TDX_FEATURES Enum. Bits	Class	Field	Description	Type	Field Size (Bytes)	Max Num Fields	Num Elem.	Elem. Size (Bytes)	Base FIELD_ID (Hex)	VMM Access	Guest Access
Always	Platform Info	NUM_PKGS	Number of CPU packages in the system (1 - 8)	Integer	4	1	1	4	0x0000000200000000	RO	None
Always	Platform Info	PKG_FMS	Array of version information (type, family, model, stepping) as returned by CPUID(1).EAX for each package. Unused entries (NUM_PKGS and above) are set to 0.	N/A	4	8	1	4	0x0000000200000001	RO	None
Always	TDX Module Version	VENDOR_ID	0x8086 for Intel	Integer	4	1	1	4	0x0800000200000000	RO	RO
Always	TDX Module Version	BUILD_DATE	Intel TDX module build data – in yyyymmdd BCD format (each digit occupies 4 bits)	BCD	4	1	1	4	0x8800000200000001	RO	None
Always	TDX Module Version	BUILD_NUM	Build number of the Intel TDX module. See the [ABI Spec] for details.	16-bit integer	2	1	1	2	0x8800000100000002	RO	None
Always	TDX Module Version	MINOR_VERSION	Minor version number of the Intel TDX module. E.g., for TDX Module version 1.5.08.04, MINOR_VERSION is 5. See the [ABI Spec] for details.	16-bit integer	2	1	1	2	0x0800000100000003	RO	RO
Always	TDX Module Version	MAJOR_VERSION	Major version number of the Intel TDX module. E.g., for TDX Module version 1.5.08.04, MAJOR_VERSION is 1. See the [ABI Spec] for details.	16-bit integer	2	1	1	2	0x0800000100000004	RO	RO
Always	TDX Module Version	UPDATE_VERSION	Update version number of the Intel TDX module. E.g., for TDX Module version 1.5.08.04, UPDATE_VERSION is 8. See the [ABI Spec] for details.	16-bit integer	2	1	1	2	0x0800000100000005	RO	None
Always	TDX Module Version	INTERNAL_VERSION	Internal version number of the Intel TDX module. E.g., for TDX Module version 1.5.08.04, INTERNAL_VERSION is 4. See the [ABI Spec] for details.	16-bit integer	2	1	1	2	0x0800000100000006	RO	None
1	TDX Module Handoff	MODULE_HV	The native handoff version that this TDX module should support.	16-bit integer	2	1	1	2	0x8900000100000000	RO	None
1	TDX Module Handoff	MIN_UPDATE_HV	The minimum handoff version that this TDX module should support.	16-bit integer	2	1	1	2	0x8900000100000001	RO	None
1	TDX Module Handoff	NO_DOWNGRADE	A boolean flag that indicates whether this TDX module should disallow downgrades.	Boolean	1	1	1	1	0x8900000000000002	RO	None
1	TDX Module Handoff	NUM_HANDOFF_PAGES	The number of 4KB pages (minus 1) allocated at the beginning of the data region for handoff data.	16-bit integer	2	1	1	2	0x8900000100000003	RO	None
1	TDX Module Handoff	HANDOFF_DATA_VALID	A boolean flag that indicates whether the handoff data is valid. Handoff data is created by TDH.SYS.SHUTDOWN and consumed by TDH.SYS.UPDATE.	Boolean	1	1	1	1	0x8900000000000004	RO	None
1	TDX Module Handoff	HANDOFF_DATA_HV	The version of the handoff data. Handoff data is created by TDH.SYS.SHUTDOWN and consumed by TDH.SYS.UPDATE.	16-bit integer	2	1	1	2	0x8900000100000005	RO	None
1	TDX Module Handoff	HANDOFF_DATA_SIZE	Size of the HV-specific data, in bytes. Handoff data is created by TDH.SYS.SHUTDOWN and consumed by TDH.SYS.UPDATE.	32-bit unsigned integer	4	1	1	4	0x8900000200000006	RO	None
Always	TDX Module Info	SYS_ATTRIBUTES	Module attributes Bits 30:0 Reserved – set to 0 Bit 31 0 indicates a production module. 1 indicates a debug module.	Bitmap	4	1	1	4	0x0A00000200000000	RO	RO
Always	TDX Module Info	NUM_TDX_FEATURES	Number of TDX_FEATURES and TDX_FEATURES_ENABLED (if supported) fields	8-bit integer	1	1	1	1	0x0A00000000000001	RO	RO
Always	TDX Module Info	TDX_FEATURES0	Enumerates TDX features. See the [ABI Spec] for details.	64-bit bitmap	8	1	1	8	0x0A00000300000008	RO	RO
Always	CMR Info	NUM_CMRS	Number of the following CMR entries	Integer	2	1	1	2	0x9000000100000000	RO	None
Always	CMR Info	CMR_BASE	Array of CMR base addresses Since a CMR is aligned on 4KB, bits 11:0 are 0.	Physical Address	8	32	1	8	0x9000000300000080	RO	None
Always	CMR Info	CMR_SIZE	Array of CMR sizes, in bytes Since a CMR is aligned on 4KB, bits 11:0 are 0. A value of 0 indicates a null entry.	Integer	8	32	1	8	0x9000000300000100	RO	None
Always	TDMR Info	MAX_TDMRS	The maximum number of TDMRs supported	Integer	2	1	1	2	0x9100000100000008	RO	None
Always	TDMR Info	MAX_RESERVED_PER_TDMR	The maximum number of reserved areas per TDMR	Integer	2	1	1	2	0x9100000100000009	RO	None
Always	TDMR Info	PAMT_4K_ENTRY_SIZE	The size of a PAMT_4K (1 entry per 4KB of TDMR) entry, in bytes – determines the number of bytes that need to be reserved for the PAMT_4K area.	Integer	2	1	1	2	0x9100000100000010	RO	None
Always	TDMR Info	PAMT_2M_ENTRY_SIZE	The size of a PAMT_2M (1 entry per 2MB of TDMR) entry, in bytes – determines the number of bytes that need to be reserved for the PAMT_2M area.	Integer	2	1	1	2	0x9100000100000011	RO	None

Always	TDMR Info	PAMT_1G_ENTRY_SIZE	The size of a PAMT_1G (1 entry per 1GB of TDMR) entry, in bytes – determines the number of bytes that need to be reserved for the PAMT_1G area.	Integer	2	1	1	2	0x9100000100000012	RO	None
36	TDMR Info	PAMT_PAGE_BITMAP_ENTRY_BITS	Size of each PAMT_PAGE_BITMAP entry, in bits	Unsigned integer	1	1	1	1	0x9100000000000013	RO	None
36	TDMR Info	MIN_DYNAMIC_PAMT_NUM_HKID_BITS	Minimum configured number of memory encryption key bits required in order to configure the TDX module for dynamic PAMT	Unsigned integer	1	1	1	1	0x9100000000000014	RO	None
Always	TD Control Structures	TDR_BASE_SIZE	Base value for the number of bytes required to hold TDR	Integer	2	1	1	2	0x9800000100000000	RO	None
Always	TD Control Structures	TDCS_BASE_SIZE	Base value for the number of bytes required to hold TDCS	Integer	2	1	1	2	0x9800000100000100	RO	None
7	TD Control Structures	TDCS_SIZE_PER_L2_VM	Number of additional TDCS bytes per L2 VM	Integer	2	1	1	2	0x9800000100000101	RO	None
Always	TD Control Structures	TDVPS_BASE_SIZE	Base value for the number of bytes required to hold TDVPS	Integer	2	1	1	2	0x9800000100000200	RO	None
7	TD Control Structures	TDVPS_SIZE_PER_L2_VM	Number of additional TDVPS bytes per L2 VM	Integer	2	1	1	2	0x9800000100000201	RO	None
Always	TD Configurability	ATTRIBUTES_FIXED0	If any certain bit is 0 in ATTRIBUTES_FIXED0, it must be 0 in any TD's ATTRIBUTES. The value of this field reflects the Intel TDX module capabilities and configuration and CPU capabilities.	Bitmap	8	1	1	8	0x1900000300000000	RO	None
Always	TD Configurability	ATTRIBUTES_FIXED1	If any certain bit is 1 in ATTRIBUTES_FIXED1, it must be 1 in any TD's ATTRIBUTES. The value of this field reflects the Intel TDX module capabilities and configuration and CPU capabilities.	Bitmap	8	1	1	8	0x1900000300000001	RO	None
Always	TD Configurability	XFAM_FIXED0	If any certain bit is 0 in XFAM_FIXED0, it must be 0 in any TD's XFAM.	Bitmap	8	1	1	8	0x1900000300000002	RO	None
Always	TD Configurability	XFAM_FIXED1	If any certain bit is 1 in XFAM_FIXED1, it must be 1 in any TD's XFAM.	Bitmap	8	1	1	8	0x1900000300000003	RO	None
Always	TD Configurability	NUM_CPUID_CONFIG	Number of the following CPUID_CONFIG entries	Unsigned 16-bit integer	2	1	1	2	0x9900000100000004	RO	None
Always	TD Configurability	CONFIG_FLAGS_FIXED0	If any certain bit is 0 in CONFIG_FLAGS_FIXED0, it must be 0 in any TD's CONFIG_FLAGS.	Bitmap	8	1	1	8	0x9900000300000006	RO	None
Always	TD Configurability	CONFIG_FLAGS_FIXED1	If any certain bit is 1 in CONFIG_FLAGS_FIXED1, it must be 1 in any TD's CONFIG_FLAGS.	Bitmap	8	1	1	8	0x9900000300000007	RO	None
20	TD Configurability	MAX_VCPUS_PER_TD	Maximum number of VCPUS per TD	Unsigned 16-bit integer	2	1	1	2	0x9900000100000008	RO	None
27	TD Configurability	MIN_VIRT_MAXPA	Minimum value of virtual MAXPA (CPUID(0x80000008).EAX[7:0]	Unsigned 8-bit integer	1	1	1	1	0x9900000000000009	RO	None
24	TD Configurability	MAX_EVENT_FILTERS	Maximum number of Perfmon event filters	Unsigned 16-bit integer	2	1	1	2	0x990000010000000A	RO	None
Always	TD Configurability	CPUID_CONFIG_LEAVES	Array of CPUID leaf / sub-leaf numbers: Bits 31:0 Leaf number Bits 63:32 Sub-leaf number. A value of -1 indicates a CPUID leaf with no sub-leaves. Note: The actual number of entries in the array is enumerated by NUM_CPUID_CONFIG above.		8	128	1	8	0x9900000300000400	RO	None
Always	TD Configurability	CPUID_CONFIG_VALUES	Array of configurable virtualization of the value returned by CPUID A CPUID bit is considered configurable if it is either: - Directly configurable (CONFIG_DIRECT) by the host VMM, or - The host VMM may allow it to be 1 (ALLOW_*_DIRECT) and its native value, as returned by the CPU, is 1. For each field in the array: Element 0[31: 0]: CPUID EAX value Element 0[63:32]: CPUID EBX value Element 1[31: 0]: CPUID ECX value Element 1[63:32]: CPUID EDX value A bit value of 1 indicates that the host VMM can configure that bit. Note: The actual number of entries in the array is enumerated by NUM_CPUID_CONFIG above.		16	128	2	8	0x9900000300000500	RO	None

Always	TD Configurability	IA32_ARCH_CAPABILITIES_CONFIG_MASK	Bit mask of configurable virtualization of IA32_ARCH_CAPABILITIES MSR. A value of 1 indicates a configurable bit.	64-bit bitmap	1	1	1	8	0x9900000300000600	RO	None
17	TD Configurability	NUM_ALLOWED_FMS	Number of valid entries in ALLOWED_FMS below	Unsigned 16-bit integer	1	1	1	2	0x9900000100000800	RO	None
17	TD Configurability	NUM_DISALLOWED_FMS	Number of valid entries in DISALLOWED_FMS below	Unsigned 16-bit integer	1	1	1	2	0x9900000100000801	RO	None
17	TD Configurability	ALLOWED_FMS	Array of 32-bit fields in CPUID(1).EAX Family/Model/Stepping format, enumerating the allowed configuration values (only for migratable TDs). For Stepping (bits 3:0), the maximum allowed configuration value is provided. Note: The actual number of valid array entries is enumerateded by NUM_ALLOWED_FMS.	CPUID(1).EAX	1	64	1	8	0x9900000300000810	RO	None
17	TD Configurability	DISALLOWED_FMS	Array of 32-bit fields in CPUID(1).EAX Family/Model/Stepping format, enumerating specific configuration values which are not allowed. Those values take precedence over the values in ALLOWED_FMS. Note: The number of valid array entries is enumerateded by NUM_DISALLOWED_FMS.	CPUID(1).EAX	1	64	1	8	0x9900000300000850	RO	None
6	Memory Management	GUEST_GPA_ATTR_MASK	Bit mask of page attributes that the guest TD can configure for GPA mapping. A bit value of 1 indicates the corresponding GPA_ATTR bit may be configured.	GPA_ATTR	8	1	1	8	0x9A00000300000000	RO	RO
22	Measurement	MAX_TDREPORT_SIZE	Maximum size of TDREPORT_STRUCT output of TDG.MR.REPORT	16-bit integer	2	1	1	2	0x9B00000100000000	RO	RO
0, 13	Migration	MIG_ATTRIBUTES	Migration attributes (details are TBD)	64-bit bitmap	8	1	1	8	0xA000000300000000	RO	RO
0, 13	Migration	MIN_EXPORT_VERSION	Minimum value of migration version supported for export	16-bit integer	2	1	1	2	0x2000000100000001	RO	RO
0, 13	Migration	MAX_EXPORT_VERSION	Maximum value of migration version supported for export	16-bit integer	2	1	1	2	0x2000000100000002	RO	RO
0, 13	Migration	MIN_IMPORT_VERSION	Minimum value of migration version supported for import	16-bit integer	2	1	1	2	0x2000000100000003	RO	RO
0, 13	Migration	MAX_IMPORT_VERSION	Maximum value of migration version supported for import	16-bit integer	2	1	1	2	0x2000000100000004	RO	RO
0, 13	Migration	MAX_MIGS	Maximum number of migration streams per TD Note: This number includes 1 backward migration stream.	Unsigned integer	2	1	1	2	0xA000000100000010	RO	None
0, 13	Migration	NUM_IMMUTABLE_STATE_PAGES	Number of pages required for exporting immutable state by TDH.EXPORT.STATE.IMMUTABLE	Integer	1	1	1	1	0xA000000000000020	RO	None
0, 13	Migration	NUM_TD_STATE_PAGES	Number of pages required for exporting TD state by TDH.EXPORT.STATE.TD	Integer	1	1	1	1	0xA000000000000021	RO	None
0, 13	Migration	NUM_VP_STATE_PAGES	Number of pages required for exporting VCPU state by TDH.EXPORT.STATE.VP	Integer	1	1	1	1	0xA000000000000022	RO	None
41	Migration	NUM_MEM_SCAN_CONTROL_PAGES	Number of pages required to be allocated by TDH.MEM.SCAN.CONFIG	Unsigned integer	1	1	1	1	0xA000000000000030	RO	None
41	Migration	MAX_MEM_SCAN_RANGES	Maximum number of memory scan GPA ranges that can be configured by TDH.MEM.SCAN.CONFIG	Unsigned integer	2	1	1	2	0xA000000100000031	RO	None
41	Migration	NUM_MEM_SCAN_CONTEXTS	Number of memory scan contexts that can be used by TDH.MEM.SCAN.COMP	Unsigned integer	2	1	1	2	0xA000000100000032	RO	None
0	Service TD	MAX_SERV_TDS	Maximum number of service TDs per TD	Unsigned integer	2	1	1	2	0xA100000100000000	RO	None
0	Service TD	SERVTD_ATTR_FIXED0	Fixed-0 bits of Service TD attributes. A bit value of 0 indicates corresponding SERVTD_ATTR bit must be 0	64-bit bitmap	8	1	1	8	0xA100000300000001	RO	None
0	Service TD	SERVTD_ATTR_FIXED1	Fixed-1 bits of Service TD attributes. A bit value of 1 indicates corresponding SERVTD_ATTR bit must be 1	64-bit bitmap	8	1	1	8	0xA100000300000002	RO	None
7	TD Partitioning	GUEST_L2_GPA_ATTR_MASK	Bit mask of page attributes that the L1 VMM can configure for L2 VM GPA mapping. A bit value of 1 indicates the corresponding GPA_ATTR_SINGLE_VM bit may be configured.	GPA_ATTR_SINGLE_VM	2	1	1	2	0xA200000100000000	RO	RO
7	TD Partitioning	VM_CTLS_FIXED0	Fixed-0 bits of TDCS.VM_CTLS. A bit value of 0 indicates corresponding VM_CTLS bit must be 0	64-bit bitmap	8	1	1	8	0xA200000300000001	RO	None
7	TD Partitioning	VM_CTLS_FIXED1	Fixed-1 bits of TDCS.VM_CTLS. A bit value of 1 indicates corresponding VM_CTLS bit must be 1	64-bit bitmap	8	1	1	8	0xA200000300000002	RO	None

7	TD Partitioning	VPCU_L2_CTLS_FIXED0	Fixed-0 bits of TDVPS.L2_CTLS. A bit value of 0 indicates corresponding L2_CTLS bit must be 0	64-bit bitmap	8	1	1	8	0xA200000300000003	RO	None
7	TD Partitioning	VCPU_L2_CTLS_FIXED1	Fixed-1 bits of TDVPS.L2_CTLS. A bit value of 1 indicates corresponding L2_CTLS bit must be 1	64-bit bitmap	8	1	1	8	0xA200000300000004	RO	None
7	TD Partitioning	VPCU_L2_DEBUG_CTLS_FIXED0	Fixed-0 bits of TDVPS.L2_DEBUG_CTLS. A bit value of 0 indicates corresponding L2_CTLS bit must be 0	64-bit bitmap	8	1	1	8	0xA200000300000005	RO	None
7	TD Partitioning	VCPU_L2_DEBUG_CTLS_FIXED1	Fixed-1 bits of TDVPS.L2_DEBUG_CTLS. A bit value of 1 indicates corresponding L2_CTLS bit must be 1	64-bit bitmap	8	1	1	8	0xA200000300000006	RO	None
6	TDX Connect	TDX_CONNECT_FEATURES	When TDX-IO capability is enabled, this bit mask provides the features supported by the TDX module and the platfrom: Bit 0 (T_REQ_WO_PASID) TDI trusted DMA requests without PASID Bit 1 (T_REQ_W_PASID) TDI trusted DMA requests with PASID Bit 2 (T_ATS) TDI trusted ATS translation requests Bit 3 (T_TRAN) TDI trusted translated requests Bit 4 (T_PRS) TDI trusted PRS translation requests Bit 5 (T_MSI) TDI trusted MSI requests Bit 6 (T_LINK_IDE) TDI assignment using Link IDE stream Bit 7 (T_SEL_IDE) TDI assignment using Selective IDE stream Bit 8 (T_MMIOL) Trusted MMIO low access supported Bit 9 (T_MMIOH) Trusted MMIO high access supported Bit 10 (T_CFG) Trusted CFG access supported Bit 11 (T_DIRECT_P2P) Trusted TDI direct P2P supported Bit 12 (T_RC_P2P) Trusted TDI Root Complex mediated P2P supported	64-bit bitmap	8	1	1	8	0x3000000300000000	RO	RO
6	TDX Connect	IDE_MT_PAGES_COUNT	Amount of pages for the TDX Module IDE stream context	Unsigned 16-bit integer	2	1	1	2	0x3000000100000001	RO	None
6	TDX Connect	SPDM_MT_PAGES_COUNT	Amount of pages for the TDX Module SPDM session context	Unsigned 16-bit integer	2	1	1	2	0x3000000100000002	RO	None
6	TDX Connect	IOMMU_MT_PAGES_COUNT	Amount of pages for the TDX Module IOMMU context	Unsigned 16-bit integer	2	1	1	2	0x3000000100000003	RO	None
6	TDX Connect	TDICS_MT_PAGES_COUNT	Amount of pages for the TDX Module IDE stream context	Unsigned 16-bit integer	2	1	1	2	0x3000000100000004	RO	None
6	TDX Connect	TDISP_MAX_TDI_REPORT_PAGES	Max supported TDI Report size in 4KB pages	Unsigned 16-bit integer	2	1	1	2	0x3000000100000005	RO	None
6	TDX Connect	TDISP_LOCK_INTERFACE_FLAGS_SUPPORTED	TDISP Lock Interface Flags supported bitmask	16-bit bitmap	2	1	1	2	0x3000000100000006	RO	None
6	TDX Connect	SPDM_MAX_DEV_INFO_PAGES	Max number of 4K pages required for the SPDM DEVICE_INFO output	Unsigned 16-bit integer	2	1	1	2	0x3000000100000007	RO	None
6	TDX Connect	SPDM_DOE_PAGES_COUNT	Number of pages for SPDM output (SPDM Request) and input (SPDM Response) buffers	Unsigned 16-bit integer	2	1	1	2	0x3000000100000008	RO	None
6	TDX Connect	TDX_MAX_TDIS_PER_TD	Max number of TDIs supported per TD	Unsigned 16-bit integer	2	1	1	2	0x3000000100000009	RO	None
6	TDX Connect	MAX_SIMULTANEOUS_SPDM_SESSIONS	Maximum number of simultaneous SPDM sessions supported by the TDX Module for TDH.SPDM.CONNECT, TDH.SPDM.DISCONNECT and TDH.SPDM.MNG	Unsigned 16-bit integer	2	1	1	2	0x300000010000000A	RO	None
6	TDX Connect	TDX_MAX_TDI_BIND_REPORT	Number of pages required for the TDI Bind Report	Unsigned 16-bit integer	2	1	1	2	0x300000010000000B	RO	None
39	NRX	MEMORY_POOL_REQUIRED_PAGES	Number of 4K memory pages required to fill the memory pool	Unsigned 16-bit integer	2	1	1	2	0x3100000100000000	RO	None
39	NRX	EXT_REQUIRED	Return true if the TDH.EXT.INIT is required to be called	Boolean	1	1	1	1	0x3100000000000001	RO	None

39	NRX	RTC	Return the current RTC. 0 If the VMM did not provide RTC value	Unsigned 64-bit integer	8	1	1	8	0x3100000300000002	RO	RO
39	NRX	EXT_MISSING_PAGES_PREV_FEATURES	Return the the missing number of memory pool pages for initializing the previously enabled features	Unsigned 64-bit integer	8	1	1	8	0x3100000300000003	RO	None
50	Quoting	QUOTE_ENABLED_QUOTE_IDS	Bitmap of attestation keys that have been enabled and available for obtaining a TDX Attestation Quote via TDH.QUOTE.GET.	64-bit bitmap	8	1	1	8	0x2300000300000000	RO	None
50	Quoting	QUOTE_ID	Bitmap, with only a single bit set, of the key ID to be used for TDX Attestation when calling TDH.QUOTE.GET without explicitly specifying an attestation key via ATTESTATION_KEY_ID input parameter.	64-bit bitmap	8	1	1	8	0x2300000300000001	RW	None
50	Quoting	QUOTE_MAX_SIZE	Maximum size of the buffer that must be allocated to contain the TDX Quote received from TDX Module	Unsigned 32-bit integer	4	1	1	4	0x2300000200000002	RO	None
50	Quoting	QUOTE_MAX_SESSIONS	Maximum number of sessions that Quoting feature supports	Unsigned 16-bit integer	2	1	1	2	0x2300000100000003	RO	None
50	Quoting	QUOTE_MAX_THREADS	Maximum number of concurrent virtual threads that Quoting feature supports	Unsigned 16-bit integer	2	1	1	2	0x2300000100000004	RO	None
50	Quoting	QUOTE_NUM_SESSIONS	The currently configured number of sessions that Quoting feature is using. The value must be less or equal to QUOTE_MAX_SESSIONS. This field can only be written by the host VMM before calling TDH.SYS.CONFIG/UPDATE.	Unsigned 16-bit integer	2	1	1	2	0x2300000100000005	RW	None
50	Quoting	QUOTE_NUM_THREADS	The currently configured number of concurrent threads that Quoting feature is using. The value must be less or equal to QUOTE_MAX_THREADS. This field can only be written by the host VMM before calling TDH.SYS.CONFIG/UPDATE.	Unsigned 16-bit integer	2	1	1	2	0x2300000100000006	RW	None