Table 2-39. Additional MSRs Supported by 6th Generation, 7th Generation, 8th Generation, 9th Generation, 10th Generation, 11th Generation, 12th Generation, and 13th Generation Intel® Core™ Processors, Intel® Xeon® Scalable Processor Family, 2nd, 3rd, and 4th Generation Intel® Xeon® Scalable Processor Family, 8th Generation Intel® Core™ i3 Processors, and Intel® Xeon® E Processors

Regi Addı		Register Name / Bit Fields	Scope	Bit Description
Hex	Dec			
		10		Package/Platform-Level Power Limiting PL1 Status (R0)
				When set, frequency is reduced below the operating system request due to package/platform-level power limiting PL1.
		11		Package/Platform-Level PL2 Power Limiting Status (R0)
				When set, frequency is reduced below the operating system request due to package/platform-level power limiting PL2/PL3.
		12		Max Turbo Limit Status (R0)
				When set, frequency is reduced below the operating system request due to multi-core turbo limits.
		13		Turbo Transition Attenuation Status (R0)
				When set, frequency is reduced below the operating system request due to Turbo transition attenuation. This prevents performance degradation due to frequent operating ratio changes.
		15:14		Reserved
		16		PROCHOT Log
				When set, indicates that the PROCHOT Status bit has asserted since the log bit was last cleared.
				This log bit will remain set until cleared by software writing 0.
		17		Thermal Log
				When set, indicates that the Thermal Status bit has asserted since the log bit was last cleared.
				This log bit will remain set until cleared by software writing 0.
		19:18		Reserved.
		20		Residency State Regulation Log
				When set, indicates that the Residency State Regulation Status bit has asserted since the log bit was last cleared.
				This log bit will remain set until cleared by software writing 0.
		21		Running Average Thermal Limit Log
				When set, indicates that the RATL Status bit has asserted since the log bit was last cleared.
				This log bit will remain set until cleared by software writing 0.

Table 2-39. Additional MSRs Supported by 6th Generation, 7th Generation, 8th Generation, 9th Generation, 10th Generation, 11th Generation, 12th Generation, and 13th Generation Intel® Core™ Processors, Intel® Xeon® Scalable Processor Family, 2nd, 3rd, and 4th Generation Intel® Xeon® Scalable Processor Family, 8th Generation Intel® Core™ i3 Processors, and Intel® Xeon® E Processors

Regi Add		Register Name / Bit Fields	Scope	Bit Description
Hex	Dec			
		22		VR Therm Alert Log
				When set, indicates that the VR Therm Alert Status bit has asserted since the log bit was last cleared.
				This log bit will remain set until cleared by software
				writing 0.
		23		VR Thermal Design Current Log
				When set, indicates that the VR TDC Status bit has asserted since the log bit was last cleared.
				This log bit will remain set until cleared by software writing 0.
		24		Other Log
				When set, indicates that the Other Status bit has asserted since the log bit was last cleared.
				This log bit will remain set until cleared by software writing 0.
		25		Reserved
		26		Package/Platform-Level PL1 Power Limiting Log
				When set, indicates that the Package or Platform Level PL1 Power Limiting Status bit has asserted since the log bit was last cleared.
				This log bit will remain set until cleared by software writing 0.
		27		Package/Platform-Level PL2 Power Limiting Log
				When set, indicates that the Package or Platform Level PL2/PL3 Power Limiting Status bit has asserted since the log bit was last cleared.
				This log bit will remain set until cleared by software writing 0.
		28		Max Turbo Limit Log
				When set, indicates that the Max Turbo Limit Status bit has asserted since the log bit was last cleared.
				This log bit will remain set until cleared by software writing 0.
		29		Turbo Transition Attenuation Log
				When set, indicates that the Turbo Transition Attenuation Status bit has asserted since the log bit was last cleared.
				This log bit will remain set until cleared by software writing 0.
		63:30		Reserved
652H	1618	MSR_PKG_HDC_CONFIG	Package	HDC Configuration (R/W)

Table 2-39. Additional MSRs Supported by 6th Generation, 7th Generation, 8th Generation, 9th Generation, 10th Generation, 11th Generation, 12th Generation, and 13th Generation Intel® Core™ Processors, Intel® Xeon® Scalable Processor Family, 2nd, 3rd, and 4th Generation Intel® Xeon® Scalable Processor Family, 8th Generation Intel® Core™ i3 Processors, and Intel® Xeon® E Processors

	ister ress	Register Name / Bit Fields	Scope	Bit Description
Hex	Dec			
		2:0		PKG_Cx_Monitor Configures Package Cx state threshold for MSR_PKG_HDC_DEEP_RESIDENCY.
		63: 3		Reserved
653H	1619	MSR_CORE_HDC_RESIDENCY	Соге	Core HDC Idle Residency (R/O)
		63:0		Core_Cx_Duty_Cycle_Cnt
655H	1621	MSR_PKG_HDC_SHALLOW_RESIDENCY	Package	Accumulate the cycles the package was in C2 state and at least one logical processor was in forced idle (R/O)
		63:0		Pkg_C2_Duty_Cycle_Cnt
656H	1622	MSR_PKG_HDC_DEEP_RESIDENCY	Package	Package Cx HDC Idle Residency (R/O)
		63:0		Pkg_Cx_Duty_Cycle_Cnt
658H	1624	MSR_WEIGHTED_CORE_CO	Package	Core-count Weighted CO Residency (R/O)
		63:0		Increment at the same rate as the TSC. The increment each cycle is weighted by the number of processor cores in the package that reside in CO. If N cores are simultaneously in CO, then each cycle the counter increments by N.
659H	1625	MSR_ANY_CORE_CO	Package	Any Core CO Residency (R/O)
		63:0		Increment at the same rate as the TSC. The increment each cycle is one if any processor core in the package is in CO.
65AH	1626	MSR_ANY_GFXE_CO	Package	Any Graphics Engine CO Residency (R/O)
		63:0		Increment at the same rate as the TSC. The increment each cycle is one if any processor graphic device's compute engines are in CO.
65BH	1627	MSR_CORE_GFXE_OVERLAP_CO	Package	Core and Graphics Engine Overlapped CO Residency (R/O)
		63:0		Increment at the same rate as the TSC. The increment each cycle is one if at least one compute engine of the processor graphics is in CO and at least one processor core in the package is also in CO.
65CH	1628	MSR_PLATFORM_POWER_LIMIT	Platform	Platform Power Limit Control (R/W-L)
				Allows platform BIOS to limit power consumption of the platform devices to the specified values. The Long Duration power consumption is specified via Platform_Power_Limit_1 and Platform_Power_Limit_1_Time. The Short Duration power consumption limit is specified via the Platform_Power_Limit_2 with duration chosen by the processor. The processor implements an exponential-weighted algorithm in the placement of the time windows.

Table 2-39. Additional MSRs Supported by 6th Generation, 7th Generation, 8th Generation, 9th Generation, 10th Generation, 11th Generation, 12th Generation, and 13th Generation Intel® Core™ Processors, Intel® Xeon® Scalable Processor Family, 2nd, 3rd, and 4th Generation Intel® Xeon® Scalable Processor Family, 8th Generation Intel® Core™ i3 Processors, and Intel® Xeon® E Processors

Regi Addı		Register Name / Bit Fields	Scope	Bit Description
Hex	Dec			
		14:0		Platform Power Limit #1
				Average Power limit value which the platform must not exceed over a time window as specified by Power_Limit_1_TIME field.
				The default value is the Thermal Design Power (TDP) and varies with product skus. The unit is specified in MSR_RAPLPOWER_UNIT.
		15		Enable Platform Power Limit #1
				When set, enables the processor to apply control policy such that the platform power does not exceed Platform Power limit #1 over the time window specified by Power Limit #1 Time Window.
		16		Platform Clamping Limitation #1
				When set, allows the processor to go below the OS requested P states in order to maintain the power below specified Platform Power Limit #1 value.
				This bit is writeable only when CPUID (EAX=6):EAX[4] is set.
		23:17		Time Window for Platform Power Limit #1
				Specifies the duration of the time window over which Platform Power Limit 1 value should be maintained for sustained long duration. This field is made up of two numbers from the following equation:
				Time Window = (float) ((1+(X/4))*(2^Y)), where:
				X = POWER_LIMIT_1_TIME[23:22]
				Y = POWER_LIMIT_1_TIME[21:17]
				The maximum allowed value in this field is defined in MSR_PKG_POWER_INFO[PKG_MAX_WIN].
				The default value is ODH, and the unit is specified in MSR_RAPL_POWER_UNIT[Time Unit].
		31:24		Reserved
		46:32		Platform Power Limit #2
				Average Power limit value which the platform must not exceed over the Short Duration time window chosen by the processor.
				The recommended default value is 1.25 times the Long Duration Power Limit (i.e., Platform Power Limit # 1).
		47		Enable Platform Power Limit #2
				When set, enables the processor to apply control policy such that the platform power does not exceed Platform Power limit #2 over the Short Duration time window.

Table 2-39. Additional MSRs Supported by 6th Generation, 7th Generation, 8th Generation, 9th Generation, 10th Generation, 11th Generation, 12th Generation, and 13th Generation Intel® Core™ Processors, Intel® Xeon® Scalable Processor Family, 2nd, 3rd, and 4th Generation Intel® Xeon® Scalable Processor Family, 8th Generation Intel® Core™ i3 Processors, and Intel® Xeon® E Processors

	ister Iress	Register Name / Bit Fields	Scope	Bit Description
Hex	Dec			
		48		Platform Clamping Limitation #2
				When set, allows the processor to go below the OS requested P states in order to maintain the power below specified Platform Power Limit #2 value.
		62:49		Reserved
		63		Lock. Setting this bit will lock all other bits of this MSR until system RESET.
690H	1680	MSR_LASTBRANCH_16_FROM_IP	Thread	Last Branch Record 16 From IP (R/W)
				One of 32 triplets of last branch record registers on the last branch record stack. This part of the stack contains pointers to the source instruction. See also: Last Branch Record Stack TOS at 1C9H.
				Section 18.12.
691H	1681	MSR_LASTBRANCH_17_FROM_IP	Thread	Last Branch Record 17 From IP (R/W)
				See description of MSR_LASTBRANCH_0_FROM_IP.
692H	1682	MSR_LASTBRANCH_18_FROM_IP	Thread	Last Branch Record 18 From IP (R/W)
				See description of MSR_LASTBRANCH_0_FROM_IP.
693H	1683	MSR_LASTBRANCH_19_FROM_IP	Thread	Last Branch Record 19From IP (R/W)
				See description of MSR_LASTBRANCH_0_FROM_IP.
694H	1684	MSR_LASTBRANCH_20_FROM_IP	Thread	Last Branch Record 20 From IP (R/W)
				See description of MSR_LASTBRANCH_0_FROM_IP.
695H	1685	MSR_LASTBRANCH_21_FROM_IP	Thread	Last Branch Record 21 From IP (R/W)
COCII	1.000	MCD LACTED ANGLE 22 CDOM ID	TI I	See description of MSR_LASTBRANCH_0_FROM_IP.
696H	1686	MSR_LASTBRANCH_22_FROM_IP	Thread	Last Branch Record 22 From IP (R/W) See description of MSR_LASTBRANCH_0_FROM_IP.
697H	1687	MCD LACTEDANICIL 22 CDOM ID	Thread	
09/11	1007	MSR_LASTBRANCH_23_FROM_IP	meau	Last Branch Record 23 From IP (R/W) See description of MSR_LASTBRANCH_0_FROM_IP.
698H	1688	MSR_LASTBRANCH_24_FROM_IP	Thread	Last Branch Record 24 From IP (R/W)
03011	1000	I I I I I I I I I I I I I I I I I I I	IIIIeau	See description of MSR_LASTBRANCH_0_FROM_IP.
699H	1689	MSR_LASTBRANCH_25_FROM_IP	Thread	Last Branch Record 25 From IP (R/W)
03311	1003	TISK_CASTBRANCIN_ES_TROTI_	1111000	See description of MSR_LASTBRANCH_0_FROM_IP.
69AH	1690	MSR_LASTBRANCH_26_FROM_IP	Thread	Last Branch Record 26 From IP (R/W)
				See description of MSR_LASTBRANCH_0_FROM_IP.
69BH	1691	MSR_LASTBRANCH_27_FROM_IP	Thread	Last Branch Record 27 From IP (R/W)
				See description of MSR_LASTBRANCH_O_FROM_IP.
69CH	1692	MSR_LASTBRANCH_28_FROM_IP	Thread	Last Branch Record 28 From IP (R/W)
				See description of MSR_LASTBRANCH_0_FROM_IP.
	·	I	I	I .

Table 2-39. Additional MSRs Supported by 6th Generation, 7th Generation, 8th Generation, 9th Generation, 10th Generation, 11th Generation, 12th Generation, and 13th Generation Intel® Core™ Processors, Intel® Xeon® Scalable Processor Family, 2nd, 3rd, and 4th Generation Intel® Xeon® Scalable Processor Family, 8th Generation Intel® Core™ i3 Processors, and Intel® Xeon® E Processors

Regi Add		Register Name / Bit Fields	Scope	Bit Description
Hex	Dec			
69DH	1693	MSR_LASTBRANCH_29_FROM_IP	Thread	Last Branch Record 29 From IP (R/W) See description of MSR_LASTBRANCH_O_FROM_IP.
69EH	1694	MSR_LASTBRANCH_30_FROM_IP	Thread	Last Branch Record 30 From IP (R/W) See description of MSR_LASTBRANCH_0_FROM_IP.
69FH	1695	MSR_LASTBRANCH_31_FROM_IP	Thread	Last Branch Record 31 From IP (R/W) See description of MSR_LASTBRANCH_O_FROM_IP.
6B0H	1712	MSR_GRAPHICS_PERF_LIMIT_REASONS	Package	Indicator of Frequency Clipping in the Processor Graphics (R/W)
				(Frequency refers to processor graphics frequency.)
		0		PROCHOT Status (R0)
				When set, frequency is reduced due to assertion of external PROCHOT.
		1		Thermal Status (R0)
				When set, frequency is reduced due to a thermal event.
		4:2		Reserved.
		5		Running Average Thermal Limit Status (R0)
				When set, frequency is reduced due to running average thermal limit.
		6		VR Therm Alert Status (R0)
				When set, frequency is reduced due to a thermal alert from a processor Voltage Regulator.
		7		VR Thermal Design Current Status (R0)
				When set, frequency is reduced due to VR TDC limit.
		8		Other Status (R0)
				When set, frequency is reduced due to electrical or other constraints.
		9		Reserved
		10		Package/Platform-Level Power Limiting PL1 Status (R0)
				When set, frequency is reduced due to package/platform-level power limiting PL1.
		11		Package/Platform-Level PL2 Power Limiting Status (R0)
				When set, frequency is reduced due to package/platform-level power limiting PL2/PL3.
		12		Inefficient Operation Status (R0)
				When set, processor graphics frequency is operating below target frequency.
		15:13		Reserved

Table 2-39. Additional MSRs Supported by 6th Generation, 7th Generation, 8th Generation, 9th Generation, 10th Generation, 11th Generation, 12th Generation, and 13th Generation Intel® Core™ Processors, Intel® Xeon® Scalable Processor Family, 2nd, 3rd, and 4th Generation Intel® Xeon® Scalable Processor Family, 8th Generation Intel® Core™ i3 Processors, and Intel® Xeon® E Processors

Regi Add		Register Name / Bit Fields	Scope	Bit Description
Hex	Dec			
		16		PROCHOT Log
				When set, indicates that the PROCHOT Status bit has asserted since the log bit was last cleared.
				This log bit will remain set until cleared by software writing 0.
		17		Thermal Log
				When set, indicates that the Thermal Status bit has asserted since the log bit was last cleared.
				This log bit will remain set until cleared by software writing 0.
		20:18		Reserved.
		21		Running Average Thermal Limit Log
				When set, indicates that the RATL Status bit has asserted since the log bit was last cleared.
				This log bit will remain set until cleared by software writing 0.
		22		VR Therm Alert Log
				When set, indicates that the VR Therm Alert Status bit has asserted since the log bit was last cleared.
				This log bit will remain set until cleared by software writing 0.
		23		VR Thermal Design Current Log
				When set, indicates that the VR Therm Alert Status bit has asserted since the log bit was last cleared.
				This log bit will remain set until cleared by software writing 0.
		24		Other Log
				When set, indicates that the OTHER Status bit has asserted since the log bit was last cleared.
				This log bit will remain set until cleared by software writing 0.
		25		Reserved
		26		Package/Platform-Level PL1 Power Limiting Log
				When set, indicates that the Package/Platform Level PL1 Power Limiting Status bit has asserted since the log bit was last cleared.
				This log bit will remain set until cleared by software writing 0.

Table 2-39. Additional MSRs Supported by 6th Generation, 7th Generation, 8th Generation, 9th Generation, 10th Generation, 11th Generation, 12th Generation, and 13th Generation Intel® Core™ Processors, Intel® Xeon® Scalable Processor Family, 2nd, 3rd, and 4th Generation Intel® Xeon® Scalable Processor Family, 8th Generation Intel® Core™ i3 Processors, and Intel® Xeon® E Processors

	ister ress	Register Name / Bit Fields	Scope	Bit Description
Hex	Dec			
		27		Package/Platform-Level PL2 Power Limiting Log
				When set, indicates that the Package/Platform Level PL2 Power Limiting Status bit has asserted since the log bit was last cleared.
				This log bit will remain set until cleared by software writing 0.
		28		Inefficient Operation Log
				When set, indicates that the Inefficient Operation Status bit has asserted since the log bit was last cleared.
				This log bit will remain set until cleared by software writing 0.
		63:29		Reserved
6B1H	1713	MSR_RING_PERF_LIMIT_REASONS	Package	Indicator of Frequency Clipping in the Ring Interconnect (R/W)
				(Frequency refers to ring interconnect in the uncore.)
		0		PROCHOT Status (R0)
				When set, frequency is reduced due to assertion of external PROCHOT.
		1		Thermal Status (R0)
				When set, frequency is reduced due to a thermal event.
		4:2		Reserved
		5		Running Average Thermal Limit Status (R0)
				When set, frequency is reduced due to running average thermal limit.
		6		VR Therm Alert Status (R0)
				When set, frequency is reduced due to a thermal alert from a processor Voltage Regulator.
		7		VR Thermal Design Current Status (R0)
				When set, frequency is reduced due to VR TDC limit.
		8		Other Status (R0)
				When set, frequency is reduced due to electrical or other constraints.
		9		Reserved
		10		Package/Platform-Level Power Limiting PL1 Status (R0)
				When set, frequency is reduced due to package/Platform-level power limiting PL1.

Table 2-39. Additional MSRs Supported by 6th Generation, 7th Generation, 8th Generation, 9th Generation, 10th Generation, 11th Generation, 12th Generation, and 13th Generation Intel® Core™ Processors, Intel® Xeon® Scalable Processor Family, 2nd, 3rd, and 4th Generation Intel® Xeon® Scalable Processor Family, 8th Generation Intel® Core™ i3 Processors, and Intel® Xeon® E Processors

	ister ress	Register Name / Bit Fields	Scope	Bit Description
Hex	Dec			
		11		Package/Platform-Level PL2 Power Limiting Status (R0)
				When set, frequency is reduced due to package/Platform-level power limiting PL2/PL3.
		15:12		Reserved
		16		PROCHOT Log
				When set, indicates that the PROCHOT Status bit has asserted since the log bit was last cleared.
				This log bit will remain set until cleared by software writing 0.
		17		Thermal Log
				When set, indicates that the Thermal Status bit has asserted since the log bit was last cleared.
				This log bit will remain set until cleared by software writing 0.
		20:18		Reserved
		21		Running Average Thermal Limit Log
				When set, indicates that the RATL Status bit has asserted since the log bit was last cleared.
				This log bit will remain set until cleared by software writing 0.
		22		VR Therm Alert Log
				When set, indicates that the VR Therm Alert Status bit has asserted since the log bit was last cleared.
				This log bit will remain set until cleared by software writing 0.
		23		VR Thermal Design Current Log
				When set, indicates that the VR Therm Alert Status bit has asserted since the log bit was last cleared.
				This log bit will remain set until cleared by software writing 0.
		24		Other Log
				When set, indicates that the OTHER Status bit has asserted since the log bit was last cleared.
				This log bit will remain set until cleared by software writing 0.
		25		Reserved

Table 2-39. Additional MSRs Supported by 6th Generation, 7th Generation, 8th Generation, 9th Generation, 10th Generation, 11th Generation, 12th Generation, and 13th Generation Intel® Core™ Processors, Intel® Xeon® Scalable Processor Family, 2nd, 3rd, and 4th Generation Intel® Xeon® Scalable Processor Family, 8th Generation Intel® Core™ i3 Processors, and Intel® Xeon® E Processors

	ister ress	Register Name / Bit Fields	Scope	Bit Description
Hex	Dec			
		26		Package/Platform-Level PL1 Power Limiting Log When set, indicates that the Package/Platform Level PL1 Power Limiting Status bit has asserted since the log bit was last cleared. This log bit will remain set until cleared by software
				writing 0.
		27		Package/Platform-Level PL2 Power Limiting Log
				When set, indicates that the Package/Platform Level PL2 Power Limiting Status bit has asserted since the log bit was last cleared.
				This log bit will remain set until cleared by software writing 0.
		63:28		Reserved
6D0H	1744	MSR_LASTBRANCH_16_TO_IP	Thread	Last Branch Record 16 To IP (R/W)
				One of 32 triplets of last branch record registers on the last branch record stack. This part of the stack contains pointers to the destination instruction. See also:
				Last Branch Record Stack TOS at 1C9H.Section 18.12.
6D1H	1745	MSR_LASTBRANCH_17_TO_IP	Thread	Last Branch Record 17 To IP (R/W)
				See description of MSR_LASTBRANCH_0_T0_IP.
6D2H	1746	MSR_LASTBRANCH_18_TO_IP	Thread	Last Branch Record 18 To IP (R/W)
				See description of MSR_LASTBRANCH_0_TO_IP.
6D3H	1747	MSR_LASTBRANCH_19_TO_IP	Thread	Last Branch Record 19To IP (R/W)
60.411	4740	MOD LASTED ANGLESS TO JE		See description of MSR_LASTBRANCH_0_TO_IP.
6D4H	1748	MSR_LASTBRANCH_20_TO_IP	Thread	Last Branch Record 20 To IP (R/W) See description of MSR_LASTBRANCH_0_T0_IP.
6D5H	1749	MSR_LASTBRANCH_21_TO_IP	Thread	Last Branch Record 21 To IP (R/W)
ODSIT	1743	TISIC_CAST BIKANCIT_2 I_10_II	Tillead	See description of MSR_LASTBRANCH_0_T0_IP.
6D6H	1750	MSR_LASTBRANCH_22_TO_IP	Thread	Last Branch Record 22 To IP (R/W)
				See description of MSR_LASTBRANCH_0_T0_IP.
6D7H	1751	MSR_LASTBRANCH_23_TO_IP	Thread	Last Branch Record 23 To IP (R/W)
				See description of MSR_LASTBRANCH_0_T0_IP.
6D8H	1752	MSR_LASTBRANCH_24_TO_IP	Thread	Last Branch Record 24 To IP (R/W)
				See description of MSR_LASTBRANCH_0_TO_IP.
6D9H	1753	MSR_LASTBRANCH_25_TO_IP	Thread	Last Branch Record 25 To IP (R/W)
				See description of MSR_LASTBRANCH_0_T0_IP.
6DAH	1754	MSR_LASTBRANCH_26_TO_IP	Thread	Last Branch Record 26 To IP (R/W)
				See description of MSR_LASTBRANCH_0_T0_IP.

Table 2-39. Additional MSRs Supported by 6th Generation, 7th Generation, 8th Generation, 9th Generation, 10th Generation, 11th Generation, 12th Generation, and 13th Generation Intel® Core™ Processors, Intel® Xeon® Scalable Processor Family, 2nd, 3rd, and 4th Generation Intel® Xeon® Scalable Processor Family, 8th Generation Intel® Core™ i3 Processors, and Intel® Xeon® E Processors

	ister ress	Register Name / Bit Fields	Scope	Bit Description
Hex	Dec			
6DBH	1755	MSR_LASTBRANCH_27_TO_IP	Thread	Last Branch Record 27 To IP (R/W)
				See description of MSR_LASTBRANCH_0_T0_IP.
6DCH	1756	MSR_LASTBRANCH_28_TO_IP	Thread	Last Branch Record 28 To IP (R/W)
				See description of MSR_LASTBRANCH_0_T0_IP.
6DDH	1757	MSR_LASTBRANCH_29_TO_IP	Thread	Last Branch Record 29 To IP (R/W)
				See description of MSR_LASTBRANCH_0_T0_IP.
6DEH	1758	MSR_LASTBRANCH_30_TO_IP	Thread	Last Branch Record 30 To IP (R/W)
SDSU	4750	MOD / AGTED ANGL. 24 TO 15		See description of MSR_LASTBRANCH_0_TO_IP.
6DFH	1759	MSR_LASTBRANCH_31_TO_IP	Thread	Last Branch Record 31 To IP (R/W)
77011	1004	IA22 DM CNADIC	Dealtese	See description of MSR_LASTBRANCH_0_T0_IP.
770H	1904	IA32_PM_ENABLE	Package	See Section 15.4.2, "Enabling HWP."
771H	1905	IA32_HWP_CAPABILITIES	Thread	See Section 15.4.3, "HWP Performance Range and Dynamic Capabilities."
772H	1906	IA32_HWP_REQUEST_PKG	Package	See Section 15.4.4, "Managing HWP."
773H	1907	IA32_HWP_INTERRUPT	Thread	See Section 15.4.6, "HWP Notifications."
774H	1908	IA32_HWP_REQUEST	Thread	See Section 15.4.4, "Managing HWP."
		7:0		Minimum Performance (R/W)
		15:8		Maximum Performance (R/W)
		23:16		Desired Performance (R/W)
		31:24		Energy/Performance Preference (R/W)
		41:32		Activity Window (R/W)
		42		Package Control (R/W)
		63:43		Reserved
777H	1911	IA32_HWP_STATUS	Thread	See Section 15.4.5, "HWP Feedback."
D90H	3472	IA32_BNDCFGS	Thread	See Table 2-2.
DAOH	3488	IA32_XSS	Thread	See Table 2-2.
DB0H	3504	IA32_PKG_HDC_CTL	Package	See Section 15.5.2, "Package level Enabling HDC."
DB1H	3505	IA32_PM_CTL1	Thread	See Section 15.5.3, "Logical-Processor Level HDC Control."
DB2H	3506	IA32_THREAD_STALL	Thread	See Section 15.5.4.1, "IA32_THREAD_STALL."
DCOH	3520	MSR_LBR_INFO_0	Thread	Last Branch Record O Additional Information (R/W)
				One of 32 triplet of last branch record registers on the last branch record stack. This part of the stack contains flag, TSX-related and elapsed cycle information. See also:
				Last Branch Record Stack TOS at 1C9H.Section 18.9.1, "LBR Stack."

Table 2-39. Additional MSRs Supported by 6th Generation, 7th Generation, 8th Generation, 9th Generation, 10th Generation, 11th Generation, 12th Generation, and 13th Generation Intel® Core™ Processors, Intel® Xeon® Scalable Processor Family, 2nd, 3rd, and 4th Generation Intel® Xeon® Scalable Processor Family, 8th Generation Intel® Core™ i3 Processors, and Intel® Xeon® E Processors

Register Address		Register Name / Bit Fields	Scope	Bit Description
Hex	Dec			
DC1H	3521	MSR_LBR_INFO_1	Thread	Last Branch Record 1 Additional Information (R/W) See description of MSR_LBR_INFO_0.
DC2H	3522	MSR_LBR_INFO_2	Thread	Last Branch Record 2 Additional Information (R/W) See description of MSR_LBR_INFO_0.
DC3H	3523	MSR_LBR_INFO_3	Thread	Last Branch Record 3 Additional Information (R/W) See description of MSR_LBR_INFO_0.
DC4H	3524	MSR_LBR_INFO_4	Thread	Last Branch Record 4 Additional Information (R/W) See description of MSR_LBR_INFO_0.
DC5H	3525	MSR_LBR_INFO_5	Thread	Last Branch Record 5 Additional Information (R/W) See description of MSR_LBR_INFO_0.
DC6H	3526	MSR_LBR_INFO_6	Thread	Last Branch Record 6 Additional Information (R/W) See description of MSR_LBR_INFO_0.
DC7H	3527	MSR_LBR_INFO_7	Thread	Last Branch Record 7 Additional Information (R/W) See description of MSR_LBR_INFO_0.
DC8H	3528	MSR_LBR_INFO_8	Thread	Last Branch Record 8 Additional Information (R/W) See description of MSR_LBR_INFO_0.
DC9H	3529	MSR_LBR_INFO_9	Thread	Last Branch Record 9 Additional Information (R/W) See description of MSR_LBR_INFO_0.
DCAH	3530	MSR_LBR_INFO_10	Thread	Last Branch Record 10 Additional Information (R/W) See description of MSR_LBR_INFO_0.
DCBH	3531	MSR_LBR_INFO_11	Thread	Last Branch Record 11 Additional Information (R/W) See description of MSR_LBR_INFO_0.
DCCH	3532	MSR_LBR_INFO_12	Thread	Last Branch Record 12 Additional Information (R/W) See description of MSR_LBR_INFO_0.
DCDH	3533	MSR_LBR_INFO_13	Thread	Last Branch Record 13 Additional Information (R/W) See description of MSR_LBR_INFO_0.
DCEH	3534	MSR_LBR_INFO_14	Thread	Last Branch Record 14 Additional Information (R/W) See description of MSR_LBR_INFO_0.
DCFH	3535	MSR_LBR_INFO_15	Thread	Last Branch Record 15 Additional Information (R/W) See description of MSR_LBR_INFO_0.
DDOH	3536	MSR_LBR_INFO_16	Thread	Last Branch Record 16 Additional Information (R/W) See description of MSR_LBR_INFO_0.
DD1H	3537	MSR_LBR_INFO_17	Thread	Last Branch Record 17 Additional Information (R/W) See description of MSR_LBR_INFO_0.
DD2H	3538	MSR_LBR_INFO_18	Thread	Last Branch Record 18 Additional Information (R/W) See description of MSR_LBR_INFO_0.

Table 2-39. Additional MSRs Supported by 6th Generation, 7th Generation, 8th Generation, 9th Generation, 10th Generation, 11th Generation, 12th Generation, and 13th Generation Intel® Core™ Processors, Intel® Xeon® Scalable Processor Family, 2nd, 3rd, and 4th Generation Intel® Xeon® Scalable Processor Family, 8th Generation Intel® Core™ i3 Processors, and Intel® Xeon® E Processors

	ister ress	Register Name / Bit Fields	Scope	Bit Description
Hex	Dec			
DD3H	3539	MSR_LBR_INFO_19	Thread	Last Branch Record 19 Additional Information (R/W)
				See description of MSR_LBR_INFO_0.
DD4H	3540	MSR_LBR_INFO_20	Thread	Last Branch Record 20 Additional Information (R/W)
				See description of MSR_LBR_INFO_0.
DD5H	3541	MSR_LBR_INFO_21	Thread	Last Branch Record 21 Additional Information (R/W)
				See description of MSR_LBR_INFO_0.
DD6H	3542	MSR_LBR_INFO_22	Thread	Last Branch Record 22 Additional Information (R/W)
				See description of MSR_LBR_INFO_0.
DD7H	3543	MSR_LBR_INFO_23	Thread	Last Branch Record 23 Additional Information (R/W)
				See description of MSR_LBR_INFO_0.
DD8H	3544	MSR_LBR_INFO_24	Thread	Last Branch Record 24 Additional Information (R/W)
				See description of MSR_LBR_INFO_0.
DD9H	3545	MSR_LBR_INFO_25	Thread	Last Branch Record 25 Additional Information (R/W)
				See description of MSR_LBR_INFO_0.
DDAH	3546	MSR_LBR_INFO_26	Thread	Last Branch Record 26 Additional Information (R/W)
				See description of MSR_LBR_INFO_0.
DDBH	3547	MSR_LBR_INFO_27	Thread	Last Branch Record 27 Additional Information (R/W)
				See description of MSR_LBR_INFO_0.
DDCH	3548	MSR_LBR_INFO_28	Thread	Last Branch Record 28 Additional Information (R/W)
				See description of MSR_LBR_INFO_0.
DDDH	3549	MSR_LBR_INFO_29	Thread	Last Branch Record 29 Additional Information (R/W)
				See description of MSR_LBR_INFO_0.
DDEH	3550	MSR_LBR_INFO_30	Thread	Last Branch Record 30 Additional Information (R/W)
				See description of MSR_LBR_INFO_0.
DDFH	3551	MSR_LBR_INFO_31	Thread	Last Branch Record 31 Additional Information (R/W)
				See description of MSR_LBR_INFO_0.

Table 2-40 lists the MSRs of uncore PMU for Intel processors with a CPUID Signature DisplayFamily_DisplayModel value of 06_4EH, 06_5EH, 06_8EH, 06_9EH, or 06_66H.

Table 2-40. Uncore PMU MSRs Supported by 6th Generation, 7th Generation, and 8th Generation Intel® Core™ Processors, and 8th generation Intel® Core™ i3 Processors

Regi Add		Register Name / Bit Fields	Scope	Bit Description
Hex	Dec			
394H	916	MSR_UNC_PERF_FIXED_CTRL	Package	Uncore Fixed Counter Control (R/W)
		19:0		Reserved
		20		Enable overflow propagation.

Table 2-40. Uncore PMU MSRs Supported by 6th Generation, 7th Generation, and 8th Generation Intel® Core™ Processors, and 8th generation Intel® Core™ i3 Processors

_	ister ress	Register Name / Bit Fields	Scope	Bit Description
Hex	Dec			
		21		Reserved
		22		Enable counting.
		63:23		Reserved
395H	917	MSR_UNC_PERF_FIXED_CTR	Package	Uncore Fixed Counter
		43:0		Current count.
		63:44		Reserved
396H	918	MSR_UNC_CBO_CONFIG	Package	Uncore C-Box Configuration Information (R/O)
		3:0		Specifies the number of C-Box units with programmable counters (including processor cores and processor graphics).
		63:4		Reserved
3B0H	946	MSR_UNC_ARB_PERFCTR0	Package	Uncore Arb Unit, Performance Counter 0
3B1H	947	MSR_UNC_ARB_PERFCTR1	Package	Uncore Arb Unit, Performance Counter 1
3B2H	944	MSR_UNC_ARB_PERFEVTSEL0	Package	Uncore Arb Unit, Counter 0 Event Select MSR
3B3H	945	MSR_UNC_ARB_PERFEVTSEL1	Package	Uncore Arb Unit, Counter 1 Event Select MSR
700H	1792	MSR_UNC_CBO_0_PERFEVTSEL0	Package	Uncore C-Box 0, Counter 0 Event Select MSR
701H	1793	MSR_UNC_CBO_0_PERFEVTSEL1	Package	Uncore C-Box O, Counter 1 Event Select MSR
706H	1798	MSR_UNC_CBO_0_PERFCTR0	Package	Uncore C-Box O, Performance Counter O
707H	1799	MSR_UNC_CBO_0_PERFCTR1	Package	Uncore C-Box O, Performance Counter 1
710H	1808	MSR_UNC_CBO_1_PERFEVTSELO	Package	Uncore C-Box 1, Counter 0 Event Select MSR
711H	1809	MSR_UNC_CBO_1_PERFEVTSEL1	Package	Uncore C-Box 1, Counter 1 Event Select MSR
716H	1814	MSR_UNC_CBO_1_PERFCTRO	Package	Uncore C-Box 1, Performance Counter 0
717H	1815	MSR_UNC_CBO_1_PERFCTR1	Package	Uncore C-Box 1, Performance Counter 1
720H	1824	MSR_UNC_CBO_2_PERFEVTSELO	Package	Uncore C-Box 2, Counter 0 Event Select MSR
721H	1825	MSR_UNC_CBO_2_PERFEVTSEL1	Package	Uncore C-Box 2, Counter 1 Event Select MSR
726H	1830	MSR_UNC_CBO_2_PERFCTRO	Package	Uncore C-Box 2, Performance Counter 0
727H	1831	MSR_UNC_CBO_2_PERFCTR1	Package	Uncore C-Box 2, Performance Counter 1
730H	1840	MSR_UNC_CBO_3_PERFEVTSELO	Package	Uncore C-Box 3, Counter 0 Event Select MSR
731H	1841	MSR_UNC_CBO_3_PERFEVTSEL1	Package	Uncore C-Box 3, Counter 1 Event Select MSR
736H	1846	MSR_UNC_CBO_3_PERFCTRO	Package	Uncore C-Box 3, Performance Counter 0
737H	1847	MSR_UNC_CBO_3_PERFCTR1	Package	Uncore C-Box 3, Performance Counter 1
E01H	3585	MSR_UNC_PERF_GLOBAL_CTRL	Package	Uncore PMU Global Control
		0		Slice 0 select.
		1		Slice 1 select.
		2		Slice 2 select.
		3		Slice 3 select.
		4		Slice 4select.

Table 2-40. Uncore PMU MSRs Supported by 6th Generation, 7th Generation, and 8th Generation Intel® Core™ Processors, and 8th generation Intel® Core™ i3 Processors

_	ister ress	Register Name / Bit Fields	Scope	Bit Description
Hex	Dec			
		18:5		Reserved
		29		Enable all uncore counters.
		30		Enable wake on PMI.
		31		Enable Freezing counter when overflow.
		63:32		Reserved
E02H	3586	MSR_UNC_PERF_GLOBAL_STATUS	Package	Uncore PMU Main Status
		0		Fixed counter overflowed.
		1		An ARB counter overflowed.
		2		Reserved
		3		A CBox counter overflowed (on any slice).
		63:4		Reserved

2.17.1 MSRs Introduced in 7th Generation and 8th Generation Intel® Core™ Processors Based on Kaby Lake Microarchitecture and Coffee Lake Microarchitecture

Table 2-41 lists additional MSRs for 7th generation and 8th generation Intel Core processors with a CPUID Signature DisplayFamily_DisplayModel value of 06_8EH or 06_9EH. For an MSR listed in Table 2-41 that also appears in the model-specific tables of prior generations, Table 2-41 supersedes prior generation tables.

Table 2-41. Additional MSRs Supported by the 7th Generation and 8th Generation Intel® Core™ Processors Based on Kaby Lake Microarchitecture and Coffee Lake Microarchitecture

Register Address		Register Name / Bit Fields	Scope	Bit Description
Hex	Dec			
80H	128	MSR_TRACE_HUB_STH_ACPIBAR_BASE	Package	NPK Address Used by AET Messages (R/W)
		0		Lock Bit
				If set, this MSR cannot be re-written anymore. Lock bit has to be set in order for the AET packets to be directed to NPK MMIO.
		17:1		Reserved
		63:18		ACPIBAR_BASE_ADDRESS
				AET target address in NPK MMIO space.
1F4H	500	MSR_PRMRR_PHYS_BASE	Core	Processor Reserved Memory Range Register - Physical Base Control Register (R/W)
		2:0		MemType
				PRMRR BASE MemType.
		11:3		Reserved
		45:12		Base
				PRMRR Base Address.
		63:46		Reserved

Table 2-41. Additional MSRs Supported by the 7th Generation and 8th Generation Intel® Core™ Processors Based on Kaby Lake Microarchitecture and Coffee Lake Microarchitecture (Contd.)

Regi Add		Register Name / Bit Fields	Scope	Bit Description
Hex	Dec			
1F5H	501	MSR_PRMRR_PHYS_MASK	Core	Processor Reserved Memory Range Register - Physical Mask Control Register (R/W)
		9:0		Reserved
		10		Lock
				Lock bit for the PRMRR.
		11		VLD
				Enable bit for the PRMRR.
		45:12		Mask
				PRMRR MASK bits.
1.50.1	507	63:46	6	Reserved
1FBH	507	MSR_PRMRR_VALID_CONFIG	Соге	Valid PRMRR Configurations (R/W)
		0		1M supported MEE size.
		4:1		Reserved
		5		32M supported MEE size.
		6		64M supported MEE size.
		7		128M supported MEE size.
		31:8		Reserved
2F4H	756	MSR_UNCORE_PRMRR_PHYS_BASE ¹	Package	(R/W)
				The PRMRR range is used to protect the processor reserved memory from unauthorized reads and writes. Any IO access to this range is aborted. This register controls the location of the PRMRR range by indicating its starting address. It functions in tandem with the PRMRR mask register.
		11:0		Reserved
		PAWIDTH-1:12		Range Base
				This field corresponds to bits PAWIDTH-1:12 of the base address memory range which is allocated to PRMRR memory.
		63:PAWIDTH		Reserved
2F5H	757	MSR_UNCORE_PRMRR_PHYS_MASK ¹	Package	(R/W)
				This register controls the size of the PRMRR range by indicating which address bits must match the PRMRR base register value.
		9:0		Reserved
		10		Lock
				Setting this bit locks all writeable settings in this register, including itself.
		11		Range_En Indicates whether the PRMRR range is enabled and valid.

Table 2-41. Additional MSRs Supported by the 7th Generation and 8th Generation Intel® Core™ Processors Based on Kaby Lake Microarchitecture and Coffee Lake Microarchitecture (Contd.)

_	ister ress	Register Name / Bit Fields	Scope	Bit Description
Hex	Dec			
		38:12		Range_Mask
				This field indicates which address bits must match PRMRR base in order to qualify as an PRMRR access.
		63:39		Reserved
620H	1568	MSR_RING_RATIO_LIMIT	Package	Ring Ratio Limit (R/W)
				This register provides Min/Max Ratio Limits for the LLC and Ring.
		6:0		MAX_Ratio
				This field is used to limit the max ratio of the LLC/Ring.
		7		Reserved
		14:8		MIN_Ratio
				Writing to this field controls the minimum possible ratio of the LLC/Ring.
		63:15		Reserved

NOTES:

2.17.2 MSRs Specific to 8th Generation Intel® Core™ i3 Processors

Table 2-42 lists additional MSRs for 8th generation Intel Core i3 processors with a CPUID Signature DisplayFamily_DisplayModel value of 06_66H. For an MSR listed in Table 2-42 that also appears in the model-specific tables of prior generations, Table 2-42 supersede prior generation tables.

Table 2-42. Additional MSRs Supported by 8th Generation Intel® Core™ i3 Processors Based on Cannon Lake Microarchitecture

Register Address		Register Name / Bit Fields	Scope	Bit Description
Hex	Dec			
ЗАН	58	IA32_FEATURE_CONTROL	Thread	Control Features in Intel 64 Processor (R/W)
				See Table 2-2.
		0		Lock (R/WL)
		1		Enable VMX Inside SMX Operation (R/WL)
		2		Enable VMX Outside SMX Operation (R/WL)
		14:8		SENTER Local Functions Enables (R/WL)
		15		SENTER Global Functions Enable (R/WL)

^{1.} This MSR is specific to 7th generation and 8th generation Intel® Core™ processors.

Table 2-42. Additional MSRs Supported by 8th Generation Intel® Core™ i3 Processors Based on Cannon Lake Microarchitecture (Contd.)

	ister Iress	Register Name / Bit Fields	Scope	Bit Description
Hex	Dec			
		17		SGX Launch Control Enable (R/WL) This bit must be set to enable runtime reconfiguration of SGX Launch Control via IA32_SGXLEPUBKEYHASHN MSR. Available only if CPUID.(EAX=07H, ECX=0H): ECX[30]
		12		= 1.
		18		SGX Global Functions Enable (R/WL)
		63:21		Reserved
350H	848	MSR_BR_DETECT_CTRL		Branch Monitoring Global Control (R/W)
		0		EnMonitoring Global enable for branch monitoring.
		1		EnExcept Enable branch monitoring event signaling on threshold trip. The branch monitoring event handler is signaled via the existing PMI signaling mechanism as programmed from the corresponding local APIC LVT entry.
		2		EnLBRFrz Enable LBR freeze on threshold trip. This will cause the LBR frozen bit 58 to be set in IA32_PERF_GLOBAL_STATUS when a triggering condition occurs and this bit is enabled.
		3		DisableInGuest
				When set to '1', branch monitoring, event triggering and LBR freeze actions are disabled when operating at VMX non-root operation.
		7:4		Reserved
		17:8		WindowSize
				Window size defined by WindowCntSel. Values 0 - 1023 are supported.
				Once the Window counter reaches the WindowSize count both the Window Counter and all Branch Monitoring Counters are cleared.
		23:18		Reserved
		25:24		WindowCntSel
				Window event count select:
				'00 = Instructions retired.
				'01 = Branch instructions retired
				'10 = Return instructions retired.
				'11 = Indirect branch instructions retired.

Table 2-42. Additional MSRs Supported by 8th Generation Intel® Core™ i3 Processors

Based on Cannon Lake Microarchitecture (Contd.)

Regi Add		Register Name / Bit Fields	Scope	Bit Description
Hex	Dec			
		26		CntAndMode
				When set to '1', the overall branch monitoring event triggering condition is true only if all enabled counters' threshold conditions are true.
				When '0', the threshold tripping condition is true if any enabled counters' threshold is true.
		63:27		Reserved
351H	849	MSR_BR_DETECT_STATUS		Branch Monitoring Global Status (R/W)
		0		Branch Monitoring Event Signaled
				When set to '1', Branch Monitoring event signaling is blocked until this bit is cleared by software.
		1		LBRsValid
				This status bit is set to '1' if the LBR state is considered valid for sampling by branch monitoring software.
		7:2		Reserved
		8		CntrHit0
				Branch monitoring counter #0 threshold hit. This status bit is sticky and once set requires clearing by software. Counter operation continues independent of the state of the bit.
		9		CntrHit1
				Branch monitoring counter #1 threshold hit. This status bit is sticky and once set requires clearing by software. Counter operation continues independent of the state of the bit.
		15:10		Reserved
				Reserved for additional branch monitoring counters threshold hit status.
		25:16		CountWindow
				The current value of the window counter. The count value is frozen on a valid branch monitoring triggering condition. This is a 10-bit unsigned value.
		31:26		Reserved
				Reserved for future extension of CountWindow.

Table 2-42. Additional MSRs Supported by 8th Generation Intel® Core™ i3 Processors Based on Cannon Lake Microarchitecture (Contd.)

	ister ress	Register Name / Bit Fields	Scope	Bit Description	
Hex	Dec				
		39:32		Count0 The current value of counter 0 updated after each occurrence of the event being counted. The count value is frozen on a valid branch monitoring triggering condition (in which case CntrHit0 will also be set). This is an 8-bit signed value (2's complement). Heuristic events which only increment will saturate and freeze at maximum value 0xFF (256). RET-CALL event counter saturate at maximum value	
		47:40		Ox7F (+127) and minimum value 0x80 (-128). Count1 The current value of counter 1 updated after each occurrence of the event being counted. The count value is frozen on a valid branch monitoring triggering condition (in which case CntrHit1 will also be set). This is an 8-bit signed value (2's complement). Heuristic events which only increment will saturate	
		63:48		and freeze at maximum value 0xFF (256). RET-CALL event counter saturate at maximum value 0x7F (+127) and minimum value 0x80 (-128). Reserved	
354H - 355H	852 - 853	MSR_BR_DETECT_COUNTER_CONFIG_i		Branch Monitoring Detect Counter Configuration (R/W)	
		0		CntrEn Enable counter.	
		7:1		CntrEvSel Event select (other values #GP) '0000000 = RETs. '0000001 = RET-CALL bias. '0000010 = RET mispredicts. '0000011 = Branch (all) mispredicts. '0000100 = Indirect branch mispredicts. '0000101 = Far branch instructions.	
		14:8		CntrThreshold Threshold (an unsigned value of 0 to 127 supported). The value 0 of counter threshold will result in event signaled after every instruction. #GP if threshold is < 2.	

Table 2-42. Additional MSRs Supported by 8th Generation Intel® Core™ i3 Processors Based on Cannon Lake Microarchitecture (Contd.)

Regi Addı		Register Name / Bit Fields	Scope	Bit Description
Hex	Dec			
		15		MispredEventCnt
				Mispredict events counting behavior:
				'0 = Mispredict events are counted in a window.
				'1 = Mispredict events are counted based on a consecutive occurrence. CntrThreshold is treated as # of consecutive mispredicts. This control bit only applies to events specified by CntrEvSel that involve a prediction (0000010, 0000011, 0000100). Setting this bit for other events is ignored.
		63:16		Reserved
3F8H	1016	MSR_PKG_C3_RESIDENCY	Package	Package C3 Residency Counter (R/O)
		63:0		Note: C-state values are processor specific C-state code names, unrelated to MWAIT extension C-state parameters or ACPI C-states.
620H	1568	MSR_RING_RATIO_LIMIT	Package	Ring Ratio Limit (R/W)
				This register provides Min/Max Ratio Limits for the LLC and Ring.
		6:0		MAX_Ratio
				This field is used to limit the max ratio of the LLC/Ring.
		7		Reserved
		14:8		MIN_Ratio
				Writing to this field controls the minimum possible ratio of the LLC/Ring.
		63:15		Reserved
660H	1632	MSR_CORE_C1_RESIDENCY	Соге	Core C1 Residency Counter (R/O)
		63:0		Value since last reset for the Core C1 residency. Counter rate is the Max Non-Turbo frequency (same as TSC). This counter counts in case both of the core's threads are in an idle state and at least one of the core's thread residency is in a C1 state or in one of its sub states. The counter is updated only after a core C state exit. Note: Always reads 0 if core C1 is unsupported. A value of zero indicates that this processor does not support core C1 or never entered core C1 level state.
662H	1634	MSR_CORE_C3_RESIDENCY	Core	Core C3 Residency Counter (R/O)
		63:0		Will always return 0.

Table 2-43 lists the MSRs of uncore PMU for Intel processors with a CPUID Signature DisplayFamily_DisplayModel value of 06_66H .

Table 2-43. Uncore PMU MSRs Supported by Intel® Core™ Processors Based on Cannon Lake Microarchitecture

Register Address		Register Name / Bit Fields	Scope	Bit Description
Hex	Dec			
394H	916	MSR_UNC_PERF_FIXED_CTRL	Package	Uncore Fixed Counter Control (R/W)
		19:0		Reserved
		20		Enable overflow propagation.
		21		Reserved
		22		Enable counting.
		63:23		Reserved
395H	917	MSR_UNC_PERF_FIXED_CTR	Package	Uncore Fixed Counter
		47:0		Current count.
		63:48		Reserved
396H	918	MSR_UNC_CBO_CONFIG	Package	Uncore C-Box Configuration Information (R/O)
		3:0		Report the number of C-Box units with performance counters, including processor cores and processor graphics.
		63:4		Reserved
3B0H	946	MSR_UNC_ARB_PERFCTR0	Package	Uncore Arb Unit, Performance Counter 0
3B1H	947	MSR_UNC_ARB_PERFCTR1	Package	Uncore Arb Unit, Performance Counter 1
3B2H	944	MSR_UNC_ARB_PERFEVTSEL0	Package	Uncore Arb Unit, Counter O Event Select MSR
3B3H	945	MSR_UNC_ARB_PERFEVTSEL1	Package	Uncore Arb unit, Counter 1 Event Select MSR
700H	1792	MSR_UNC_CBO_0_PERFEVTSEL0	Package	Uncore C-Box 0, Counter 0 Event Select MSR
701H	1793	MSR_UNC_CBO_0_PERFEVTSEL1	Package	Uncore C-Box 0, Counter 1 Event Select MSR
702H	1794	MSR_UNC_CBO_0_PERFCTR0	Package	Uncore C-Box 0, Performance Counter 0
703H	1795	MSR_UNC_CBO_0_PERFCTR1	Package	Uncore C-Box O, Performance Counter 1
708H	1800	MSR_UNC_CBO_1_PERFEVTSELO	Package	Uncore C-Box 1, Counter 0 Event Select MSR
709H	1801	MSR_UNC_CBO_1_PERFEVTSEL1	Package	Uncore C-Box 1, Counter 1 Event Select MSR
70AH	1802	MSR_UNC_CBO_1_PERFCTR0	Package	Uncore C-Box 1, Performance Counter 0
70BH	1803	MSR_UNC_CBO_1_PERFCTR1	Package	Uncore C-Box 1, Performance Counter 1
710H	1808	MSR_UNC_CBO_2_PERFEVTSEL0	Package	Uncore C-Box 2, Counter 0 Event Select MSR
711H	1809	MSR_UNC_CBO_2_PERFEVTSEL1	Package	Uncore C-Box 2, Counter 1 Event Select MSR
712H	1810	MSR_UNC_CBO_2_PERFCTRO	Package	Uncore C-Box 2, Performance Counter 0
713H	1811	MSR_UNC_CBO_2_PERFCTR1	Package	Uncore C-Box 2, Performance Counter 1
718H	1816	MSR_UNC_CBO_3_PERFEVTSELO	Package	Uncore C-Box 3, Counter 0 Event Select MSR
719H	1817	MSR_UNC_CBO_3_PERFEVTSEL1	Package	Uncore C-Box 3, Counter 1 Event Select MSR
71AH	1818	MSR_UNC_CBO_3_PERFCTR0	Package	Uncore C-Box 3, Performance Counter 0
71BH	1819	MSR_UNC_CBO_3_PERFCTR1	Package	Uncore C-Box 3, Performance Counter 1
720H	1824	MSR_UNC_CBO_4_PERFEVTSELO	Package	Uncore C-Box 4, Counter 0 Event Select MSR

Table 2-43. Uncore PMU MSRs Supported by Intel® Core™ Processors Based on Cannon Lake Microarchitecture

Register Address		Register Name / Bit Fields	Scope	Bit Description
Hex	Dec			
721H	1825	MSR_UNC_CBO_4_PERFEVTSEL1	Package	Uncore C-Box 4, Counter 1 Event Select MSR
722H	1826	MSR_UNC_CBO_4_PERFCTRO	Package	Uncore C-Box 4, Performance Counter 0
723H	1827	MSR_UNC_CBO_4_PERFCTR1	Package	Uncore C-Box 4, Performance Counter 1
728H	1832	MSR_UNC_CBO_5_PERFEVTSELO	Package	Uncore C-Box 5, Counter 0 Event Select MSR
729H	1833	MSR_UNC_CBO_5_PERFEVTSEL1	Package	Uncore C-Box 5, Counter 1 Event Select MSR
72AH	1834	MSR_UNC_CBO_5_PERFCTRO	Package	Uncore C-Box 5, Performance Counter 0
72BH	1835	MSR_UNC_CBO_5_PERFCTR1	Package	Uncore C-Box 5, Performance Counter 1
730H	1840	MSR_UNC_CBO_6_PERFEVTSEL0	Package	Uncore C-Box 6, Counter 0 Event Select MSR
731H	1841	MSR_UNC_CBO_6_PERFEVTSEL1	Package	Uncore C-Box 6, Counter 1 Event Select MSR
732H	1842	MSR_UNC_CBO_6_PERFCTRO	Package	Uncore C-Box 6, Performance Counter 0
733H	1843	MSR_UNC_CBO_6_PERFCTR1	Package	Uncore C-Box 6, Performance Counter 1
738H	1848	MSR_UNC_CBO_7_PERFEVTSEL0	Package	Uncore C-Box 7, Counter 0 Event Select MSR
739H	1849	MSR_UNC_CBO_7_PERFEVTSEL1	Package	Uncore C-Box 7, Counter 1 Event Select MSR
73AH	1850	MSR_UNC_CBO_7_PERFCTR0	Package	Uncore C-Box 7, Performance Counter 0
73BH	1851	MSR_UNC_CBO_7_PERFCTR1	Package	Uncore C-Box 7, Performance Counter 1
E01H	3585	MSR_UNC_PERF_GLOBAL_CTRL	Package	Uncore PMU Global Control
		0		Slice 0 select.
		1		Slice 1 select.
		2		Slice 2 select.
		3		Slice 3 select.
		4		Slice 4select.
		18:5		Reserved
		29		Enable all uncore counters.
		30		Enable wake on PMI.
		31		Enable Freezing counter when overflow.
		63:32		Reserved
E02H	3586	MSR_UNC_PERF_GLOBAL_STATUS	Package	Uncore PMU Main Status
		0		Fixed counter overflowed.
		1		An ARB counter overflowed.
		2		Reserved
		3		A CBox counter overflowed (on any slice).
		63:4		Reserved

2.17.3 MSRs Introduced in 10th Generation Intel® Core™ Processors

Table 2-44 lists additional MSRs for 10th generation Intel Core processors with a CPUID Signature DisplayFamily_DisplayModel value of 06_7DH or 06_7EH. For an MSR listed in Table 2-44 that also appears in the model-specific tables of prior generations, Table 2-44 supersede prior generation tables.

Table 2-44. MSRs Supported by 10th Generation Intel® Core™ Processors Based on Ice Lake Microarchitecture

Regi Add	ister ress	Register Name / Bit Fields	Scope	Bit Description
Hex	Dec			
33H	51	MSR_MEMORY_CTRL	Core	Memory Control Register
		28:0		Reserved.
		29		SPLIT_LOCK_DISABLE
				If set to 1, a split lock will cause an #AC(0) exception.
				See Section 9.1.2.3, "Features to Disable Bus Locks."
		30		Reserved.
		31		Reserved.
48H	72	IA32_SPEC_CTRL	Соге	See Table 2-2.
49H	73	IA32_PREDICT_CMD	Thread	See Table 2-2.
8CH	140	IA32_SGXLEPUBKEYHASH0	Thread	See Table 2-2.
8DH	141	IA32_SGXLEPUBKEYHASH1	Thread	See Table 2-2.
8EH	142	IA32_SGXLEPUBKEYHASH2	Thread	See Table 2-2.
8FH	143	IA32_SGXLEPUBKEYHASH3	Thread	See Table 2-2.
AOH	160	MSR_BIOS_MCU_ERRORCODE	Package	BIOS MCU ERRORCODE (R/O)
				This MSR indicates if WRMSR 0x79 failed to configure PRM memory and gives a hint to debug BIOS.
		15:0	Package	Error Codes (R/O)
		30:16		Reserved.
		31	Thread	MCU Partial Success (R/O)
				When set to 1, WRMSR 0x79 skipped part of the functionality during BIOS.
A5H	165	MSR_FIT_BIOS_ERROR	Thread	FIT BIOS ERROR (R/W)
				Report error codes for debug in case the processor
				failed to parse the Firmware Table in BIOS. Can also be used to log BIOS information.
		7:0		Error Codes (R/W)
		7.5		Error codes for debug.
		15:8		Entry Type (R/W)
				Failed FIT entry type.
		16		FIT MCU Entry (R/W)
				FIT contains MCU entry.
		62:17		Reserved.
		63		LOCK (R/W)
				When set to 1, writes to this MSR will be skipped.
10BH	267	IA32_FLUSH_CMD	Thread	See Table 2-2.
151H	337	MSR_BIOS_DONE	Thread	BIOS Done (R/WO)

Table 2-44. MSRs Supported by 10th Generation Intel® Core™ Processors Based on Ice Lake Microarchitecture

Register Address		Register Name / Bit Fields	Scope	Bit Description
Hex	Dec	1		
		0	Thread	BIOS Done Indication (R/WO) Set by BIOS when it finishes programming the processor and wants to lock the memory configuration from changes by software that is running on this thread.
		1	Package	Writes to the bit will be ignored if EAX[0] is 0. Package BIOS Done Indication (R/0) When set to 1, all threads in the package have bit 0 of this MSR set.
		31:2		Reserved.
1F1H	497	MSR_CRASHLOG_CONTROL	Thread	Write Data to a Crash Log Configuration
		0		CDDIS: CrashDump_Disable If set, indicates that Crash Dump is disabled.
		63:1		Reserved.
2A0H	672	MSR_PRMRR_BASE_0	Core	Processor Reserved Memory Range Register - Physical Base Control Register (R/W)
		2:0		MEMTYPE: PRMRR BASE Memory Type.
		3		CONFIGURED: PRMRR BASE Configured.
		11:4		Reserved.
		51:12		BASE: PRMRR Base Address.
		63:52		Reserved.
30CH	780	IA32_FIXED_CTR3	Thread	Fixed-Function Performance Counter Register 3 (R/W) Bit definitions are the same as found in IA32_FIXED_CTR0, offset 309H. See Table 2-2.
329H	809	MSR_PERF_METRICS	Thread	Performance Metrics (R/W) Reports metrics directly. Software can check (and/or expose to its guests) the availability of PERF_METRICS feature using IA32_PERF_CAPABILITIES.PERF_METRICS_AVAILABL E (bit 15).
		7:0		Retiring. Percent of utilized slots by uops that eventually retire (commit).
		15:8		Bad Speculation. Percent of wasted slots due to incorrect speculation, covering utilized by uops that do not retire, or recovery bubbles (unutilized slots).
		23:16		Frontend Bound. Percent of unutilized slots where front-end did not deliver a uop while back-end is ready.
		31:24		Backend Bound. Percent of unutilized slots where a uop was not delivered to back-end due to lack of back-end resources.
		63:25		Reserved.

Table 2-44. MSRs Supported by 10th Generation Intel® Core™ Processors Based on Ice Lake Microarchitecture

Register Address		Register Name / Bit Fields	Scope	Bit Description
Hex	Dec			
3F2H	1010	MSR_PEBS_DATA_CFG	Thread	PEBS Data Configuration (R/W) Provides software the capability to select data groups of interest and thus reduce the record size in memory and record generation latency. Hence, a PEBS record's size and layout vary based on the selected groups. The MSR also allows software to select LBR depth for branch data records.
		0		Memory Info. Setting this bit will capture memory information such as the linear address, data source and latency of the memory access in the PEBS record.
		1		GPRs. Setting this bit will capture the contents of the General Purpose registers in the PEBS record.
		2		XMMs. Setting this bit will capture the contents of the XMM registers in the PEBS record.
		3		LBRs. Setting this bit will capture LBR TO, FROM, and INFO in the PEBS record.
		23:4		Reserved.
		31:24		LBR Entries. Set the field to the desired number of entries - 1. For example, if the LBR_entries field is 0, a single entry will be included in the record. To include 32 LBR entries, set the LBR_entries field to 31 (0x1F). To ensure all PEBS records are 16-byte aligned, software can use LBR_entries that is multiple of 3.
541H	1345	MSR_CORE_UARCH_CTL	Core	Core Microarchitecture Control MSR (R/W)
		0		L1 Scrubbing Enable When set to 1, enable L1 scrubbing.
		31:1		Reserved.
657H	1623	MSR_FAST_UNCORE_MSRS_CTL	Thread	Fast WRMSR/RDMSR Control MSR (R/W)
		3:0		FAST_ACCESS_ENABLE: Bit 0: When set to '1', provides a hint for the hardware to enable fast access mode for the IA32_HWP_REQUEST MSR. This bit is sticky and is cleaned by the hardware only
				during reset time. This bit is valid only if FAST_UNCORE_MSRS_CAPABILITY[0] is set. Setting this bit will cause CPUID[6].EAX[18] to be set.
		31:4		Reserved.

Table 2-44. MSRs Supported by 10th Generation Intel® Core™ Processors Based on Ice Lake Microarchitecture

Register Address		Register Name / Bit Fields	Scope	Bit Description
Hex	Dec			
65EH	1630	MSR_FAST_UNCORE_MSRS_STATUS	Thread	Indication of Uncore MSRs, Post Write Activates
		0		Indicates whether the CPU is still in the middle of writing IA32_HWP_REQUEST MSR, even after the WRMSR instruction has retired.
				A value of 1 indicates the last write of IA32_HWP_REQUEST is still ongoing.
				A value of 0 indicates the last write of IA32_HWP_REQUEST is visible outside the logical processor.
				Software can use the status of this bit to avoid overwriting IA32_HWP_REQUEST.
		31:1		Reserved.
65FH	1631	MSR_FAST_UNCORE_MSRS_CAPABILITY	Thread	Fast WRMSR/RDMSR Enumeration MSR (R/O)
		3:0		MSRS_CAPABILITY:
				Bit 0: If set to '1', hardware supports the fast access mode for the IA32_HWP_REQUEST MSR.
		31:4		Reserved.
772H	1906	IA32_HWP_REQUEST_PKG	Package	See Table 2-2.
775H	1909	IA32_PECI_HWP_REQUEST_INFO	Thread	See Table 2-2.
777H	1911	IA32_HWP_STATUS	Thread	See Table 2-2.

2.17.4 MSRs Introduced in the 11th Generation Intel® Core™ Processors based on Tiger Lake Microarchitecture

Table 2-45 lists additional MSRs for 11th generation Intel Core processors with a CPUID Signature DisplayFamily_DisplayModel value of 06_8CH or 06_8DH. The MSRs listed in Table 2-44 are also supported by these processors. For an MSR listed in Table 2-45 that also appears in the model-specific tables of prior generations, Table 2-45 supersedes prior generation tables.

Table 2-45. Additional MSRs Supported by the 11th Generation Intel® Core™ Processors Based on Tiger Lake Microarchitecture

Register Address		Register Name / Bit Fields	Scope	Bit Description
Hex	Dec			
AOH	160	MSR_BIOS_MCU_ERRORCODE	Package	BIOS MCU ERRORCODE (R/O)
		15:0		Error Codes
		31:16		Reserved
A7H	167	MSR_BIOS_DEBUG	Thread	BIOS DEBUG (R/O)
				This MSR indicates if WRMSR 79H failed to configure PRM memory and gives a hint to debug BIOS.
		30:0		Reserved

Table 2-45. Additional MSRs Supported by the 11th Generation Intel® Core™ Processors Based on Tiger Lake Microarchitecture (Contd.)

	ister ress	Register Name / Bit Fields	Scope	Bit Description
Hex	Dec			
		31		MCU Partial Success When set to 1, WRMSR 79H skipped part of the functionality during BIOS.
		63:32		Reserved
CFH	207	IA32_CORE_CAPABILITIES	Package	IA32 Core Capabilities Register (R/O) If CPUID.(EAX=07H, ECX=0):EDX[30] = 1. This MSR provides an architectural enumeration function for model-specific behavior.
		1:0		Reserved
		2		FUSA_SUPPORTED
		3		RSM_IN_CPL0_ONLY
				When set to 1, the RSM instruction is only allowed in CPLO (#GP triggered in any CPL!= 0).
				When set to 0, then any CPL may execute the RSM instruction.
		4		Reserved
		5		SPLIT_LOCK_DISABLE_SUPPORTED
				When read as 1, software can set bit 29 of MSR_MEMORY_CTRL (MSR address 33H).
		31:6		Reserved
492H	1170	IA32_VMX_PROCBASED_CTLS3	Core	IA32_VMX_PROCBASED_CTLS3
				This MSR enumerates the allowed 1-settings of the third set of processor-based controls. Specifically, VM entry allows bit X of the tertiary processor-based VM-execution controls to be 1 if and only if bit X of the MSR is set to 1.
				If bit X of the MSR is cleared to 0, VM entry fails if control X and the "activate tertiary controls" primary processor-based VM-execution control are both 1.
		0		LOADIWKEY
				This control determines whether executions of LOADIWKEY cause VM exits.
		63:1		Reserved
601H	1537	MSR_VR_CURRENT_CONFIG	Package	Power Limit 4 (PL4)
				Package-level maximum power limit (in Watts).
				It is a proactive, instantaneous limit.
		12:0		PL4 Value
				PL4 value in 0.125 A increments. This field is locked by VR_CURRENT_CONFIG[LOCK]. When the LOCK bit is set to 1b, this field becomes Read Only.
		30:13		Reserved

Table 2-45. Additional MSRs Supported by the 11th Generation Intel® Core™ Processors Based on Tiger Lake Microarchitecture (Contd.)

	ister ress	Register Name / Bit Fields	Scope	Bit Description
Hex	Dec			
		31		Lock Indication (LOCK) This bit will lock the CURRENT_LIMIT settings in this register and will also lock this setting. This means that once set to 1b, the CURRENT_LIMIT setting and this bit become Read Only until the next Warm Reset.
		62:32		Not in use.
		63		Reserved
6A0H	1696	IA32_U_CET		Configure User Mode CET (R/W) See Table 2-2.
6A2H	1698	IA32_S_CET		Configure Supervisor Mode CET (R/W) See Table 2-2.
6A4H	1700	IA32_PL0_SSP		Linear address to be loaded into SSP on transition to privilege level 0. (R/W) See Table 2-2.
6A5H	1701	IA32_PL1_SSP		Linear address to be loaded into SSP on transition to privilege level 1. (R/W) See Table 2-2.
6A6H	1702	IA32_PL2_SSP		Linear address to be loaded into SSP on transition to privilege level 2. (R/W) See Table 2-2.
6A7H	1703	IA32_PL3_SSP		Linear address to be loaded into SSP on transition to privilege level 3. (R/W) See Table 2-2.
6A8H	1704	IA32_INTERRUPT_SSP_TABLE_ADDR		Linear address of a table of seven shadow stack pointers that are selected in IA-32e mode using the IST index (when not 0) from the interrupt gate descriptor. (R/W) See Table 2-2.
981H	2433	IA32_TME_CAPABILITY		See Table 2-2.
982H	2434	IA32_TME_ACTIVATE		See Table 2-2.
983H	2435	IA32_TME_EXCLUDE_MASK		See Table 2-2.
984H	2436	IA32_TME_EXCLUDE_BASE		See Table 2-2.
990H	2448	IA32_COPY_STATUS ¹	Thread	See Table 2-2.
991H	2449	IA32_IWKEYBACKUP_STATUS ¹	Platform	See Table 2-2.
C82H	3202	IA32_L2_QOS_CFG	Соге	IA32_CR_L2_QOS_CFG
				This MSR provides software an enumeration of the parameters that L2 QoS (Intel RDT) support in any particular implementation.

Table 2-45. Additional MSRs Supported by the 11th Generation Intel® Core™ Processors Based on Tiger Lake Microarchitecture (Contd.)

_	ister ress	Register Name / Bit Fields	Scope	Bit Description
Hex	Dec			
		0		CDP_ENABLE
				When set to 1, it will enable the code and data prioritization for the L2 CAT/Intel RDT feature.
				When set to 0, code and data prioritization is disabled for L2 CAT/Intel RDT. See Chapter 18, "Debug, Branch Profile, TSC, and Intel® Resource Director Technology (Intel® RDT) Features," for further details on CDP.
		31:1		Reserved
D10H	3220	IA32_L2_QOS_MASK_[0-7]	Package	IA32_CR_L2_QOS_MASK_[0-7]
- D17H	- 3351			Controls MLC (L2) Intel RDT allocation. For more details on CAT/RDT, see Chapter 18, "Debug, Branch Profile, TSC, and Intel® Resource Director Technology (Intel® RDT) Features."
		19:0		WAYS_MASK
				Setting a 1 in this bit X allows threads with CLOS <n> (where N is [0-7]) to allocate to way X in the MLC. Ones are only allowed to be written to ways that physically exist in the MLC (CPUID.4.2:EBX[31:22] will indicate this).</n>
				Writing a 1 to a value beyond the highest way or a non-contiguous set of 1s will cause a #GP on the WRMSR to this MSR.
		31:20		Reserved
D91H	3473	IA32_COPY_LOCAL_TO_PLATFORM ¹	Thread	See Table 2-2.
D92H	3474	IA32_COPY_PLATFORM_TO_LOCAL ¹	Thread	See Table 2-2.

NOTES:

https://software.intel.com/content/www/us/en/develop/download/intel-key-locker-specification.html.

2.17.5 MSRs Introduced in the 12th and 13th Generation Intel® Core™ Processors Supporting Performance Hybrid Architecture

Table 2-46 lists additional MSRs for 12th and 13th generation Intel Core processors with a CPUID Signature DisplayFamily_DisplayModel value of 06_97H, 06_9AH, 06_BAH, 06_B7H, or 06_BFH. Table 2-47 lists the MSRs unique to the processor P-core. Table 2-48 lists the MSRs unique to the processor E-core.

The MSRs listed in Table 2-44¹ and Table 2-45 are also supported by these processors. For an MSR listed in Table 2-46, Table 2-47, or Table 2-48 that also appears in the model-specific tables of prior generations, Table 2-46, Table 2-47, and Table 2-48 supersede prior generation tables.

^{1.} Further details on Key Locker and usage of this MSR can be found here:

^{1.} MSRs at the following addresses are not supported in the 12th and 13th generation Intel Core processor E-core: 30CH, 329H, 541H, and 657H. The MSR at address 657H is not supported in the 12th and 13th generation Intel Core processor P-core.

Table 2-46. Additional MSRs Supported by the 12th and 13th Generation Intel® Core™ Processors Supporting Performance Hybrid Architecture

	ister ress	Register Name / Bit Fields	ce Hybrid Archi Scope	Bit Description
Hex	Dec			
33H	51	MSR_MEMORY_CTRL	Соге	Memory Control Register
		26:0		Reserved.
		27		UC_STORE_THROTTLE
				If set to 1, when enabled, the processor will only allow one in-progress UC store at a time.
		28		UC_LOCK_DISABLE
				If set to 1, a UC lock will cause a #GP(0) exception.
				See Section 9.1.2.3, "Features to Disable Bus Locks."
		29		SPLIT_LOCK_DISABLE
				If set to 1, a split lock will cause an #AC(0) exception.
				See Section 9.1.2.3, "Features to Disable Bus Locks."
		30		Reserved.
		31		Reserved.
BCH	188	IA32_MISC_PACKAGE_CTLS	Package	Power Filtering Control (R/W) IA32_ARCH_CAPABILITIES[bit 10] enumerates support for this MSR.
				See Table 2-2.
C7H	199	IA32_PMC6	Core	General Performance Counter 6 (R/W)
				See Table 2-2.
C8H	200	IA32_PMC7	Соге	General Performance Counter 7 (R/W)
				See Table 2-2.
CFH	207	IA32_CORE_CAPABILITIES	Package	IA32 Core Capabilities Register (R/O)
				If CPUID.(EAX=07H, ECX=0):EDX[30] = 1.
				This MSR provides an architectural enumeration function for model-specific behavior.
		0		STLB_QOS_SUPPORTED
				When set to 1, the STLB QoS feature is supported and the STLB QoS MSRs (1A8FH -1A97H) are accessible. When set to 0, access to these MSRs will #GP.
		1		Reserved
		2		FUSA_SUPPORTED
		3		RSM_IN_CPLO_ONLY
				When set to 1, the RSM instruction is only allowed in CPLO (#GP triggered in any CPL != 0).
				When set to 0, then any CPL may execute the RSM instruction.
		4		UC_LOCK_DISABLE_SUPPORTED
				When read as 1, software can set bit 28 of MSR_MEMORY_CTRL (MSR address 33H).

Table 2-46. Additional MSRs Supported by the 12th and 13th Generation Intel® Core™ Processors Supporting Performance Hybrid Architecture (Contd.)

	ister ress	Register Name / Bit Fields	Scope	Bit Description
Hex	Dec			
		5		SPLIT_LOCK_DISABLE_SUPPORTED
				When read as 1, software can set bit 29 of MSR_MEMORY_CTRL.
		6		SNOOP_FILTER_QOS_SUPPORTED
				When set to 1, the Snoop Filter Qos Mask MSRs are supported.
				When set to 0, access to these MSRs will #GP.
		7		UC_STORE_THROTTLING_SUPPORTED
				When set 1, UC Store throttle capability exist through MSR_MEMORY_CTRL (33H) bit 27.
		31:8		Reserved
E1H	225	IA32_UMWAIT_CONTROL		UMWAIT Control (R/W)
				See Table 2-2.
10AH	266	IA32_ARCH_CAPABILITIES		Enumeration of Architectural Features (R/O)
				See Table 2-2.
18CH	396	IA32_PERFEVTSEL6	Соге	See Table 2-20.
18DH	397	IA32_PERFEVTSEL7	Core	See Table 2-20.
195H	405	IA32_OVERCLOCKING_STATUS	Package	Overclocking Status (R/O)
				IA32_ARCH_CAPABILITIES[bit 23] enumerates support for this MSR.
				See Table 2-2.
1ADH	429	MSR_PRIMARY_TURBO_RATIO_LIMIT	Package	Primary Maximum Turbo Ratio Limit (R/W)
				Software can configure these limits when MSR_PLATFORM_INFO[28] = 1.
				Specifies Maximum Ratio Limit for each group. Maximum ratio for groups with more cores must decrease monotonically.
		7:0		MAX_TURBO_GROUP_0:
				Maximum turbo ratio limit with 1 core active.
		15:8		MAX_TURBO_GROUP_1:
				Maximum turbo ratio limit with 2 cores active.
		23:16		MAX_TURBO_GROUP_2:
				Maximum turbo ratio limit with 3 cores active.
		31:24		MAX_TURBO_GROUP_3:
				Maximum turbo ratio limit with 4 cores active.
		39:32		MAX_TURBO_GROUP_4:
				Maximum turbo ratio limit with 5 cores active.
		47:40		MAX_TURBO_GROUP_5:
				Maximum turbo ratio limit with 6 cores active.

Table 2-46. Additional MSRs Supported by the 12th and 13th Generation Intel® Core™ Processors Supporting Performance Hybrid Architecture (Contd.)

Regi Add		Register Name / Bit Fields	Scope	Bit Description
Hex	Dec			
		55:48		MAX_TURBO_GROUP_6:
				Maximum turbo ratio limit with 7 cores active.
		63:56		MAX_TURBO_GROUP_7:
				Maximum turbo ratio limit with 8 cores active.
493H	1171	IA32_VMX_EXIT_CTLS2		See Table 2-2.
4C7H	1223	IA32_A_PMC6		Full Width Writable IA32_PMC6 Alias (R/W)
				See Table 2-2.
4C8H	1224	IA32_A_PMC7		Full Width Writable IA32_PMC7 Alias (R/W)
				See Table 2-2.
650H	1616	MSR_SECONDARY_TURBO_RATIO_LIMIT	Package	Secondary Maximum Turbo Ratio Limit (R/W)
				Software can configure these limits when MSR_PLATFORM_INFO[28] = 1.
				Specifies Maximum Ratio Limit for each group. Maximum ratio for groups with more cores must decrease monotonically.
		7:0		MAX_TURBO_GROUP_0:
				Maximum turbo ratio limit with 1 core active.
		15:8		MAX_TURBO_GROUP_1:
				Maximum turbo ratio limit with 2 cores active.
		23:16		MAX_TURBO_GROUP_2:
				Maximum turbo ratio limit with 3 cores active.
		31:24		MAX_TURBO_GROUP_3:
				Maximum turbo ratio limit with 4 cores active.
		39:32		MAX_TURBO_GROUP_4:
				Maximum turbo ratio limit with 5 cores active.
		47:40		MAX_TURBO_GROUP_5:
				Maximum turbo ratio limit with 6 cores active.
		55:48		MAX_TURBO_GROUP_6:
				Maximum turbo ratio limit with 7 cores active.
		63:56		MAX_TURBO_GROUP_7:
				Maximum turbo ratio limit with 8 cores active.
664H	1636	MSR_MC6_RESIDENCY_COUNTER	Module	Module C6 Residency Counter (R/0)
				Note: C-state values are processor specific C-state code names, unrelated to MWAIT extension C-state parameters or ACPI C-States.
		63:0		Time that this module is in module-specific C6 states since last reset. Counts at 1 Mhz frequency.
6E1H	1761	IA32_PKRS		Specifies the PK permissions associated with each protection domain for supervisor pages (R/W)
				See Table 2-2.

Table 2-46. Additional MSRs Supported by the 12th and 13th Generation Intel® Core™ Processors Supporting Performance Hybrid Architecture (Contd.)

Regi Add		Register Name / Bit Fields	Scope	Bit Description
Hex	Dec			
776H	1910	IA32_HWP_CTL		See Table 2-2.
981H	2433	IA32_TME_CAPABILITY		Memory Encryption Capability MSR
				See Table 2-2.
1200H	4608	IA32_LBR_x_INFO		Last Branch Record Entry X Info Register (R/W)
- 121FH	4639			See Table 2-2.
14CEH	5326	IA32_LBR_CTL		Last Branch Record Enabling and Configuration Register (R/W)
				See Table 2-2.
14CFH	5327	IA32_LBR_DEPTH		Last Branch Record Maximum Stack Depth Register (R/W)
				See Table 2-2.
1500H	5376	IA32_LBR_x_FROM_IP		Last Branch Record Entry X Source IP Register (R/W)
- 151FH	- 5407			See Table 2-2.
1600H -	5632 -	IA32_LBR_x_TO_IP		Last Branch Record Entry X Destination IP Register (R/W)
161FH	5663			See Table 2-2.
17D2H	6098	IA32_THREAD_FEEDBACK_CHAR		Thread Feedback Characteristics (R/O)
				See Table 2-2.
17D4H	6100	IA32_HW_FEEDBACK_THREAD_CONFIG		Hardware Feedback Thread Configuration (R/W)
				See Table 2-2.
17DAH	6106	IA32_HRESET_ENABLE		History Reset Enable (R/W)
				See Table 2-2.

The MSRs listed in Table 2-47 are unique to the 12th and 13th generation Intel Core processor P-core. These MSRs are not supported on the processor E-core.

Table 2-47. MSRs Supported by 12th and 13th Generation Intel® Core™ Processor P-core

Regi Add		Register Name / Bit Fields	Scope	Bit Description
Hex	Dec			
1A4H	420	MSR_PREFETCH_CONTROL		Prefetch Disable Bits (R/W)
		0		L2_HARDWARE_PREFETCHER_DISABLE
				If 1, disables the L2 hardware prefetcher, which fetches additional lines of code or data into the L2 cache.
		1		L2_ADJACENT_CACHE_LINE_PREFETCHER_DISABLE
				If 1, disables the adjacent cache line prefetcher, which fetches the cache line that comprises a cache line pair (128 bytes).

Table 2-47. MSRs Supported by 12th and 13th Generation Intel® Core™ Processor P-core

	ister ress	Register Name / Bit Fields	Scope	Bit Description
Hex	Dec			
		2		DCU_HARDWARE_PREFETCHER_DISABLE If 1, disables the L1 data cache prefetcher, which fetches the next cache line into L1 data cache.
		3		DCU_IP_PREFETCHER_DISABLE
				If 1, disables the L1 data cache IP prefetcher, which uses sequential load history (based on instruction pointer of previous loads) to determine whether to prefetch additional lines.
		4		Reserved.
		5		AMP_PREFETCH_DISABLE
				If 1, disables the L2 Adaptive Multipath Probability (AMP) prefetcher.
		63:6		Reserved.
3F7H	1015	MSR_PEBS_FRONTEND	Thread	FrontEnd Precise Event Condition Select (R/W) See Table 2-39.
540H	1344	MSR_THREAD_UARCH_CTL	Thread	Thread Microarchitectural Control (R/W)
		0		WB_MEM_STRM_LD_DISABLE
				Disable streaming behavior for MOVNTDQA loads to WB memory type. If set, these accesses will be treated like regular cacheable loads (Data will be cached).
		63:1		Reserved
541H	1345	MSR_CORE_UARCH_CTL	Соге	Core Microarchitecture Control MSR (R/W) See Table 2-44.
D10H	3220	IA32_L2_QOS_MASK_[0-7]	Соге	IA32_CR_L2_QOS_MASK_[0-7]
- D17H	- 3351			If CPUID.(EAX=10H, ECX=1):EDX.COS_MAX[15:0] \geq 0.
DITTI	3331			Controls MLC (L2) Intel RDT allocation. For more details on CAT/RDT, see Chapter 18, "Debug, Branch Profile, TSC, and Intel® Resource Director Technology (Intel® RDT) Features."
		19:0		WAYS_MASK
				Setting a 1 in this bit X allows threads with CLOS <n> (where N is [0-7]) to allocate to way X in the MLC. Ones are only allowed to be written to ways that physically exist in the MLC (CPUID.4.2:EBX[31:22] will indicate this).</n>
				Writing a 1 to a value beyond the highest way or a non-contiguous set of 1s will cause a #GP on the WRMSR to this MSR.
		31:20		Reserved

The MSRs listed in Table 2-48 are unique to the 12th and 13th generation Intel Core processor E-core. These MSRs are not supported on the processor P-core.

Table 2-48. MSRs Supported by 12th and 13th Generation Intel® Core™ Processor E-core

Regi Add		Register Name / Bit Fields	Scope	Bit Description
Hex	Dec			
D10H	3220	IA32_L2_QOS_MASK_[0-15]	Module	IA32_CR_L2_QOS_MASK_[0-15]
D1FH	- 3359			If CPUID.(EAX=10H, ECX=1):EDX.COS_MAX[15:0] \geq 0.
	3333			Controls MLC (L2) Intel RDT allocation. For more details on CAT/RDT, see Chapter 18, "Debug, Branch Profile, TSC, and Intel® Resource Director Technology (Intel® RDT) Features."
		19:0		WAYS_MASK
				Setting a 1 in this bit X allows threads with CLOS <n> (where N is [0-7]) to allocate to way X in the MLC. Ones are only allowed to be written to ways that physically exist in the MLC (CPUID.4.2:EBX[31:22] will indicate this).</n>
				Writing a 1 to a value beyond the highest way or a non-contiguous set of 1s will cause a #GP on the WRMSR to this MSR.
		31:20		Reserved
1309H	4873	MSR_RELOAD_FIXED_CTRx		Reload value for IA32_FIXED_CTRx (R/W)
- 130BH	- 4875	47:0		Value loaded into IA32_FIXED_CTRx when a PEBS record is generated while PEBS_EN_FIXEDx = 1 and PEBS_OUTPUT = 01B in IA32_PEBS_ENABLE, and FIXED_CTRx is overflowed.
		63:48		Reserved
14C1H	5313	MSR_RELOAD_PMCx	Core	Reload value for IA32_PMCx (R/W)
- 14C6H	- 5318	47:0		Value loaded into IA32_PMCx when a PEBS record is generated while PEBS_EN_PMCx = 1 and PEBS_OUTPUT = 01B in IA32_PEBS_ENABLE, and PMCx is overflowed.
		63:48		Reserved

Table 2-49 lists the MSRs of uncore PMU for Intel processors with a CPUID Signature DisplayFamily_DisplayModel value of 06_97H , 06_9AH , 06_BAH , 06_B7H , or 06_BFH .

Table 2-49. Uncore PMU MSRs Supported by 12th and 13th Generation Intel® Core™ Processors

Regi Addi		Register Name / Bit Fields	Scope	Bit Description
Hex	Dec			
396H	918	MSR_UNC_CBO_CONFIG	Package	Uncore C-Box Configuration Information (R/O)
		3:0		Specifies the number of C-Box units with programmable counters (including processor cores and processor graphics).
		63:4		Reserved
2000H	8192	MSR_UNC_CBO_0_PERFEVTSEL0	Package	Uncore C-Box O, Counter O Event Select MSR
2001H	8193	MSR_UNC_CBO_0_PERFEVTSEL1	Package	Uncore C-Box O, Counter 1 Event Select MSR

Table 2-49. Uncore PMU MSRs Supported by 12th and 13th Generation Intel® Core™ Processors

Register Address		Register Name / Bit Fields	Scope	Bit Description
Hex	Dec			
2002H	8194	MSR_UNC_CBO_0_PERFCTR0	Package	Uncore C-Box 0, Performance Counter 0
2003H	8195	MSR_UNC_CBO_0_PERFCTR1	Package	Uncore C-Box 0, Performance Counter 1
2008H	8200	MSR_UNC_CBO_1_PERFEVTSEL0	Package	Uncore C-Box 1, Counter 0 Event Select MSR
2009H	8201	MSR_UNC_CBO_1_PERFEVTSEL1	Package	Uncore C-Box 1, Counter 1 Event Select MSR
200AH	8202	MSR_UNC_CBO_1_PERFCTRO	Package	Uncore C-Box 1, Performance Counter 0
200BH	8203	MSR_UNC_CBO_1_PERFCTR1	Package	Uncore C-Box 1, Performance Counter 1
2010H	8208	MSR_UNC_CBO_2_PERFEVTSEL0	Package	Uncore C-Box 2, Counter 0 Event Select MSR
2011H	8209	MSR_UNC_CBO_2_PERFEVTSEL1	Package	Uncore C-Box 2, Counter 1 Event Select MSR
2012H	8210	MSR_UNC_CBO_2_PERFCTRO	Package	Uncore C-Box 2, Performance Counter 0
2013H	8211	MSR_UNC_CBO_2_PERFCTR1	Package	Uncore C-Box 2, Performance Counter 1
2018H	8216	MSR_UNC_CBO_3_PERFEVTSEL0	Package	Uncore C-Box 3, Counter 0 Event Select MSR
2019H	8217	MSR_UNC_CBO_3_PERFEVTSEL1	Package	Uncore C-Box 3, Counter 1 Event Select MSR
201AH	8218	MSR_UNC_CBO_3_PERFCTRO	Package	Uncore C-Box 3, Performance Counter 0
201BH	8219	MSR_UNC_CBO_3_PERFCTR1	Package	Uncore C-Box 3, Performance Counter 1
2020H	8224	MSR_UNC_CBO_4_PERFEVTSEL0	Package	Uncore C-Box 4, Counter 0 Event Select MSR
2021H	8225	MSR_UNC_CBO_4_PERFEVTSEL1	Package	Uncore C-Box 4, Counter 1 Event Select MSR
2022H	8226	MSR_UNC_CBO_4_PERFCTRO	Package	Uncore C-Box 4, Performance Counter 0
2023H	8227	MSR_UNC_CBO_4_PERFCTR1	Package	Uncore C-Box 4, Performance Counter 1
2028H	8232	MSR_UNC_CBO_5_PERFEVTSEL0	Package	Uncore C-Box 5, Counter 0 Event Select MSR
2029H	8233	MSR_UNC_CBO_5_PERFEVTSEL1	Package	Uncore C-Box 5, Counter 1 Event Select MSR
202AH	8234	MSR_UNC_CBO_5_PERFCTRO	Package	Uncore C-Box 5, Performance Counter 0
202BH	8235	MSR_UNC_CBO_5_PERFCTR1	Package	Uncore C-Box 5, Performance Counter 1
2030H	8240	MSR_UNC_CBO_6_PERFEVTSELO	Package	Uncore C-Box 6, Counter 0 Event Select MSR
2031H	8241	MSR_UNC_CBO_6_PERFEVTSEL1	Package	Uncore C-Box 6, Counter 1 Event Select MSR
2032H	8242	MSR_UNC_CBO_6_PERFCTRO	Package	Uncore C-Box 6, Performance Counter 0
2033H	8243	MSR_UNC_CBO_6_PERFCTR1	Package	Uncore C-Box 6, Performance Counter 1
2038H	8248	MSR_UNC_CBO_7_PERFEVTSEL0	Package	Uncore C-Box 7, Counter 0 Event Select MSR
2039H	8249	MSR_UNC_CBO_7_PERFEVTSEL1	Package	Uncore C-Box 7, Counter 1 Event Select MSR
203AH	8250	MSR_UNC_CBO_7_PERFCTRO	Package	Uncore C-Box 7, Performance Counter 0
203BH	8251	MSR_UNC_CBO_7_PERFCTR1	Package	Uncore C-Box 7, Performance Counter 1
2040H	8256	MSR_UNC_CBO_8_PERFEVTSEL0	Package	Uncore C-Box 8, Counter 0 Event Select MSR
2041H	8257	MSR_UNC_CBO_8_PERFEVTSEL1	Package	Uncore C-Box 8, Counter 1 Event Select MSR
2042H	8258	MSR_UNC_CBO_8_PERFCTR0	Package	Uncore C-Box 8, Performance Counter 0
2043H	8259	MSR_UNC_CBO_8_PERFCTR1	Package	Uncore C-Box 8, Performance Counter 1
2048H	8264	MSR_UNC_CBO_9_PERFEVTSELO	Package	Uncore C-Box 9, Counter 0 Event Select MSR
2049H	8265	MSR_UNC_CBO_9_PERFEVTSEL1	Package	Uncore C-Box 9, Counter 1 Event Select MSR
204AH	8266	MSR_UNC_CBO_9_PERFCTR0	Package	Uncore C-Box 9, Performance Counter 0

Table 2-49. Uncore PMU MSRs Supported by 12th and 13th Generation Intel® Core™ Processors

	ister ress	Register Name / Bit Fields	Scope	Bit Description
Hex	Dec			
204BH	8267	MSR_UNC_CBO_9_PERFCTR1	Package	Uncore C-Box 9, Performance Counter 1
2FD0H	12240	MSR_UNC_ARB_O_PERFEVTSELO	Package	Uncore Arb Unit 0, Counter 0 Event Select MSR
2FD1H	12241	MSR_UNC_ARB_0_PERFEVTSEL1	Package	Uncore Arb Unit 0, Counter 1 Event Select MSR
2FD2H	12242	MSR_UNC_ARB_O_PERFCTRO	Package	Uncore Arb Unit 0, Performance Counter 0
2FD3H	12243	MSR_UNC_ARB_0_PERFCTR1	Package	Uncore Arb Unit 0, Performance Counter 1
2FD4H	12244	MSR_UNC_ARB_O_PERF_STATUS	Package	Uncore Arb Unit O, Performance Status
2FD5H	12245	MSR_UNC_ARB_0_PERF_CTRL	Package	Uncore Arb Unit O, Performance Control
2FD8H	12248	MSR_UNC_ARB_1_PERFEVTSEL0	Package	Uncore Arb Unit 1, Counter 0 Event Select MSR
2FD9H	12249	MSR_UNC_ARB_1_PERFEVTSEL1	Package	Uncore Arb Unit 1, Counter 1 Event Select MSR
2FDAH	12250	MSR_UNC_ARB_1_PERFCTR0	Package	Uncore Arb Unit 1, Performance Counter 0
2FDBH	12251	MSR_UNC_ARB_1_PERFCTR1	Package	Uncore Arb Unit 1, Performance Counter 1
2FDCH	12252	MSR_UNC_ARB_1_PERF_STATUS	Package	Uncore Arb Unit 1, Performance Status
2FDDH	12253	MSR_UNC_ARB_1_PERF_CTRL	Package	Uncore Arb Unit 1, Performance Control
2FDEH	12254	MSR_UNC_PERF_FIXED_CTRL	Package	Uncore Fixed Counter Control (R/W)
		19:0		Reserved
		20		Enable overflow propagation.
		21		Reserved
		22		Enable counting.
		63:23		Reserved
2FDFH	12255	MSR_UNC_PERF_FIXED_CTR	Package	Uncore Fixed Counter
		43:0		Current count.
		63:44		Reserved
2FF0H	12272	MSR_UNC_PERF_GLOBAL_CTRL	Package	Uncore PMU Global Control
		0		Slice 0 select.
		1		Slice 1 select.
		2		Slice 2 select.
		3		Slice 3 select.
		4		Slice 4 select.
		18:5		Reserved
		29		Enable all uncore counters.
		30		Enable wake on PMI.
		31		Enable Freezing counter when overflow.
		63:32		Reserved
2FF2H	12274	MSR_UNC_PERF_GLOBAL_STATUS	Package	Uncore PMU Main Status
		0		Fixed counter overflowed.
		1		An ARB counter overflowed.
		2		Reserved

Table 2-49. Uncore PMU MSRs Supported by 12th and 13th Generation Intel® Core™ Processors

Register Address		Register Name / Bit Fields	Scope	Bit Description
Hex	Dec			
		3		A CBox counter overflowed (on any slice).
		63:4		Reserved

2.17.6 MSRs Introduced in the Intel® Xeon® Scalable Processor Family

The Intel $^{\$}$ Xeon $^{\$}$ Scalable Processor Family (CPUID Signature DisplayFamily_DisplayModel value of 06_55H) supports the MSRs listed in Table 2-50.

Table 2-50. MSRs Supported by the Intel® Xeon® Scalable Processor Family with a CPUID Signature DisplayFamily_DisplayModel Value of 06_55H

Regi Add		Register Name / Bit Fields Scope (Former MSR Name)	Scope	Bit Description
Hex	Dec			
ЗАН	58	IA32_FEATURE_CONTROL	Thread	Control Features in Intel 64 Processor (R/W)
				See Table 2-2.
		0		Lock (R/WL)
		1		Enable VMX Inside SMX Operation (R/WL)
		2		Enable VMX Outside SMX Operation (R/WL)
		14:8		SENTER Local Functions Enables (R/WL)
		15		SENTER Global Functions Enable (R/WL)
		18		SGX Global Functions Enable (R/WL)
		20		LMCE_ENABLED (R/WL)
		63:21		Reserved
4EH	78	IA32_PPIN_CTL	Package	Protected Processor Inventory Number Enable Control
		(MSR_PPIN_CTL)		(R/W)
		0		LockOut (R/WO)
				See Table 2-2.
		1		Enable_PPIN (R/W)
				See Table 2-2.
		63:2		Reserved
4FH	79	IA32_PPIN (MSR_PPIN)	Package	Protected Processor Inventory Number (R/O)
		63:0		Protected Processor Inventory Number (R/0)
		03.0		See Table 2-2.
CEH	206	MSR_PLATFORM_INFO	Package	Platform Information
				Contains power management and other model specific features enumeration. See http://biosbits.org.
		7:0		Reserved
		15:8	Package	Maximum Non-Turbo Ratio (R/O)
				See Table 2-26.

Table 2-50. MSRs Supported by the Intel® Xeon® Scalable Processor Family with a CPUID Signature DisplayFamily_DisplayModel Value of 06_55H (Contd.)

	ister ress	Register Name / Bit Fields (Former MSR Name)	Scope	Bit Description
Hex	Dec			
		22:16		Reserved.
		23	Package	PPIN_CAP (R/O)
				See Table 2-26.
		27:24		Reserved
		28	Package	Programmable Ratio Limit for Turbo Mode (R/O)
				See Table 2-26.
		29	Package	Programmable TDP Limit for Turbo Mode (R/O)
				See Table 2-26.
		30	Package	Programmable TJ OFFSET (R/O)
				See Table 2-26.
		39:31		Reserved
		47:40	Package	Maximum Efficiency Ratio (R/O)
				See Table 2-26.
		63:48		Reserved
E2H	226	MSR_PKG_CST_CONFIG_CONTROL	Соге	C-State Configuration Control (R/W)
				Note: C-state values are processor specific C-state code names, unrelated to MWAIT extension C-state parameters or ACPI C-states.
				See http://biosbits.org.
		2:0		Package C-State Limit (R/W)
				Specifies the lowest processor-specific C-state code name (consuming the least power) for the package. The default is set as factory-configured package C-state limit.
				The following C-state code name encodings are supported:
				000b: CO/C1 (no package C-state support) 001b: C2
				010b: C6 (non-retention)
				011b: C6 (retention)
				111b: No Package C state limits. All C states supported by the processor are available.
		9:3		Reserved
		10		I/O MWAIT Redirection Enable (R/W)
		14:11		Reserved
		15		CFG Lock (R/WO)
		16		Automatic C-State Conversion Enable (R/W)
				If 1, the processor will convert HALT or MWAT(C1) to MWAIT(C6).
		24:17		Reserved

Table 2-50. MSRs Supported by the Intel® Xeon® Scalable Processor Family with a CPUID Signature DisplayFamily_DisplayModel Value of 06_55H (Contd.)

Regi Addi			Scope	Bit Description
Hex	Dec			
		25		C3 State Auto Demotion Enable (R/W)
		26		C1 State Auto Demotion Enable (R/W)
		27		Enable C3 Undemotion (R/W)
		28		Enable C1 Undemotion (R/W)
		29		Package C State Demotion Enable (R/W)
		30		Package C State UnDemotion Enable (R/W)
		63:31		Reserved
179H	377	IA32_MCG_CAP	Thread	Global Machine Check Capability (R/O)
		7:0		Count
		8		MCG_CTL_P
		9		MCG_EXT_P
		10		MCP_CMCI_P
		11		MCG_TES_P
		15:12		Reserved
		23:16		MCG_EXT_CNT
		24		MCG_SER_P
		25		MCG_EM_P
		26		MCG_ELOG_P
		63:27		Reserved
17DH	381	MSR_SMM_MCA_CAP	THREAD	Enhanced SMM Capabilities (SMM-RO)
				Reports SMM capability Enhancement. Accessible only while in SMM.
		57:0		Reserved
		58		SMM_Code_Access_Chk (SMM-RO)
				If set to 1 indicates that the SMM code access restriction is supported and a host-space interface is available to SMM handler.
		59		Long_Flow_Indication (SMM-RO)
				If set to 1 indicates that the SMM long flow indicator is supported and a host-space interface is available to SMM handler.
		63:60		Reserved
19CH	412	IA32_THERM_STATUS	Core	Thermal Monitor Status (R/W)
				See Table 2-2.
		0		Thermal Status (R/O)
				See Table 2-2.
		1		Thermal Status Log (R/WC0)
				See Table 2-2.

Table 2-50. MSRs Supported by the Intel® Xeon® Scalable Processor Family with a CPUID Signature DisplayFamily_DisplayModel Value of 06_55H (Contd.)

Regi Add		Register Name / Bit Fields	Scope	Bit Description
Hex	Dec	(Former MSR Name)		
		2		PROTCHOT # or FORCEPR# Status (R/O) See Table 2-2.
		3		PROTCHOT # or FORCEPR# Log (R/WC0) See Table 2-2.
		4		Critical Temperature Status (R/O) See Table 2-2.
		5		Critical Temperature Status Log (R/WC0) See Table 2-2.
		6		Thermal Threshold #1 Status (R/O) See Table 2-2.
		7		Thermal Threshold #1 Log (R/WC0) See Table 2-2.
		8		Thermal Threshold #2 Status (R/0) See Table 2-2.
		9		Thermal Threshold #2 Log (R/WC0) See Table 2-2.
		10		Power Limitation Status (R/0) See Table 2-2.
		11		Power Limitation Log (R/WCO) See Table 2-2.
		12		Current Limit Status (R/0) See Table 2-2.
		13		Current Limit Log (R/WCO) See Table 2-2.
		14		Cross Domain Limit Status (R/O) See Table 2-2.
		15		Cross Domain Limit Log (R/WC0) See Table 2-2.
		22:16		Digital Readout (R/O) See Table 2-2.
		26:23		Reserved
		30:27		Resolution in Degrees Celsius (R/0) See Table 2-2.
		31		Reading Valid (R/O) See Table 2-2.
		63:32		Reserved
1A2H	418	MSR_TEMPERATURE_TARGET	Package	Temperature Target
		15:0		Reserved

Table 2-50. MSRs Supported by the Intel® Xeon® Scalable Processor Family with a CPUID Signature DisplayFamily_DisplayModel Value of 06_55H (Contd.)

Regi Add		Register Name / Bit Fields (Former MSR Name)	Scope	Bit Description
Hex	Dec			·
		23:16		Temperature Target (R/O) See Table 2-26.
		27:24		TCC Activation Offset (R/W) See Table 2-26.
		63:28		Reserved
1ADH	429	MSR_TURBO_RATIO_LIMIT	Package	This register defines the ratio limits. RATIO[0:7] must be populated in ascending order. RATIO[i+1] must be less than or equal to RATIO[i]. Entries with RATIO[i] will be ignored. If any of the rules above are broken, the configuration is silently rejected. If the programmed ratio is:
				 Above the fused ratio for that core count, it will be clipped to the fuse limits (assuming !OC). Below the min supported ratio, it will be clipped.
		7:0		RATIO_0
				Defines ratio limits.
		15:8		RATIO_1
				Defines ratio limits.
		23:16		RATIO_2
				Defines ratio limits.
		31:24		RATIO_3
				Defines ratio limits.
		39:32		RATIO_4
				Defines ratio limits.
		47:40		RATIO_5
				Defines ratio limits.
		55:48		RATIO_6
		22.50		Defines ratio limits.
		63:56		RATIO_7
105:	422	MCD TUDDO DATIO LIVIT COSCI		Defines ratio limits.
1AEH	430	MSR_TURBO_RATIO_LIMIT_CORES	Package	This register defines the active core ranges for each frequency point. NUMCORE[0:7] must be populated in ascending order. NUMCORE[i+1] must be greater than NUMCORE[i]. Entries with NUMCORE[i] == 0 will be ignored. The last valid entry must have NUMCORE >= the number of cores in the SKU. If any of the rules above are broken, the configuration is silently rejected.
		7:0		NUMCORE_0
				Defines the active core ranges for each frequency point.

Table 2-50. MSRs Supported by the Intel® Xeon® Scalable Processor Family with a CPUID Signature DisplayFamily_DisplayModel Value of 06_55H (Contd.)

	ister ress	Register Name / Bit Fields	Scope	Bit Description
Hex	Dec	(Former MSR Name)		
		15:8		NUMCORE_1
				Defines the active core ranges for each frequency point.
		23:16		NUMCORE_2
				Defines the active core ranges for each frequency point.
		31:24		NUMCORE_3
				Defines the active core ranges for each frequency point.
		39:32		NUMCORE_4
				Defines the active core ranges for each frequency point.
		47:40		NUMCORE_5
				Defines the active core ranges for each frequency point.
		55:48		NUMCORE_6
				Defines the active core ranges for each frequency point.
		63:56		NUMCORE_7
				Defines the active core ranges for each frequency point.
280H	640	IA32_MC0_CTL2	Соге	See Table 2-2.
281H	641	IA32_MC1_CTL2	Соге	See Table 2-2.
282H	642	IA32_MC2_CTL2	Соге	See Table 2-2.
283H	643	IA32_MC3_CTL2	Соге	See Table 2-2.
284H	644	IA32_MC4_CTL2	Package	See Table 2-2.
285H	645	IA32_MC5_CTL2	Package	See Table 2-2.
286H	646	IA32_MC6_CTL2	Package	See Table 2-2.
287H	647	IA32_MC7_CTL2	Package	See Table 2-2.
288H	648	IA32_MC8_CTL2	Package	See Table 2-2.
289H	649	IA32_MC9_CTL2	Package	See Table 2-2.
28AH	650	IA32_MC10_CTL2	Package	See Table 2-2.
28BH	651	IA32_MC11_CTL2	Package	See Table 2-2.
28CH	652	IA32_MC12_CTL2	Package	See Table 2-2.
28DH	653	IA32_MC13_CTL2	Package	See Table 2-2.
28EH	654	IA32_MC14_CTL2	Package	See Table 2-2.
28FH	655	IA32_MC15_CTL2	Package	See Table 2-2.
290H	656	IA32_MC16_CTL2	Package	See Table 2-2.
291H	657	IA32_MC17_CTL2	Package	See Table 2-2.

Table 2-50. MSRs Supported by the Intel® Xeon® Scalable Processor Family with a CPUID Signature DisplayFamily_DisplayModel Value of 06_55H (Contd.)

Register Address		Register Name / Bit Fields	Scope	Bit Description
Hex	Dec	(Former MSR Name)		
292H	658	IA32_MC18_CTL2	Package	See Table 2-2.
293H	659	IA32_MC19_CTL2	Package	See Table 2-2.
400H	1024	IA32_MC0_CTL	Core	See Section 16.3.2.1, "IA32_MCi_CTL MSRs," through
401H	1025	IA32_MC0_STATUS	Core	Section 16.3.2.4, "IA32_MCi_MISC MSRs."
402H	1026	IA32_MCO_ADDR	Соге	Bank MCO reports MC errors from the IFU module.
403H	1027	IA32_MCO_MISC	Соге	
404H	1028	IA32_MC1_CTL	Core	See Section 16.3.2.1, "IA32_MCi_CTL MSRs," through
405H	1029	IA32_MC1_STATUS	Core	Section 16.3.2.4, "IA32_MCi_MISC MSRs."
406H	1030	IA32_MC1_ADDR	Соге	Bank MC1 reports MC errors from the DCU module.
407H	1031	IA32_MC1_MISC	Core	
408H	1032	IA32_MC2_CTL	Core	See Section 16.3.2.1, "IA32_MCi_CTL MSRs," through
409H	1033	IA32_MC2_STATUS	Соге	Section 16.3.2.4, "IA32_MCi_MISC MSRs."
40AH	1034	IA32_MC2_ADDR	Core	Bank MC2 reports MC errors from the DTLB module.
40BH	1035	IA32_MC2_MISC	Соге	
40CH	1036	IA32_MC3_CTL	Соге	See Section 16.3.2.1, "IA32_MCi_CTL MSRs," through
40DH	1037	IA32_MC3_STATUS	Соге	Section 16.3.2.4, "IA32_MCi_MISC MSRs."
40EH	1038	IA32_MC3_ADDR	Core	Bank MC3 reports MC errors from the MLC module.
40FH	1039	IA32_MC3_MISC	Core	
410H	1040	IA32_MC4_CTL	Package	See Section 16.3.2.1, "IA32_MCi_CTL MSRs," through
411H	1041	IA32_MC4_STATUS	Package	Section 16.3.2.4, "IA32_MCi_MISC MSRs."
412H	1042	IA32_MC4_ADDR	Package	Bank MC4 reports MC errors from the PCU module.
413H	1043	IA32_MC4_MISC	Package	
414H	1044	IA32_MC5_CTL	Package	See Section 16.3.2.1, "IA32_MCi_CTL MSRs," through
415H	1045	IA32_MC5_STATUS	Package	Section 16.3.2.4, "IA32_MCi_MISC MSRs."
416H	1046	IA32_MC5_ADDR	Package	Bank MC5 reports MC errors from a link interconnect module.
417H	1047	IA32_MC5_MISC	Package	
418H	1048	IA32_MC6_CTL	Package	See Section 16.3.2.1, "IA32_MCi_CTL MSRs," through
419H	1049	IA32_MC6_STATUS	Package	Section 16.3.2.4, "IA32_MCi_MISC MSRs."
41AH	1050	IA32_MC6_ADDR	Package	Bank MC6 reports MC errors from the integrated I/O module.
41BH	1051	IA32_MC6_MISC	Package	<u> </u>
41CH	1052	IA32_MC7_CTL	Package	See Section 16.3.2.1, "IA32_MCi_CTL MSRs," through
41DH	1053	IA32_MC7_STATUS	Package	Section 16.3.2.4, "IA32_MCi_MISC MSRs."
41EH	1054	IA32_MC7_ADDR	Package	Bank MC7 reports MC errors from the M2M 0.
41FH	1055	IA32_MC7_MISC	Package	1

Table 2-50. MSRs Supported by the Intel® Xeon® Scalable Processor Family with a CPUID Signature DisplayFamily_DisplayModel Value of 06_55H (Contd.)

A20H 1056 IA32_MCB_STATUS Package Section 16.3.2.1, "IA32_MCI_CTL MSRs," through	_	ister ress	Register Name / Bit Fields	Scope	Bit Description
421H 1057 IA32_MCB_STATUS Package 422H 1058 IA32_MCB_ADDR Package 423H 1059 IA32_MCB_MISC Package 424H 1060 IA32_MCG_STATUS Package 425H 1061 IA32_MCG_STATUS Package 426H 1062 IA32_MCG_MISC Package 427H 1063 IA32_MCG_MISC Package 428H 1064 IA32_MCI_MISC MSRs." Banks MC9 - MC11 report MC errors from the CHA 429H 1065 IA32_MC10_CTL Package 428H 1066 IA32_MC10_MISC Package 428H 1066 IA32_MC10_MISC Package 420H 1066 IA32_MC10_MISC Package 420H 1068 IA32_MC11_STATUS Package 420H 1069 IA32_MC11_MISC Package 420H 1070 IA32_MC11_ADDR Package 430H 1072 IA32_MC1_STATUS Package 431H 1073 IA32_MC1_ATUS	Hex	Dec	(Former MSR Name)		
A22H 1059	420H	1056	IA32_MC8_CTL	Package	
423H 1058 IA32_MCB_MISC Package 424H 1060 IA32_MC9_CTL Package 425H 1061 IA32_MC9_STATUS Package 426H 1062 IA32_MC9_ADDR Package 427H 1063 IA32_MC9_MISC Package 428H 1064 IA32_MC10_CTL Package 429H 1065 IA32_MC10_STATUS Package 429H 1065 IA32_MC10_ADDR Package 420H 1066 IA32_MC10_ADDR Package 420H 1067 IA32_MC10_MISC Package 420H 1068 IA32_MC11_CTL Package 420H 1069 IA32_MC11_STATUS Package 420H 1069 IA32_MC11_ADDR Package 420H 1070 IA32_MC12_STATUS Package 430H 1072 IA32_MC13_STATUS Package 430H 1072 IA32_MC13_STATUS Package 433H 1075 IA32_MC13_STATUS Package <td>421H</td> <td>1057</td> <td>IA32_MC8_STATUS</td> <td>Package</td> <td></td>	421H	1057	IA32_MC8_STATUS	Package	
424H 1060 IA32_MC9_CTL Package See Section 16.3.2.1, "IA32_MCI_CTL MSRs," through 425H 1061 IA32_MC9_STATUS Package Seetion 16.3.2.1, "IA32_MCI_MISC MSRs." 426H 1062 IA32_MC9_ADDR Package See Section 16.3.2.1, "IA32_MCI_CTL MSRs," through 428H 1064 IA32_MC10_STATUS Package See Section 16.3.2.1, "IA32_MCI_CTL MSRs," through 429H 1065 IA32_MC10_ADDR Package See Section 16.3.2.1, "IA32_MCI_CTL MSRs," through 428H 1066 IA32_MC10_MISC Package See Section 16.3.2.1, "IA32_MCI_CTL MSRs," through 42BH 1066 IA32_MC10_MISC Package See Section 16.3.2.1, "IA32_MCI_CTL MSRs," through 42BH 1068 IA32_MC11_STATUS Package See Section 16.3.2.1, "IA32_MCI_CTL MSRs," through 42BH 1070 IA32_MC11_MISC Package See Section 16.3.2.1, "IA32_MCI_CTL MSRs," through 42BH 1071 IA32_MC12_STATUS Package See Section 16.3.2.1, "IA32_MCI_CTL MSRs," through 43BH 1073 IA32_MC12_MISC Package See Section 16.3.2.1, "IA32_MCI_CTL MSRs," throug	422H	1058	IA32_MC8_ADDR	Package	Bank MC8 reports MC errors from the M2M 1.
425H 1061 IA32_MC9_STATUS	423H	1059	IA32_MC8_MISC	Package	
A25H 1061 A32_MC3_ADDR	424H	1060	IA32_MC9_CTL	Package	
426H 1062 IA32_MC9_AIDDR	425H	1061	IA32_MC9_STATUS	Package	. – –
428H 1064 IA32_MC10_CTL Package See Section 16.3.2.1, "IA32_MCI_CTL MSRs," through 429H 1065 IA32_MC10_STATUS Package Section 16.3.2.1, "IA32_MCI_MISC MSRs." 42BH 1066 IA32_MC10_ADDR Package Banks MC9 - MC11 report MC errors from the CHA. 42BH 1067 IA32_MC11_MISC Package See Section 16.3.2.1, "IA32_MCI_CTL MSRs," through Section 16.3.2.4, "IA32_MCI_MISC MSRs." 42DH 1069 IA32_MC11_ADDR Package See Section 16.3.2.1, "IA32_MCI_MISC MSRs." 42EH 1070 IA32_MC11_MISC Package See Section 16.3.2.1, "IA32_MCI_CTL MSRs," through Section 16.3.2.4, "IA32_MCI_MISC MSRs." 431H 1073 IA32_MC12_ADDR Package See Section 16.3.2.1, "IA32_MCI_MISC MSRs." 433H 1075 IA32_MC13_STATUS Package See Section 16.3.2.1, "IA32_MCI_CTL MSRs," through Section 16.3.2.4, "IA32_MCI_MISC MSRs." 436H 1078 IA32_MC13_MISC Package See Section 16.3.2.1, "IA32_MCI_MISC MSRs." 437H 1079 IA32_MC13_MISC Package See Section 16.3.2.1, "IA32_MCI_MISC MSRs." 438H 1080 IA32_MC14_STATUS </td <td>426H</td> <td>1062</td> <td>IA32_MC9_ADDR</td> <td>Package</td> <td>Banks MC9 - MC11 report MC errors from the CHA</td>	426H	1062	IA32_MC9_ADDR	Package	Banks MC9 - MC11 report MC errors from the CHA
429H 1065 IA32_MC10_STATUS Package 42AH 1066 IA32_MC10_ADDR Package 42BH 1067 IA32_MC10_MISC Package 42CH 1068 IA32_MC11_CTL Package 42DH 1069 IA32_MC11_STATUS Package 42EH 1070 IA32_MC11_ADDR Package 42FH 1071 IA32_MC11_MISC Package 430H 1072 IA32_MC12_CTL Package 431H 1073 IA32_MC12_STATUS Package 432H 1074 IA32_MC12_ADDR Package 433H 1075 IA32_MC13_CTL Package 434H 1076 IA32_MC13_CTL Package 434H 1076 IA32_MC13_CTL Package 435H 1077 IA32_MC13_STATUS Package 436H 1078 IA32_MC13_MISC Package 437H 1079 IA32_MC13_MISC Package 438H 1080 IA32_MC14_CTL Package	427H	1063	IA32_MC9_MISC	Package	
42AH 1066	428H	1064	IA32_MC10_CTL	Package	
42AH 1066 IA32_MC10_MISC Package 42CH 1068 IA32_MC11_CTL Package 42DH 1069 IA32_MC11_STATUS Package 42EH 1070 IA32_MC11_ADDR Package 42FH 1071 IA32_MC11_MISC Package 430H 1072 IA32_MC12_CTL Package 431H 1073 IA32_MC12_STATUS Package 432H 1074 IA32_MC12_ADDR Package 433H 1075 IA32_MC12_MISC Package 434H 1076 IA32_MC13_STATUS Package 435H 1077 IA32_MC13_STATUS Package 436H 1078 IA32_MC13_STATUS Package 437H 1079 IA32_MC13_STATUS Package 438H 1080 IA32_MC14_STATUS Package 438H 1080 IA32_MC14_STATUS Package 438H 1080 IA32_MC14_STATUS Package 438H 1081 IA32_MC14_STATUS Package </td <td>429H</td> <td>1065</td> <td>IA32_MC10_STATUS</td> <td>Package</td> <td></td>	429H	1065	IA32_MC10_STATUS	Package	
42CH 1068 IA32_MC11_CTL Package See Section 16.3.2.1, "IA32_MCi_CTL MSRs," through Section 16.3.2.4, "IA32_MCi_MISC MSRs." 42DH 1069 IA32_MC11_STATUS Package Section 16.3.2.4, "IA32_MCi_MISC MSRs." 42EH 1070 IA32_MC11_MISC Package Banks MC9 - MC11 report MC errors from the CHA. 43DH 1072 IA32_MC12_CTL Package See Section 16.3.2.1, "IA32_MCi_CTL MSRs," through Section 16.3.2.4, "IA32_MCi_MISC MSRs." 43H 1073 IA32_MC12_STATUS Package Section 16.3.2.4, "IA32_MCi_MISC MSRs." 43H 1075 IA32_MC12_MISC Package See Section 16.3.2.1, "IA32_MCi_CTL MSRs," through Section 16.3.2.4, "IA32_MCi_MISC MSRs." 43H 1076 IA32_MC13_STATUS Package See Section 16.3.2.4, "IA32_MCi_MISC MSRs." 43H 1071 IA32_MC13_ADDR Package Banks MC13 through MC 18 report MC errors from the integrated memory controllers. 43H 1079 IA32_MC13_MISC Package See Section 16.3.2.1, "IA32_MCi_CTL MSRs," through Section 16.3.2.4, "IA32_MCi_MISC MSRs." 43H 1080 IA32_MC14_STATUS Package See Section 16.3.2.4, "IA32_MCi_MISC MSRs."	42AH	1066	IA32_MC10_ADDR	Package	Banks MC9 - MC11 report MC errors from the CHA.
42DH 1069 IA32_MC11_STATUS Package 42EH 1070 IA32_MC11_ADDR Package 42FH 1071 IA32_MC11_MISC Package 430H 1072 IA32_MC12_CTL Package 431H 1073 IA32_MC12_STATUS Package 432H 1074 IA32_MC12_ADDR Package 433H 1075 IA32_MC12_MISC Package 434H 1076 IA32_MC13_STATUS Package 435H 1077 IA32_MC13_STATUS Package 436H 1078 IA32_MC13_ADDR Package 437H 1079 IA32_MC13_MISC Package 438H 1080 IA32_MC14_CTL Package 438H 1080 IA32_MC14_CTL Package 438H 1080 IA32_MC14_MISC Package 438H 1080 IA32_MC14_CTL Package 438H 1081 IA32_MC14_MISC Package 438H 1082 IA32_MC14_MISC Package	42BH	1067	IA32_MC10_MISC	Package	
42EH 1069 IA32_MC11_ADDR Package 42EH 1070 IA32_MC11_MISC Package 430H 1072 IA32_MC12_CTL Package 431H 1073 IA32_MC12_STATUS Package 432H 1074 IA32_MC12_ADDR Package 433H 1075 IA32_MC12_MISC Package 433H 1075 IA32_MC13_GTL Package 434H 1076 IA32_MC13_STATUS Package 435H 1077 IA32_MC13_STATUS Package 436H 1078 IA32_MC13_ADDR Package 437H 1079 IA32_MC13_ADDR Package 438H 1080 IA32_MC13_MISC Package 438H 1080 IA32_MC14_CTL Package 439H 1081 IA32_MC14_STATUS Package 439H 1081 IA32_MC14_ADDR Package 439H 1081 IA32_MC14_ADDR Package 439H 1082 IA32_MC14_ADDR Package	42CH	1068	IA32_MC11_CTL	Package	
42EH 1070 IA32_MC11_ADDR Package 42FH 1071 IA32_MC11_MISC Package 430H 1072 IA32_MC12_CTL Package 431H 1073 IA32_MC12_STATUS Package 432H 1074 IA32_MC12_ADDR Package 433H 1075 IA32_MC12_MISC Package 434H 1076 IA32_MC13_STATUS Package 435H 1077 IA32_MC13_STATUS Package 436H 1078 IA32_MC13_ADDR Package 437H 1079 IA32_MC13_MISC Package 438H 1080 IA32_MC14_CTL Package 438H 1080 IA32_MC14_CTL Package 439H 1081 IA32_MC14_STATUS Package 43AH 1082 IA32_MC14_ADDR Package 43BH 1083 IA32_MC14_STATUS Package 43BH 1081 IA32_MC14_STATUS Package 43BH 1082 IA32_MC14_ADDR Package <	42DH	1069	IA32_MC11_STATUS	Package	
430H 1072 IA32_MC12_CTL Package See Section 16.3.2.1, "IA32_MCi_CTL MSRs," through Section 16.3.2.4, "IA32_MCi_MISC MSRs." 431H 1073 IA32_MC12_STATUS Package Banks MC12 report MC errors from each channel of a link interconnect module. 432H 1074 IA32_MC12_MISC Package Banks MC12 report MC errors from each channel of a link interconnect module. 434H 1075 IA32_MC13_CTL Package See Section 16.3.2.1, "IA32_MCi_CTL MSRs," through Section 16.3.2.4, "IA32_MCi_MISC MSRs." 436H 1078 IA32_MC13_STATUS Package Banks MC13 through MC 18 report MC errors from the integrated memory controllers. 437H 1079 IA32_MC13_MISC Package See Section 16.3.2.1, "IA32_MCi_CTL MSRs," through Section 16.3.2.4, "IA32_MCi_MISC MSRs." 439H 1080 IA32_MC14_STATUS Package Section 16.3.2.1, "IA32_MCi_MISC MSRs." 43AH 1082 IA32_MC14_ADDR Package Banks MC13 through MC 18 report MC errors from the integrated memory controllers. 43BH 1083 IA32_MC15_STATUS Package See Section 16.3.2.1, "IA32_MCi_CTL MSRs," through Section 16.3.2.4, "IA32_MCi_MISC MSRs." 43DH 1085 IA32_MC15_ADDR <td>42EH</td> <td>1070</td> <td>IA32_MC11_ADDR</td> <td>Package</td> <td>Banks MC9 - MC11 report MC errors from the CHA.</td>	42EH	1070	IA32_MC11_ADDR	Package	Banks MC9 - MC11 report MC errors from the CHA.
431H 1073 IA32_MC12_STATUS Package Section 16.3.2.4, "IA32_MCi_MISC MSRs." 432H 1074 IA32_MC12_ADDR Package Banks MC12 report MC errors from each channel of a link interconnect module. 433H 1075 IA32_MC13_CTL Package See Section 16.3.2.1, "IA32_MCi_CTL MSRs," through Section 16.3.2.4, "IA32_MCi_MISC MSRs." 435H 1077 IA32_MC13_STATUS Package See Section 16.3.2.1, "IA32_MCi_MISC MSRs." 436H 1078 IA32_MC13_ADDR Package Banks MC13 through MC 18 report MC errors from the integrated memory controllers. 437H 1079 IA32_MC14_CTL Package See Section 16.3.2.1, "IA32_MCi_CTL MSRs," through Section 16.3.2.4, "IA32_MCi_MISC MSRs." 439H 1081 IA32_MC14_STATUS Package See Section 16.3.2.1, "IA32_MCi_MISC MSRs." 43H 1082 IA32_MC14_ADDR Package Banks MC13 through MC 18 report MC errors from the integrated memory controllers. 43CH 1084 IA32_MC15_STATUS Package See Section 16.3.2.1, "IA32_MCi_CTL MSRs," through Section 16.3.2.4, "IA32_MCi_MISC MSRs." 43DH 1085 IA32_MC15_ADDR Package See Section 16.3.2.4, "IA32_MCi_MISC MSRs.	42FH	1071	IA32_MC11_MISC	Package	
431H1073IA32_MC12_ADDRPackage432H1074IA32_MC12_ADDRPackage433H1075IA32_MC12_MISCPackage434H1076IA32_MC13_CTLPackage435H1077IA32_MC13_STATUSPackage436H1078IA32_MC13_ADDRPackage437H1079IA32_MC13_ADDRPackage438H1080IA32_MC13_MISCPackage439H1081IA32_MC14_CTLPackage43AH1082IA32_MC14_STATUSPackage43AH1082IA32_MC14_ADDRPackage43BH1083IA32_MC14_MISCPackage43CH1084IA32_MC15_CTLPackage43CH1085IA32_MC15_CTLPackage43CH1085IA32_MC15_CTLPackage43CH1086IA32_MC15_STATUSPackage43CH1086IA32_MC15_STATUSPackage43CH1086IA32_MC15_STATUSPackage43CH1086IA32_MC15_ADDRPackage See Section 16.3.2.1, "IA32_MC1_MISC MSRs." Banks MC13 through MC 18 report MC errors from the integrated memory controllers.	430H	1072	IA32_MC12_CTL	Package	
432H 1074 IA32_MC12_ADDR Package link interconnect module. 433H 1075 IA32_MC13_CTL Package See Section 16.3.2.1, "IA32_MCi_CTL MSRs," through Section 16.3.2.4, "IA32_MCi_MISC MSRs." 435H 1077 IA32_MC13_STATUS Package Section 16.3.2.4, "IA32_MCi_MISC MSRs." 436H 1078 IA32_MC13_ADDR Package Banks MC13 through MC 18 report MC errors from the integrated memory controllers. 437H 1079 IA32_MC13_MISC Package See Section 16.3.2.1, "IA32_MCi_CTL MSRs," through Section 16.3.2.4, "IA32_MCi_MISC MSRs." 439H 1081 IA32_MC14_STATUS Package Section 16.3.2.4, "IA32_MCi_MISC MSRs." 43AH 1082 IA32_MC14_ADDR Package Banks MC13 through MC 18 report MC errors from the integrated memory controllers. 43BH 1084 IA32_MC15_CTL Package See Section 16.3.2.1, "IA32_MCi_CTL MSRs," through Section 16.3.2.4, "IA32_MCi_MISC MSRs." 43DH 1085 IA32_MC15_STATUS Package See Section 16.3.2.4, "IA32_MCi_MISC MSRs." 43CH 1086 IA32_MC15_ADDR Package See Section 16.3.2.4, "IA32_MCi_MISC MSRs."	431H	1073	IA32_MC12_STATUS	Package	
434H 1076 IA32_MC13_CTL Package See Section 16.3.2.1, "IA32_MCi_CTL MSRs," through Section 16.3.2.4, "IA32_MCi_MISC MSRs." 436H 1078 IA32_MC13_ADDR Package Banks MC13 through MC 18 report MC errors from the integrated memory controllers. 437H 1079 IA32_MC13_MISC Package See Section 16.3.2.1, "IA32_MCi_CTL MSRs," through Section 16.3.2.4, "IA32_MCi_CTL MSRs," through Section 16.3.2.4, "IA32_MCi_CTL MSRs," through Section 16.3.2.4, "IA32_MCi_MISC MSRs." 438H 1080 IA32_MC14_STATUS Package Banks MC13 through MC 18 report MC errors from the integrated memory controllers. 438H 1082 IA32_MC14_ADDR Package See Section 16.3.2.1, "IA32_MCi_CTL MSRs," through Section 16.3.2.4, "IA3	432H	1074	IA32_MC12_ADDR	Package	·
435H1077IA32_MC13_STATUSPackageSection 16.3.2.4, "IA32_MCi_MISC MSRs."436H1078IA32_MC13_ADDRPackageBanks MC13 through MC 18 report MC errors from the integrated memory controllers.437H1079IA32_MC13_MISCPackageSee Section 16.3.2.1, "IA32_MCi_CTL MSRs," through Section 16.3.2.4, "IA32_MCi_MISC MSRs."439H1081IA32_MC14_STATUSPackageSee Section 16.3.2.4, "IA32_MCi_MISC MSRs."438H1082IA32_MC14_ADDRPackageBanks MC13 through MC 18 report MC errors from the integrated memory controllers.43BH1083IA32_MC14_MISCPackageSee Section 16.3.2.1, "IA32_MCi_CTL MSRs," through Section 16.3.2.4, "IA32_MCi_MISC MSRs."43DH1085IA32_MC15_STATUSPackageSee Section 16.3.2.4, "IA32_MCi_MISC MSRs."43EH1086IA32_MC15_ADDRPackageBanks MC13 through MC 18 report MC errors from the integrated memory controllers.	433H	1075	IA32_MC12_MISC	Package	
436H1077IA32_MC13_ADDRPackageBanks MC13 through MC 18 report MC errors from the integrated memory controllers.437H1079IA32_MC13_MISCPackageSee Section 16.3.2.1, "IA32_MCi_CTL MSRs," through Section 16.3.2.4, "IA32_MCi_MISC MSRs."438H1080IA32_MC14_STATUSPackageBanks MC13 through MC 18 report MC errors from the integrated memory controllers.438H1082IA32_MC14_ADDRPackageBanks MC13 through MC 18 report MC errors from the integrated memory controllers.438H1083IA32_MC14_MISCPackageSee Section 16.3.2.1, "IA32_MCi_CTL MSRs," through Section 16.3.2.4, "IA32_MCi_CTL MSRs," through Section 16.3.2.4, "IA32_MCi_MISC MSRs."43CH1085IA32_MC15_STATUSPackageSee Section 16.3.2.4, "IA32_MCi_MISC MSRs."43CH1086IA32_MC15_ADDRPackageBanks MC13 through MC 18 report MC errors from the integrated memory controllers.	434H	1076	IA32_MC13_CTL	Package	
436H1078IA32_MC13_ADDRPackage437H1079IA32_MC13_MISCPackage438H1080IA32_MC14_CTLPackageSee Section 16.3.2.1, "IA32_MCi_CTL MSRs," through Section 16.3.2.4, "IA32_MCi_MISC MSRs."439H1081IA32_MC14_STATUSPackageBanks MC13 through MC 18 report MC errors from the integrated memory controllers.43AH1082IA32_MC14_ADDRPackageSee Section 16.3.2.1, "IA32_MCi_CTL MSRs," through integrated memory controllers.43CH1084IA32_MC15_CTLPackageSee Section 16.3.2.1, "IA32_MCi_CTL MSRs," through Section 16.3.2.4, "IA32_MCi_MISC MSRs."43CH1085IA32_MC15_STATUSPackageSection 16.3.2.4, "IA32_MCi_MISC MSRs."43CH1086IA32_MC15_ADDRPackageBanks MC13 through MC 18 report MC errors from the integrated memory controllers.	435H	1077	IA32_MC13_STATUS	Package	
437H1079IA32_MC13_MISCPackage438H1080IA32_MC14_CTLPackageSee Section 16.3.2.1, "IA32_MCi_CTL MSRs," through Section 16.3.2.4, "IA32_MCi_MISC MSRs."439H1081IA32_MC14_STATUSPackageBanks MC13 through MC 18 report MC errors from the integrated memory controllers.43BH1083IA32_MC14_MISCPackageSee Section 16.3.2.1, "IA32_MCi_CTL MSRs," through Section 16.3.2.1, "IA32_MCi_CTL MSRs," through43CH1084IA32_MC15_CTLPackageSee Section 16.3.2.1, "IA32_MCi_CTL MSRs," through Section 16.3.2.4, "IA32_MCi_MISC MSRs."43CH1085IA32_MC15_STATUSPackageBanks MC13 through MC 18 report MC errors from the 	436H	1078	IA32_MC13_ADDR	Package	· · · · · · · · · · · · · · · · · · ·
439H1081IA32_MC14_STATUSPackageSection 16.3.2.4, "IA32_MCi_MISC MSRs."43AH1082IA32_MC14_ADDRPackageBanks MC13 through MC 18 report MC errors from the integrated memory controllers.43BH1083IA32_MC14_MISCPackageSee Section 16.3.2.1, "IA32_MCi_CTL MSRs," through Section 16.3.2.4, "IA32_MCi_MISC MSRs."43CH1085IA32_MC15_STATUSPackageSee Section 16.3.2.4, "IA32_MCi_MISC MSRs."43EH1086IA32_MC15_ADDRPackageBanks MC13 through MC 18 report MC errors from the integrated memory controllers.	437H	1079	IA32_MC13_MISC	Package	
439H1081IA32_MC14_STATUSPackageSection 16.3.2.4, "IA32_MCi_MISC MSRs."43AH1082IA32_MC14_ADDRPackageBanks MC13 through MC 18 report MC errors from the integrated memory controllers.43BH1083IA32_MC14_MISCPackageSee Section 16.3.2.1, "IA32_MCi_CTL MSRs," through Section 16.3.2.4, "IA32_MCi_MISC MSRs."43CH1085IA32_MC15_STATUSPackageSee Section 16.3.2.4, "IA32_MCi_MISC MSRs."43EH1086IA32_MC15_ADDRPackageBanks MC13 through MC 18 report MC errors from the integrated memory controllers.	438H	1080	IA32_MC14_CTL	Package	See Section 16.3.2.1, "IA32_MCi_CTL MSRs," through
43AH1082IA32_MC14_ADDRPackage43BH1083IA32_MC14_MISCPackage43CH1084IA32_MC15_CTLPackageSee Section 16.3.2.1, "IA32_MCi_CTL MSRs," through Section 16.3.2.4, "IA32_MCi_MISC MSRs."43DH1085IA32_MC15_STATUSPackageBanks MC13 through MC 18 report MC errors from the integrated memory controllers.	439H	1081			Section 16.3.2.4, "IA32_MCi_MISC MSRs."
43BH1083IA32_MC14_MISCPackage43CH1084IA32_MC15_CTLPackageSee Section 16.3.2.1, "IA32_MCi_CTL MSRs," through Section 16.3.2.4, "IA32_MCi_MISC MSRs."43DH1085IA32_MC15_STATUSPackageBanks MC13 through MC 18 report MC errors from the integrated memory controllers.	43AH	1082	IA32_MC14_ADDR	Package	
43DH 1085 IA32_MC15_STATUS Package Section 16.3.2.4, "IA32_MCi_MISC MSRs." 43EH 1086 IA32_MC15_ADDR Package Banks MC13 through MC 18 report MC errors from the integrated memory controllers.	43BH	1083	IA32_MC14_MISC	Package	miceg. steed memory controllers.
43DH 1085 IA32_MC15_STATUS Package Section 16.3.2.4, "IA32_MCi_MISC MSRs." 43EH 1086 IA32_MC15_ADDR Package Banks MC13 through MC 18 report MC errors from the integrated memory controllers.	43CH	1084	IA32_MC15_CTL	Package	See Section 16.3.2.1, "IA32_MCi_CTL MSRs," through
43EH 1086 IA32_MC15_ADDR Package Banks MC13 through MC 18 report MC errors from the integrated memory controllers.					Section 16.3.2.4, "IA32_MCi_MISC MSRs."
integrated memory controllers.					
, 	43FH	1087	IA32_MC15_MISC	Package	integrated memory controllers.

Table 2-50. MSRs Supported by the Intel® Xeon® Scalable Processor Family with a CPUID Signature DisplayFamily_DisplayModel Value of 06_55H (Contd.)

Regi Add		Register Name / Bit Fields	Scope	Bit Description
Hex	Dec	(Former MSR Name)		
440H	1088	IA32_MC16_CTL	Package	See Section 16.3.2.1, "IA32_MCi_CTL MSRs," through
441H	1089	IA32_MC16_STATUS	Package	Section 16.3.2.4, "IA32_MCi_MISC MSRs."
442H	1090	IA32_MC16_ADDR	Package	Banks MC13 through MC 18 report MC errors from the integrated memory controllers
443H	1091	IA32_MC16_MISC	Package	
444H	1092	IA32_MC17_CTL	Package	See Section 16.3.2.1, "IA32_MCi_CTL MSRs," through
445H	1093	IA32_MC17_STATUS	Package	Section 16.3.2.4, "IA32_MCi_MISC MSRs."
446H	1094	IA32_MC17_ADDR	Package	Banks MC13 through MC 18 report MC errors from the integrated memory controllers.
447H	1095	IA32_MC17_MISC	Package	
448H	1096	IA32_MC18_CTL	Package	See Section 16.3.2.1, "IA32_MCi_CTL MSRs," through
449H	1097	IA32_MC18_STATUS	Package	Section 16.3.2.4, "IA32_MCi_MISC MSRs."
44AH	1098	IA32_MC18_ADDR	Package	Banks MC13 through MC 18 report MC errors from the integrated memory controllers.
44BH	1099	IA32_MC18_MISC	Package	
44CH	1100	IA32_MC19_CTL	Package	See Section 16.3.2.1, "IA32_MCi_CTL MSRs," through
44DH	1101	IA32_MC19_STATUS	Package	Section 16.3.2.4, "IA32_MCi_MISC MSRs."
44EH	1102	IA32_MC19_ADDR	Package	Bank MC19 reports MC errors from a link interconnect module.
44FH	1103	IA32_MC19_MISC	Package	
606H	1542	MSR_RAPL_POWER_UNIT	Package	Unit Multipliers Used in RAPL Interfaces (R/O)
		3:0	Package	Power Units
				See Section 15.10.1, "RAPL Interfaces."
		7:4	Package	Reserved
		12:8	Package	Energy Status Units
				Energy related information (in Joules) is based on the multiplier, 1/2^ESU; where ESU is an unsigned integer represented by bits 12:8. Default value is 0EH (or 61 micro-joules).
		15:13	Package	Reserved
		19:16	Package	Time Units
				See Section 15.10.1, "RAPL Interfaces."
		63:20		Reserved
618H	1560	MSR_DRAM_POWER_LIMIT	Package	DRAM RAPL Power Limit Control (R/W)
				See Section 15.10.5, "DRAM RAPL Domain."
619H	1561	MSR_DRAM_ENERGY_STATUS	Package	DRAM Energy Status (R/O)
				Energy consumed by DRAM devices.
		31:0		Energy in 15.3 micro-joules. Requires BIOS configuration to enable DRAM RAPL mode 0 (Direct VR).
		63:32		Reserved

Table 2-50. MSRs Supported by the Intel® Xeon® Scalable Processor Family with a CPUID Signature DisplayFamily_DisplayModel Value of 06_55H (Contd.)

	ister ress	Register Name / Bit Fields (Former MSR Name)	Scope	Bit Description
Hex	Dec			
61BH	1563	MSR_DRAM_PERF_STATUS	Package	DRAM Performance Throttling Status (R/O)
				See Section 15.10.5, "DRAM RAPL Domain."
61CH	1564	MSR_DRAM_POWER_INFO	Package	DRAM RAPL Parameters (R/W)
				See Section 15.10.5, "DRAM RAPL Domain."
620H	1568	MSR UNCORE_RATIO_LIMIT	Package	Uncore Ratio Limit (R/W)
				Out of reset, the min_ratio and max_ratio fields represent the widest possible range of uncore frequencies. Writing to these fields allows software to control the minimum and the maximum frequency that hardware will select.
		63:15		Reserved
		14:8		MIN_RATIO
				Writing to this field controls the minimum possible ratio of the LLC/Ring.
		7		Reserved
		6:0		MAX_RATIO
				This field is used to limit the max ratio of the LLC/Ring.
639H	1593	MSR_PPO_ENERGY_STATUS	Package	Reserved (R/O)
				Reads return 0.
C8DH	3213	IA32_QM_EVTSEL	THREAD	Monitoring Event Select Register (R/W)
				If CPUID.(EAX=07H, ECX=0):EBX.RDT-M[bit 12] = 1.
		7:0		EventID (R/W)
				Event encoding:
				0x00: No monitoring.
				0x01: L3 occupancy monitoring. 0x02: Total memory bandwidth monitoring.
				0x03: Local memory bandwidth monitoring.
				All other encoding reserved.
		31:8		Reserved
		41:32		RMID (R/W)
		63:42		Reserved
C8FH	3215	IA32_PQR_ASSOC	THREAD	Resource Association Register (R/W)
		9:0		RMID
		31:10		Reserved
		51:32		COS (R/W)
		63: 52		Reserved
C90H	3216	IA32_L3_QOS_MASK_0	Package	L3 Class Of Service Mask - COS 0 (R/W)
				If CPUID.(EAX=10H, ECX=1):EDX.COS_MAX[15:0] >=0.
		0:19		CBM: Bit vector of available L3 ways for COS 0 enforcement.

Table 2-50. MSRs Supported by the Intel® Xeon® Scalable Processor Family with a CPUID Signature DisplayFamily_DisplayModel Value of 06_55H (Contd.)

	ister ress	Register Name / Bit Fields	Scope	Bit Description
Hex	Dec	(Former MSR Name)		
		63:20		Reserved
C91H	3217	IA32_L3_QOS_MASK_1	Package	L3 Class Of Service Mask - COS 1 (R/W)
				If CPUID.(EAX=10H, ECX=1):EDX.COS_MAX[15:0] >=1.
		0:19		CBM: Bit vector of available L3 ways for COS 1 enforcement.
		63:20		Reserved
C92H	3218	IA32_L3_QOS_MASK_2	Package	L3 Class Of Service Mask - COS 2 (R/W)
				If CPUID.(EAX=10H, ECX=1):EDX.COS_MAX[15:0] >=2.
		0:19		CBM: Bit vector of available L3 ways for COS 2 enforcement.
		63:20		Reserved
C93H	3219	IA32_L3_QOS_MASK_3	Package	L3 Class Of Service Mask - COS 3 (R/W). If CPUID.(EAX=10H, ECX=1):EDX.COS_MAX[15:0] >=3.
		0:19		CBM: Bit vector of available L3 ways for COS 3 enforcement.
		63:20		Reserved
C94H	3220	IA32_L3_QOS_MASK_4	Package	L3 Class Of Service Mask - COS 4 (R/W)
				If CPUID.(EAX=10H, ECX=1):EDX.COS_MAX[15:0] >=4.
		0:19		CBM: Bit vector of available L3 ways for COS 4 enforcement.
		63:20		Reserved
C95H	3221	IA32_L3_QOS_MASK_5	Package	L3 Class Of Service Mask - COS 5 (R/W) If CPUID.(EAX=10H, ECX=1):EDX.COS_MAX[15:0] >=5.
		0:19		CBM: Bit vector of available L3 ways for COS 5 enforcement.
		63:20		Reserved
C96H	3222	IA32_L3_QOS_MASK_6	Package	L3 Class Of Service Mask - COS 6 (R/W)
				If CPUID.(EAX=10H, ECX=1):EDX.COS_MAX[15:0] >=6.
		0:19		CBM: Bit vector of available L3 ways for COS 6 enforcement.
		63:20		Reserved
C97H	3223	IA32_L3_QOS_MASK_7	Package	L3 Class Of Service Mask - COS 7 (R/W)
				If CPUID.(EAX=10H, ECX=1):EDX.COS_MAX[15:0] >=7.
		0:19		CBM: Bit vector of available L3 ways for COS 7 enforcement.
		63:20		Reserved
C98H	3224	IA32_L3_QOS_MASK_8	Package	L3 Class Of Service Mask - COS 8 (R/W)
				If CPUID.(EAX=10H, ECX=1):EDX.COS_MAX[15:0] >=8.
		0:19		CBM: Bit vector of available L3 ways for COS 8 enforcement.

Table 2-50. MSRs Supported by the Intel® Xeon® Scalable Processor Family with a CPUID Signature DisplayFamily_DisplayModel Value of 06_55H (Contd.)

	ister ress	Register Name / Bit Fields	Scope	Bit Description
Hex	Dec	(Former MSR Name)		
		63:20		Reserved
C99H	3225	IA32_L3_QOS_MASK_9	Package	L3 Class Of Service Mask - COS 9 (R/W) If CPUID.(EAX=10H, ECX=1):EDX.COS_MAX[15:0] >=9.
		0:19		CBM: Bit vector of available L3 ways for COS 9 enforcement.
		63:20		Reserved
C9AH	3226	IA32_L3_QOS_MASK_10	Package	L3 Class Of Service Mask - COS 10 (R/W)
				If CPUID.(EAX=10H, ECX=1):EDX.COS_MAX[15:0] >=10.
		0:19		CBM: Bit vector of available L3 ways for COS 10 enforcement.
		63:20		Reserved
C9BH	3227	IA32_L3_QOS_MASK_11	Package	L3 Class Of Service Mask - COS 11 (R/W) If CPUID.(EAX=10H, ECX=1):EDX.COS_MAX[15:0] >=11.
		0:19		CBM: Bit vector of available L3 ways for COS 11 enforcement.
		63:20		Reserved
C9CH	3228	IA32_L3_QOS_MASK_12	Package	L3 Class Of Service Mask - COS 12 (R/W)
				If CPUID.(EAX=10H, ECX=1):EDX.COS_MAX[15:0] >=12.
		0:19		CBM: Bit vector of available L3 ways for COS 12 enforcement.
		63:20		Reserved
C9DH	3229	IA32_L3_QOS_MASK_13	Package	L3 Class Of Service Mask - COS 13 (R/W)
				If CPUID.(EAX=10H, ECX=1):EDX.COS_MAX[15:0] >=13.
		0:19		CBM: Bit vector of available L3 ways for COS 13 enforcement.
		63:20		Reserved
C9EH	3230	IA32_L3_QOS_MASK_14	Package	L3 Class Of Service Mask - COS 14 (R/W) If CPUID.(EAX=10H, ECX=1):EDX.COS_MAX[15:0] >=14.
		0:19		CBM: Bit vector of available L3 ways for COS 14 enforcement.
		63:20		Reserved
C9FH	3231	IA32_L3_QOS_MASK_15	Package	L3 Class Of Service Mask - COS 15 (R/W)
				If CPUID.(EAX=10H, ECX=1):EDX.COS_MAX[15:0] >=15.
		0:19		CBM: Bit vector of available L3 ways for COS 15 enforcement.

Table 2-50. MSRs Supported by the Intel® Xeon® Scalable Processor Family with a CPUID Signature DisplayFamily_DisplayModel Value of 06_55H (Contd.)

_	ister ress	Register Name / Bit Fields	Scope	Bit Description
Hex	Dec	(Former MSR Name)		
		63:20		Reserved

2.17.7 MSRs Specific to 3rd Generation Intel® Xeon® Scalable Processor Family Based on Ice Lake Microarchitecture

The 3rd generation Intel[®] Xeon[®] Scalable Processor Family based on Ice Lake microarchitecture (CPUID Signature DisplayFamily_DisplayModel value of 06_6AH or 06_6CH) support the MSRs listed in Table 2-51.

Table 2-51. MSRs Supported by the 3rd Generation Intel® Xeon® Scalable Processor Family with a CPUID Signature DisplayFamily_DisplayModel Value of 06_6AH or 06_6CH

	ister ress	Register Name / Bit Fields	Scope	Bit Description
Hex	Dec			
612H	1554	MSR_PACKAGE_ENERGY_TIME_STATUS	Package	Package energy consumed by the entire CPU (R/W)
		31:0		Total amount of energy consumed since last reset.
		63:32		Total time elapsed when the energy was last updated. This is a monotonic increment counter with auto wrap back to zero after overflow. Unit is 10ns.
618H	1560	MSR_DRAM_POWER_LIMIT	Package	Allows software to set power limits for the DRAM domain and measurement attributes associated with each limit.
		14:0		DRAM_PP_PWR_LIM:
				Power Limit[0] for DDR domain. Units = Watts, Format = 11.3, Resolution = 0.125W, Range = 0-2047.875W.
		15		PWR_LIM_CTRL_EN:
				Power Limit[0] enable bit for DDR domain.
		16		Reserved
		23:17		CTRL_TIME_WIN:
				Power Limit[0] time window Y value, for DDR domain. Actual time_window for RAPL is:
				(1/1024 seconds) * (1+(x/4)) * (2^y)
		62:24		Reserved
		63		PP_PWR_LIM_LOCK:
				When set, this entire register becomes read-only. This bit will typically be set by BIOS during boot.
619H	1561	MSR_DRAM_ENERGY_STATUS	Package	DRAM Energy Status (R/O)
				See Section 15.10.5, "DRAM RAPL Domain."
		31:0		Energy in 15.3 micro-joules. Requires BIOS configuration to enable DRAM RAPL mode 0 (Direct VR).
		63:32		Reserved

Table 2-51. MSRs Supported by the 3rd Generation Intel® Xeon® Scalable Processor Family with a CPUID Signature DisplayFamily_DisplayModel Value of 06_6AH or 06_6CH

Regi Add		Register Name / Bit Fields	Scope	Bit Description
Hex	Dec			
61BH	1563	MSR_DRAM_PERF_STATUS	Package	DRAM Performance Throttling Status (R/O) See Section 15.10.5, "DRAM RAPL Domain."
61CH	1564	MSR_DRAM_POWER_INFO	Package	DRAM Power Parameters (R/W)
		14:0		Spec DRAM Power (DRAM_TDP): The Spec power allowed for DRAM. The TDP setting is typical (not guaranteed). The units for this value are defined in MSR_DRAM_POWER_INFO_UNIT[PWR_UNIT].
		15		Reserved
		30:16		Minimal DRAM Power (DRAM_MIN_PWR): The minimal power setting allowed for DRAM. Lower values will be clamped to this value. The minimum setting is typical (not guaranteed). The units for this value are defined in MSR_DRAM_POWER_INFO_UNIT[PWR_UNIT].
		31		Reserved
		46:32		Maximal Package Power (DRAM_MAX_PWR): The maximal power setting allowed for DRAM. Higher values will be clamped to this value. The maximum setting is typical (not guaranteed). The units for this value are defined in MSR_DRAM_POWER_INFO_UNIT[PWR_UNIT].
		47		Reserved
		54:48		Maximal Time Window (DRAM_MAX_WIN): The maximal time window allowed for the DRAM. Higher values will be clamped to this value. x = PKG_MAX_WIN[54:53] y = PKG_MAX_WIN[52:48] The timing interval window is a floating-point number given by 1.x *power(2,y). The unit of measurement is defined in MSR_DRAM_POWER_INFO_UNIT[TIME_UNIT].
		62:55		Reserved
		63		LOCK: Lock bit to lock the register.
981H	2433	IA32_TME_CAPABILITY		See Table 2-2.
982H	2434	IA32_TME_ACTIVATE		See Table 2-2.
983H	2435	IA32_TME_EXCLUDE_MASK		See Table 2-2.
984H	2436	IA32_TME_EXCLUDE_BASE		See Table 2-2.

2.17.8 MSRs Specific to the 4th Generation Intel® Xeon® Scalable Processor Family Based on Sapphire Rapids Microarchitecture

The 4th generation Intel[®] Xeon[®] Scalable Processor Family based on Sapphire Rapids microarchitecture (CPUID Signature DisplayFamily_DisplayModel value of 06_8FH) supports the MSRs listed in Section 2.17, "MSRs In the 6th Generation, 7th Generation, 8th Generation, 9th Generation, 10th Generation, 11th Generation, 12th Generation, and 13th Generation Intel® Core[™] Processors, Intel® Xeon® Scalable Processor Family, 2nd, 3rd, and 4th Generation Intel® Xeon® Scalable Processor Family, 8th Generation Intel® Core[™] i3 Processors, and Intel® Xeon® E processors," including Table 2-52. For an MSR listed in Table 2-52 that also appears in the model-specific tables of prior generations, Table 2-52 supersedes prior generation tables.

Table 2-52. Additional MSRs Supported by the 4th Generation Intel® Xeon® Scalable Processor Family with a CPUID Signature DisplayFamily DisplayModel Value of 06 8FH

Register Address		Register Name / Bit Fields Scope	Bit Description	
Hex	Dec			
33H	51	MSR_MEMORY_CTRL	Core	Memory Control Register (R/W)
		27:0		Reserved.
		28		UC_LOCK_DISABLE
				If set to 1, a UC lock will cause a #GP(0) exception.
				See Section 9.1.2.3, "Features to Disable Bus Locks."
		29		SPLIT_LOCK_DISABLE
				If set to 1, a split lock will cause an #AC(0) exception.
				See Section 9.1.2.3, "Features to Disable Bus Locks."
		31:30		Reserved.
A7H	167	MSR_BIOS_DEBUG	Thread	BIOS DEBUG (R/O)
				See Table 2-45.
BCH	188	IA32_MISC_PACKAGE_CTLS	Package	Power Filtering Control (R/W)
				IA32_ARCH_CAPABILITIES[bit 10] enumerates
				support for this MSR. See Table 2-2.
CFH	207	LAZZ CODE CADADILITIES	Cons	
CFH	207	IA32_CORE_CAPABILITIES	Соге	IA32 Core Capabilities Register (R/W) If CPUID.(EAX=07H, ECX=0):EDX[30] = 1.
				This MSR provides an architectural enumeration
				function for model-specific behavior.
		0		Reserved: returns zero.
		1		Reserved: returns zero.
		2		INTEGRITY_CAPABILITIES
				When set to 1, the processor supports MSR_INTEGRITY_CAPABILITIES.
		3		RSM_IN_CPLO_ONLY
				Indicates that RSM will only be allowed in CPLO and will #GP for all non-CPLO privilege levels.
		4		UC_LOCK_DISABLE_SUPPORTED
				When read as 1, software can set bit 28 of MSR_MEMORY_CTRL (MSR address 33H).

Table 2-52. Additional MSRs Supported by the 4th Generation Intel® Xeon® Scalable Processor Family with a CPUID Signature DisplayFamily_DisplayModel Value of 06_8FH

	ister ress	Register Name / Bit Fields	Scope	Bit Description
Hex	Dec			
		5		SPLIT_LOCK_DISABLE_SUPPORTED
				When read as 1, software can set bit 29 of MSR_MEMORY_CTRL.
		6		Reserved: returns zero.
		7		UC_STORE_THROTTLING_SUPPORTED
				Indicates that the snoop filter quality of service MSRs are supported on this core. This is based on the existence of a non-inclusive cache and the L2/MLC QoS feature supported.
		63:8		Reserved: returns zero.
E1H	225	IA32_UMWAIT_CONTROL		UMWAIT Control (R/W)
				See Table 2-2.
EDH	237	MSR_RAR_CONTROL	Thread	RAR Control (R/W)
		63:32		Reserved.
		31		ENABLE
				RAR events are recognized. When RAR is not enabled, RARs are dropped.
		30		IGNORE_IF
				Allow RAR servicing at the RLP regardless of the value of RFLAGS.IF.
		29:0		Reserved.
EEH	238	MSR_RAR_ACTION_VECTOR_BASE	Thread	Pointer to RAR Action Vector (R/W)
		63:MAXPHYADDR		Reserved.
		MAXPHYADDR-1:6		VECTOR_PHYSICAL_ADDRESS
				Pointer to the physical address of the 64B aligned RAR action vector.
		5:0		Reserved.
EFH	239	MSR_RAR_PAYLOAD_TABLE_BASE	Thread	Pointer to Base of RAR Payload Table (R/W)
		63:MAXPHYADDR		Reserved.
		MAXPHYADDR-1:12		TABLE_PHYSICAL_ADDRESS
				Pointer to the base physical address of the 4K aligned RAR payload table.
		11:0		Reserved.
F0H	240	MSR_RAR_INFO	Thread	Read Only RAR Information (RO)
		63:38		Always zero.
		37:32		Table Max Index
				Maximum supported payload table index.
		31:0		Supported payload type bitmap. A value of 1 in bit position [i] indicates that payload type [i] is supported.

Table 2-52. Additional MSRs Supported by the 4th Generation Intel® Xeon® Scalable Processor Family with a CPUID Signature DisplayFamily_DisplayModel Value of 06_8FH

Regi Add		Register Name / Bit Fields	Scope	Bit Description
Hex	Dec			
105H	261	MSR_CORE_BIST	Core	Core BIST (R/W) Controls Array BIST activation and status checking as part of FUSA.
		31:0		BIST_ARRAY
				Bitmap indicating which arrays to run BIST on (WRITE).
				Bitmap indicating which arrays were not processed, i.e., completion mask (READ).
		39:32		BANK
				Array bank of the [least significant set bit] array indicated in EAX to start BIST(WRITE).
				Array bank interrupted or failed (READ).
		47:40		DWORD
				Array dword of the [least significant set bit] array indicated in EAX to start BIST (WRITE).
				Array dword interrupted or failed (READ).
		62:48		Reserved
		63		CTRL_RESULT
				Indicates whether WRMSR should signal Machine- Check upon BIST-error (WRITE).
				BIST result PASS(0)/FAIL(1) of the (least significant set bit) array indicated in EAX (READ).
10AH	266	IA32_ARCH_CAPABILITIES		Enumeration of Architectural Features (R/O) See Table 2-2.
1A4H	420	MSR_PREFETCH_CONTROL		Prefetch Disable Bits (R/W)
.,,,,,		0		L2_HARDWARE_PREFETCHER_DISABLE
				If 1, disables the L2 hardware prefetcher, which fetches additional lines of code or data into the L2 cache.
		1		L2_ADJACENT_CACHE_LINE_PREFETCHER_DISABLE
				If 1, disables the adjacent cache line prefetcher, which fetches the cache line that comprises a cache line pair (128 bytes).
		2		DCU_HARDWARE_PREFETCHER_DISABLE
				If 1, disables the L1 data cache prefetcher, which fetches the next cache line into L1 data cache.
		3		DCU_IP_PREFETCHER_DISABLE
				If 1, disables the L1 data cache IP prefetcher, which uses sequential load history (based on instruction pointer of previous loads) to determine whether to prefetch additional lines.
		4		Reserved.

Table 2-52. Additional MSRs Supported by the 4th Generation Intel® Xeon® Scalable Processor Family with a CPUID Signature DisplayFamily_DisplayModel Value of 06_8FH

1ADH 4 1AEH 4 1C4H 4 1C5H 4	429 430 452	5 63:6 MSR_PRIMARY_TURBO_RATIO_LIMIT MSR_TURBO_RATIO_LIMIT_CORES	Package	AMP_PREFETCH_DISABLE If 1, disables the L2 Adaptive Multipath Probability (AMP) prefetcher. Reserved. Primary Maximum Turbo Ratio Limit (R/W)
1AEH 4 1C4H 4 1C5H 4	430	63:6 MSR_PRIMARY_TURBO_RATIO_LIMIT MSR_TURBO_RATIO_LIMIT_CORES	Package	If 1, disables the L2 Adaptive Multipath Probability (AMP) prefetcher. Reserved.
1AEH 4 1C4H 4 1C5H 4	430	MSR_PRIMARY_TURBO_RATIO_LIMIT MSR_TURBO_RATIO_LIMIT_CORES	Package	
1AEH 4 1C4H 4 1C5H 4	430	MSR_TURBO_RATIO_LIMIT_CORES	Package	Primary Maximum Turbo Ratio Limit (R/W)
1C4H 4				See Table 2-46.
1C5H 4	452		Package	See Table 2-50.
		IA32_XFD		Extended Feature Detect (R/W) See Table 2-2.
2C2H 7	453	IA32_XFD_ERR		XFD Error Code (R/W) See Table 2-2.
	706	MSR_COPY_SCAN_HASHES	Die	COPY_SCAN_HASHES (W)
		63:0		SCAN_HASH_ADDR Contains the linear address of the SCAN Test HASH Binary loaded into memory.
2C3H 7	707	MSR_SCAN_HASHES_STATUS		SCAN_HASHES_STATUS (R/O)
		15:0	Die	CHUNK_SIZE
				Chunk size of the test in KB.
		23:16	Die	NUM_CHUNKS
				Total number of chunks.
		31:24		Reserved: all zeros.
		39:32	Thread	ERROR_CODE The error-code refers to the LP that runs WRMSR(2C2H). Ox0: No error reported. Ox1: Attempt to copy scan-hashes when copy already in progress. Ox2: Secure Memory not set up correctly. Ox3: Scan-image header Image_info.ProgramID doesn't match RDMSR(2D9H)[31:24], or scan-image header Processor-Signature doesn't match F/M/S, or scan-image header Processor-Flags doesn't match PlatformID. Ox4: Reserved Ox5: Integrity check failed. Ox6: Re-install of scan test image attempted when current scan test image is in use by other LPs.

Table 2-52. Additional MSRs Supported by the 4th Generation Intel® Xeon® Scalable Processor Family with a CPUID Signature DisplayFamily_DisplayModel Value of 06_8FH

Regi: Addr		Register Name / Bit Fields	Scope	Bit Description
Hex	Dec			
		62:51	Die	MAX_CORE_LIMIT Maximum Number of cores that can run Intel® In-field Scan simultaneously minus 1. O means 1 core at a time.
		63	Die	Valid Valid bit is set when COPY_SCAN_HASHES has completed successfully.
2C4H	708	MSR_AUTHENTICATE_AND_COPY_CHUNK	Die	AUTHENTICATE_AND_COPY_CHUNK (W)
		7:0		CHUNK_INDEX
				Chunk Index, should be less than the total number of chunks defined by NUM_CHUNKS (MSR_SCAN_HASHES_STATUS[23:16]).
		63:8		CHUNK_ADDR
				Bits 63:8 of 256B aligned Linear address of scan chunk in memory.
2C5H	709	MSR_CHUNKS_AUTHENTICATION_STATUS		CHUNKS_AUTHENTICATION_STATUS (R/O)
		7:0	Die	VALID_CHUNKS
				Total number of Valid (authenticated) chunks.
		15:8	Die	TOTAL_CHUNKS
				Total number of chunks.
		31:16		Reserved: all zeros.
		39:32	Thread	ERROR_CODE
				The error code refers to the LP that runs WRMSR(2C4H).
				0x0: No error reported.
				0x1: Attempt to authenticate a CHUNK which is already marked as authentic or is currently being installed by another core.
				0x2: CHUNK authentication error. HASH of chunk did not match expected value.
		63:40		Reserved: set to all zeros.
2C6H	710	MSR_ACTIVATE_SCAN	Thread	ACTIVATE_SCAN (W)
		7:0		CHUNK_START_INDEX
				Indicates chunk index to start from.
		15:8		CHUNK_STOP_INDEX
				Indicates what chunk index to stop at (inclusive).
		31:16		Reserved: all zeros.
		62:32		THREAD_WAIT_DELAY
				TSC based delay to allow threads to rendezvous.

Table 2-52. Additional MSRs Supported by the 4th Generation Intel® Xeon® Scalable Processor Family with a CPUID Signature DisplayFamily_DisplayModel Value of 06_8FH

Regi Add		Register Name / Bit Fields	Scope	Bit Description
Hex	Dec			
		63		SIGNAL_MCE
				If 1, then on scan-error log MC in MC4_STATUS and signal MCE if machine check signaling enabled in MC4_CTL[0].
				If 0, then no logging/no signaling.
2C7H	711	MSR_SCAN_STATUS		SCAN_STATUS (R/O)
		7:0	Соге	CHUNK_NUM
				SCAN Chunk that was reached.
		15:8	Core	CHUNK_STOP_INDEX
				Indicates what chunk index to stop at (inclusive). Maps to same field in WRMSR(ACTIVATE_SCAN).
		31:16		Reserved: return all zeros.
		39:32	Thread	ERROR_CODE
				0x0: No error.
				Ox1: SCAN operation did not start. Other thread did not join in time.
				0x2: SCAN operation did not start. Interrupt occurred prior to threads rendezvous.
				0x3: SCAN operation did not start. Power Management conditions are inadequate to run Intel Infield Scan.
				Ox4: SCAN operation did not start. Non-valid chunks in the range CHUNK_STOP_INDEX: CHUNK_START_INDEX.
				0x5: SCAN operation did not start. Mismatch in arguments between threads T0/T1.
				Ox6: SCAN operation did not start. Core not capable of performing SCAN currently.
				Ox8: SCAN operation did not start. Exceeded number of Logical Processors (LP) allowed to run Intel In-field Scan concurrently. MAX_CORE_LIMIT exceeded.
				0x9: Interrupt occurred. Scan operation aborted prematurely, not all chunks requested have been executed.
		61:40		Reserved: return all zeros.
		62	Core	SCAN_CONTROL_ERROR
				Scan-System-Controller malfunction.
		63	Core	SCAN_SIGNATURE_ERROR
				Core failed SCAN-SIGNATURE checking for this chunk.
2C8H	712	MSR_SCAN_MODULE_ID	Module	SCAN_MODULE_ID (R/O)
		31:0		RevID of the currently installed scan test image. Maps to Revision field in external header (offset 4).
		63:32		Reserved: return all zeros.
		1		

Table 2-52. Additional MSRs Supported by the 4th Generation Intel® Xeon® Scalable Processor Family with a CPUID Signature DisplayFamily_DisplayModel Value of 06_8FH

Regi Add		Register Name / Bit Fields	Scope	Bit Description
Hex	Dec			
2C9H	713	MSR_LAST_SAF_WP	Core	LAST_SAF_WP (R/O)
		31:0		LAST_WP
				Provides information about the core when the last WRMSR(ACTIVATE_SCAN) was executed. Available only if enumerated in MSR_INTEGRITY_CAPABILITIES[10:9].
		63:32		Reserved: return all zeros.
2D9H	729	MSR_INTEGRITY_CAPABILITIES	Module	INTEGRITY_CAPABILITIES (R/O)
		0		STARTUP_SCAN_BIST
				When set, supports Intel In-field Scan.
		3:1		Reserved: return all zeros.
		4		PERIODIC_SCAN_BIST
				When set, supports Intel In-field Scan.
		23:5		Reserved: return all zeros.
		31:24		ID of the scan programs supported for this part. WRMSR(2C2H) verifies this value against the corresponding value in the scan-image header, i.e., Image_info.
410H	1040	IA32_MC4_CTL	Package	See Section 16.3.2.1, "IA32_MCi_CTL MSRs," through
411H	1041	IA32_MC4_STATUS	Package	Section 16.3.2.4, "IA32_MCi_MISC MSRs."
412H	1042	IA32_MC4_ADDR	Package	Bank MC4 reports MC errors from the PCU module. — If SIGNAL_MCE is set, a Scan Status is logged in
413H	1043	IA32_MC4_MISC	Package	MC4_STATUS and MC4_MISC.
492H	1170	IA32_VMX_PROCBASED_CTLS3		Capability Reporting Register of Tertiary Processor- Based VM-Execution Controls (R/O)
				See Table 2-2.
493H	1171	IA32_VMX_EXIT_CTLS2		Capability Reporting Register of Secondary VM-Exit Controls (R/O)
				See Table 2-2.
540H	1344	MSR_THREAD_UARCH_CTL	Thread	Thread Microarchitectural Control (R/W) See Table 2-47.
64DH	1613	MSR_PLATFORM_ENERGY_STATUS	Package	Platform Energy Status (R/O)
		31:0		TOTAL_ENERGY_CONSUMED
				Total energy consumption in J (32.0), in 10nsec units.
		63:32		TIME_STAMP
				Time stamp (U32.0).
65CH	1628	MSR_PLATFORM_POWER_LIMIT	Package	Platform Power Limit Control (R/W-L)

Table 2-52. Additional MSRs Supported by the 4th Generation Intel® Xeon® Scalable Processor Family with a CPUID Signature DisplayFamily_DisplayModel Value of 06_8FH

Regi Addı		Register Name / Bit Fields	Scope	Bit Description
Hex	Dec			
		16:0		POWER_LIMIT_1
				The average power limit value that the platform must not exceed over a time window as specified by the Power_Limit_1_TIME field.
				The default value is the Thermal Design Power (TDP) and varies with product skus. The unit is specified in MSR_RAPL_POWER_UNIT.
		17		POWER_LIMIT_1_EN
				When set, the processor can apply control policies such that the platform average power does not exceed the Power_Limit_1 value over an exponential weighted moving average of the time window.
		18		CRITICAL_POWER_CLAMP_1
				When set, the processor can go below the OS-requested P States to maintain the power below the specified Power_Limit_1 value.
		25:19		POWER_LIMIT_1_TIME
				This indicates the time window over which the Power_Limit_1 value should be maintained.
				This field is made up of two numbers from the following equation:
				Time Window = $(float)((1+(X/4))*(2^Y))$, where:
				X = POWER_LIMIT_1_TIME[23:22]
				Y = POWER_LIMIT_1_TIME[21:17]
				The maximum allowed value in this field is defined in MSR_PKG_POWER_INFO[PKG_MAX_WIN].
				The default value is ODH, and the unit is specified in MSR_RAPL_POWER_UNIT[Time Unit].
		31:26		Reserved
		48:32		POWER_LIMIT_2
				This is the Duration Power limit value that the platform must not exceed.
				The unit is specified in MSR_RAPL_POWER_UNIT.
		49		Enable Platform Power Limit #2
				When set, enables the processor to apply control policy such that the platform power does not exceed Platform Power limit #2 over the Short Duration time window.
		50		Platform Clamping Limitation #2
				When set, allows the processor to go below the OS requested P states in order to maintain the power below specified Platform Power Limit #2 value.

Table 2-52. Additional MSRs Supported by the 4th Generation Intel® Xeon® Scalable Processor Family with a CPUID Signature DisplayFamily_DisplayModel Value of 06_8FH

Register Address		Register Name / Bit Fields	Scope	Bit Description
Hex	Dec			
		57:51		POWER_LIMIT_2_TIME This indicates the time window over which the Power_Limit_2 value should be maintained. This field has the same format as the POWER_LIMIT_1_TIME field.
		62:58		Reserved
		63		LOCK Setting this bit will lock all other bits of this MSR until system RESET.
665H	1637	MSR_PLATFORM_POWER_INFO	Package	Platform Power Information (R/W)
		16:0		MAX_PPL1 Maximum PP L1 value. The unit is specified in MSR_RAPL_POWER_UNIT.
		31:17		MIN_PPL1 Minimum PP L1 value. The unit is specified in MSR_RAPL_POWER_UNIT.
		48:32		MAX_PPL2 Maximum PP L2 value. The unit is specified in MSR_RAPL_POWER_UNIT.
		55:49		MAX_TW Maximum time window. The unit is specified in MSR_RAPL_POWER_UNIT.
		62:56		Reserved
		63		LOCK Setting this bit will lock all other bits of this MSR until system RESET.
666H	1638	MSR_PLATFORM_RAPL_SOCKET_PERF_ STATUS	Package	Platform RAPL Socket Performance Status (R/O)
		31:0		Count of limited performance due to platform RAPL limit.
6A0H	1696	IA32_U_CET		Configure User Mode CET (R/W) See Table 2-2.
6A2H	1698	IA32_S_CET		Configure Supervisor Mode CET (R/W) See Table 2-2.
6A4H	1700	IA32_PL0_SSP		Linear address to be loaded into SSP on transition to privilege level 0. (R/W) See Table 2-2.
6A5H	1701	IA32_PL1_SSP		Linear address to be loaded into SSP on transition to privilege level 1. (R/W) See Table 2-2.

Table 2-52. Additional MSRs Supported by the 4th Generation Intel® Xeon® Scalable Processor Family with a CPUID Signature DisplayFamily_DisplayModel Value of 06_8FH

privilege level 2. (R/W) See Table 2-2. 6A7H 1703 IA32_PL3_SSP Linear address to be loaded into SSP on transition to privilege level 3. (R/W) See Table 2-2. 6A8H 1704 IA32_INTERRUPT_SSP_TABLE_ADDR Linear address of a table of seven shadow stack	Register Address		Register Name / Bit Fields	Scope	Bit Description
privilege level 2. (R/W) See Table 2-2. 6A7H 1703 IA32_PL3_SSP Linear address to be loaded into SSP on transition to privilege level 3. (R/W) See Table 2-2. 6A8H 1704 IA32_INTERRUPT_SSP_TABLE_ADDR Linear address of a table of seven shadow stack pointers that are selected in IA-32e mode using the IST index (when not 0) from the interrupt gate descriptor. (R/W) See Table 2-2. 6E1H 1761 IA32_PKRS Specifies the PK permissions associated with each protection domain for supervisor pages (R/W) See Table 2-2. 776H 1910 IA32_HWP_CTL See Table 2-2. 981H 2433 IA32_TME_CAPABILITY Memory Encryption Capability MSR See Table 2-2. 985H 2437 IA32_UINTR_RR User Interrupt Request Register (R/W) See Table 2-2. 986H 2438 IA32_UINTR_HANDLER User Interrupt Handler Address (R/W) See Table 2-2. 987H 2439 IA32_UINTR_STACKADJUST User Interrupt Stack Adjustment (R/W) See Table 2-2. 988H 2440 IA32_UINTR_MISC User-Interrupt Target-Table Size and Notification Vector (R/W) See Table 2-2. 989H 2441 IA32_UINTR_PD User Interrupt PID Address (R/W) See Table 2-2. 989H 2442 IA32_UINTR_TT User-Interrupt Target Table (R/W) See Table 2-2.	Hex	Dec			
privilege level 3. (R/W) See Table 2-2. 6A8H 1704 IA32_INTERRUPT_SSP_TABLE_ADDR Linear address of a table of seven shadow stack pointers that are selected in IA-32e mode using the IST index (when not 0) from the interrupt gate descriptor. (R/W) See Table 2-2. 6E1H 1761 IA32_PKRS Specifies the PK permissions associated with each protection domain for supervisor pages (R/W) See Table 2-2. 776H 1910 IA32_HWP_CTL See Table 2-2. 981H 2433 IA32_TME_CAPABILITY Memory Encryption Capability MSR See Table 2-2. 985H 2437 IA32_UINTR_RR User Interrupt Request Register (R/W) See Table 2-2. 986H 2438 IA32_UINTR_HANDLER User Interrupt Handler Address (R/W) See Table 2-2. 987H 2439 IA32_UINTR_STACKADJUST User Interrupt Target-Table Size and Notification Vector (R/W) See Table 2-2. 988H 2440 IA32_UINTR_PD User Interrupt Target-Table Size and Notification Vector (R/W) See Table 2-2. 989H 2441 IA32_UINTR_PD User Interrupt Target Table (R/W) See Table 2-2. 98AH 2442 IA32_UINTR_TT User-Interrupt Target Table (R/W) See Table 2-2.	6A6H	1702	IA32_PL2_SSP		
pointers that are selected in IA-32e mode using the IST index (when not 0) from the interrupt gate descriptor. (R/W) See Table 2-2. 6E1H 1761 IA32_PKRS Specifies the PK permissions associated with each protection domain for supervisor pages (R/W) See Table 2-2. 776H 1910 IA32_HWP_CTL See Table 2-2. 981H 2433 IA32_TME_CAPABILITY Memory Encryption Capability MSR See Table 2-2. 985H 2437 IA32_UINTR_RR User Interrupt Request Register (R/W) See Table 2-2. 986H 2438 IA32_UINTR_HANDLER User Interrupt Handler Address (R/W) See Table 2-2. 987H 2439 IA32_UINTR_STACKADJUST User Interrupt Stack Adjustment (R/W) See Table 2-2. 988H 2440 IA32_UINTR_MISC User-Interrupt Target-Table Size and Notification Vector (R/W) See Table 2-2. 989H 2441 IA32_UINTR_PD User Interrupt PID Address (R/W) See Table 2-2. 988H 2442 IA32_UINTR_TT User-Interrupt Target Table (R/W) See Table 2-2.	6A7H	1703	IA32_PL3_SSP		
protection domain for supervisor pages (R/W) See Table 2-2. 776H 1910 IA32_HWP_CTL See Table 2-2. 981H 2433 IA32_TME_CAPABILITY Memory Encryption Capability MSR See Table 2-2. 985H 2437 IA32_UINTR_RR User Interrupt Request Register (R/W) See Table 2-2. 986H 2438 IA32_UINTR_HANDLER User Interrupt Handler Address (R/W) See Table 2-2. 987H 2439 IA32_UINTR_STACKADJUST User Interrupt Stack Adjustment (R/W) See Table 2-2. 988H 2440 IA32_UINTR_MISC User-Interrupt Target-Table Size and Notification Vector (R/W) See Table 2-2. 989H 2441 IA32_UINTR_PD User Interrupt PID Address (R/W) See Table 2-2. 98AH 2442 IA32_UINTR_TT User-Interrupt Target Table (R/W) See Table 2-2.	6A8H	1704	IA32_INTERRUPT_SSP_TABLE_ADDR		pointers that are selected in IA-32e mode using the IST index (when not 0) from the interrupt gate descriptor. (R/W)
981H 2433 IA32_TME_CAPABILITY Memory Encryption Capability MSR See Table 2-2. 985H 2437 IA32_UINTR_RR User Interrupt Request Register (R/W) See Table 2-2. 986H 2438 IA32_UINTR_HANDLER User Interrupt Handler Address (R/W) See Table 2-2. 987H 2439 IA32_UINTR_STACKADJUST User Interrupt Stack Adjustment (R/W) See Table 2-2. 988H 2440 IA32_UINTR_MISC User-Interrupt Target-Table Size and Notification Vector (R/W) See Table 2-2. 989H 2441 IA32_UINTR_PD User Interrupt PID Address (R/W) See Table 2-2. 98AH 2442 IA32_UINTR_TT User-Interrupt Target Table (R/W) See Table 2-2.	6E1H	1761	IA32_PKRS		protection domain for supervisor pages (R/W)
See Table 2-2. 985H 2437 IA32_UINTR_RR User Interrupt Request Register (R/W) See Table 2-2. 986H 2438 IA32_UINTR_HANDLER User Interrupt Handler Address (R/W) See Table 2-2. 987H 2439 IA32_UINTR_STACKADJUST User Interrupt Stack Adjustment (R/W) See Table 2-2. 988H 2440 IA32_UINTR_MISC User-Interrupt Target-Table Size and Notification Vector (R/W) See Table 2-2. 989H 2441 IA32_UINTR_PD User Interrupt PID Address (R/W) See Table 2-2. 98AH 2442 IA32_UINTR_TT User-Interrupt Target Table (R/W) See Table 2-2.	776H	1910	IA32_HWP_CTL		See Table 2-2.
See Table 2-2. 986H 2438 IA32_UINTR_HANDLER User Interrupt Handler Address (R/W) See Table 2-2. 987H 2439 IA32_UINTR_STACKADJUST User Interrupt Stack Adjustment (R/W) See Table 2-2. 988H 2440 IA32_UINTR_MISC User-Interrupt Target-Table Size and Notification Vector (R/W) See Table 2-2. 989H 2441 IA32_UINTR_PD User Interrupt PID Address (R/W) See Table 2-2. 98AH 2442 IA32_UINTR_TT User-Interrupt Target Table (R/W) See Table 2-2.	981H	2433	IA32_TME_CAPABILITY		1
See Table 2-2. 987H 2439 IA32_UINTR_STACKADJUST User Interrupt Stack Adjustment (R/W) See Table 2-2. 988H 2440 IA32_UINTR_MISC User-Interrupt Target-Table Size and Notification Vector (R/W) See Table 2-2. 989H 2441 IA32_UINTR_PD User Interrupt PID Address (R/W) See Table 2-2. 98AH 2442 IA32_UINTR_TT User-Interrupt Target Table (R/W) See Table 2-2.	985H	2437	IA32_UINTR_RR		
See Table 2-2. 988H 2440 IA32_UINTR_MISC User-Interrupt Target-Table Size and Notification Vector (R/W) See Table 2-2. 989H 2441 IA32_UINTR_PD User Interrupt PID Address (R/W) See Table 2-2. 98AH 2442 IA32_UINTR_TT User-Interrupt Target Table (R/W) See Table 2-2.	986H	2438	IA32_UINTR_HANDLER		
Vector (R/W) See Table 2-2. 989H 2441 IA32_UINTR_PD User Interrupt PID Address (R/W) See Table 2-2. 98AH 2442 IA32_UINTR_TT User-Interrupt Target Table (R/W) See Table 2-2.	987H	2439	IA32_UINTR_STACKADJUST		
See Table 2-2. 98AH 2442 IA32_UINTR_TT User-Interrupt Target Table (R/W) See Table 2-2.	988H	2440	IA32_UINTR_MISC		Vector (R/W)
See Table 2-2.	989H	2441	IA32_UINTR_PD		
C70H 3184 MSR_B1_PMON_EVNT_SEL0 Package Uncore B-box 1 perfmon event select MSR.	98AH	2442	IA32_UINTR_TT		
	C70H	3184	MSR_B1_PMON_EVNT_SEL0	Package	Uncore B-box 1 perfmon event select MSR.
C71H 3185 MSR_B1_PMON_CTRO Package Uncore B-box 1 perfmon counter MSR.	C71H	3185	MSR_B1_PMON_CTR0	Package	Uncore B-box 1 perfmon counter MSR.
C72H 3186 MSR_B1_PMON_EVNT_SEL1 Package Uncore B-box 1 perfmon event select MSR.	C72H	3186	MSR_B1_PMON_EVNT_SEL1	Package	Uncore B-box 1 perfmon event select MSR.
C73H 3187 MSR_B1_PMON_CTR1 Package Uncore B-box 1 perfmon counter MSR.	C73H	3187	MSR_B1_PMON_CTR1	Package	Uncore B-box 1 perfmon counter MSR.
C74H 3188 MSR_B1_PMON_EVNT_SEL2 Package Uncore B-box 1 perfmon event select MSR.	C74H	3188	MSR_B1_PMON_EVNT_SEL2	Package	Uncore B-box 1 perfmon event select MSR.
C75H 3189 MSR_B1_PMON_CTR2 Package Uncore B-box 1 perfmon counter MSR.	C75H	3189	MSR_B1_PMON_CTR2	Package	Uncore B-box 1 perfmon counter MSR.

Table 2-52. Additional MSRs Supported by the 4th Generation Intel® Xeon® Scalable Processor Family with a CPUID Signature DisplayFamily DisplayModel Value of 06 8FH

Register Address		Register Name / Bit Fields	Scope	Bit Description
Hex	Dec			
C76H	3190	MSR_B1_PMON_EVNT_SEL3	Package	Uncore B-box 1vperfmon event select MSR.
C77H	3191	MSR_B1_PMON_CTR3	Package	Uncore B-box 1 perfmon counter MSR.
C82H	3122	MSR_W_PMON_BOX_OVF_CTRL	Package	Uncore W-box perfmon local box overflow control MSR.
C8FH	3215	IA32_PQR_ASSOC		See Table 2-2.
C90H -	3216	IA32_L3_QOS_MASK_0 through IA32_L3_QOS_MASK_14	Package	See Table 2-50.
D10H - D17H	3230 3344 - 3351	IA32_L2_QOS_MASK_[0-7]	Core	$\begin{split} & \text{IA32_CR_L2_QOS_MASK_[0-7]} \\ & \text{If CPUID.(EAX=10H, ECX=1):EDX.COS_MAX[15:0]} \geq 0. \\ & \text{See Table 2-2.} \end{split}$
D93H	3475	IA32_PASID		See Table 2-2.
1200H - 121FH	4608 - 4639	IA32_LBR_x_INFO		Last Branch Record Entry X Info Register (R/W) See Table 2-2.
1406H	5126	IA32_MCU_CONTROL		See Table 2-2.
14CEH	5326	IA32_LBR_CTL		Last Branch Record Enabling and Configuration Register (R/W) See Table 2-2.
14CFH	5327	IA32_LBR_DEPTH		Last Branch Record Maximum Stack Depth Register (R/W) See Table 2-2.
1500H - 151FH	5376 - 5407	IA32_LBR_x_FROM_IP		Last Branch Record Entry X Source IP Register (R/W) See Table 2-2.
1600H - 161FH	5632 - 5663	IA32_LBR_x_TO_IP		Last Branch Record Entry X Destination IP Register (R/W) See Table 2-2.

2.18 MSRS IN THE INTEL® XEON PHI™ PROCESSOR 3200/5200/7200 SERIES AND THE INTEL® XEON PHI™ PROCESSOR 7215/7285/7295 SERIES

The Intel[®] Xeon Phi[™] processor 3200, 5200, 7200 series, with a CPUID Signature DisplayFamily_DisplayModel value of 06_57H, supports the MSR interfaces listed in Table 2-53. These processors are based on the Knights Landing microarchitecture. The Intel[®] Xeon Phi[™] processor 7215, 7285, 7295 series, with a CPUID Signature DisplayFamily_DisplayModel value of 06_85H, supports the MSR interfaces listed in Table 2-53 and Table 2-54. These processors are based on the Knights Mill microarchitecture. Some MSRs are shared between a pair of processor cores, and the scope is marked as module.