Trusted Platform

Trusted Platform

The following table lists the trusted platform BIOS settings that you can configure through a BIOS policy or the default BIOS settings:

Name	Description	Supported Attributes			
		Versions	Platforms	Values	Dependencies
Multikey Total Memory Encryption (MK-TME)	MK-TME allows you to have multiple encryption domains with one with own key. Different memory pages can be encrypted with different keys.	4.2(1), 5.0(1), 5.0(2)	C240 M6, C220 M6, C225 M6, C245 M6, B200 M6, X210c M6, C220 M7, C240 M7, X210c M7, X410c M7	**Enabled**, Disabled	
Software Guard Extensions (SGX)	Allows you to enableSoftware Guard Extensions(SGX) feature.	4.2(1), 5.0(1), 5.0(2)	C240 M6, C220 M6, C225 M6, C245 M6, B200 M6, X210c M6, C220 M7, C240 M7, X210c M7, X410c M7	**Enabled**, Disabled	
Total Memory Encryption (TME)	Allows you to provide the capability to encrypt the entirety of the physical memory of a system.	4.2(1), 5.0(1), 5.0(2)	C240 M6, C220 M6, C225 M6, C245 M6, B200 M6, X210c M6, C220 M7, C240 M7, X210c M7, X410c M7	**Enabled**, Disabled	

Name	Description	Supported Attributes			
		Versions	Platforms	Values	Dependencies
Select Owner EPOCH Input Type	Allows you to change the seed for the security key used for the locked memory region that is created.	4.2(1), 5.0(1), 5.0(2)	C240 M6, C220 M6, C225 M6, C245 M6, B200 M6, X210c M6, C220 M7, C240 M7, X210c M7, X410c M7	SGX Owner EPOCH activated, Change to New Random Owner EPOCHs, **Manual User Defined Owner EPOCHs**	
SGX Auto MP Registration Agent	Allows you to enable the registration authority service to store the platform keys.	4.2(1), 5.0(1), 5.0(2)	C240 M6, C220 M6, C225 M6, C245 M6, B200 M6, X210c M6, C220 M7, C240 M7, X210c M7, X410c M7	**Enabled**, Disabled	
SGX Epoch 0	Allows you to define the SGX EPOCH owner value for the EPOCH number designated by 0.	4.2(1), 5.0(1), 5.0(2)	C240 M6, C220 M6, C225 M6, C245 M6, B200 M6, X210c M6, C220 M7, C240 M7, X210c M7, X410c M7	**Enabled**, Disabled	
SGX Epoch 1	Allows you to define the SGX EPOCH owner value for the EPOCH number designated by 1.	4.2(1), 5.0(1), 5.0(2)	C240 M6, C220 M6, C225 M6, C245 M6, B200 M6, X210c M6, C220 M7, C240 M7, X210c M7, X410c M7	**Enabled**, Disabled	
SGX Factory Reset	Allows the system to perform SGX factory reset on subsequent boot.	4.2(1), 5.0(1), 5.0(2)	C240 M6, C220 M6, C225 M6, C245 M6, B200 M6, X210c M6, C220 M7, C240 M7, X210c M7, X410c M7	**Enabled**, Disabled	

Name	Description	Supported Attributes			
		Versions	Platforms	Values	Dependencies
SGX PubKey Hash*n* where *n* ranges from 0 to 3.	Allows you to set the Software Guard Extensions (SGX) value.	4.2(1), 5.0(1), 5.0(2)	C240 M6, C220 M6, C225 M6, C245 M6, B200 M6, X210c M6, C220 M7, C240 M7, X210c M7, X410c M7	**SGX PUBKEY HASH0**, SGX PUBKEY HASH1, SGX PUBKEY HASH2, SGX PUBKEY HASH3 • SGX PUBKEY HASH0—Between 7-0. • SGX PUBKEY HASH1—Between 15-8. • SGX PUBKEY HASH2—Between 23-16. • SGX PUBKEY HASH3—Between 31-24.	
SGX Write Enable	Allows you to enable SGX Write feature.	4.2(1), 5.0(1), 5.0(2)	C240 M6, C220 M6, C225 M6, C245 M6, B200 M6, X210c M6, C220 M7, C240 M7, X210c M7, X410c M7	**Enabled**, Disabled	
SGX Package Information In-Band Access	Allows you to enable SGX Package Info In-Band Access.	4.2(1), 5.0(1), 5.0(2)	C240 M6, C220 M6, C225 M6, C245 M6, B200 M6, X210c M6, C220 M7, C240 M7, X210c M7, X410c M7	Enabled, **Disabled**	

Name	Description	Supported Attributes			
		Versions	Platforms	Values	Dependencies
SGX QoS	Allows you to enable SGX QoS.	4.2(1), 5.0(1), 5.0(2)	C240 M6, C220 M6, C225 M6, C245 M6, B200 M6, X210c M6, C220 M7, C240 M7, X210c M7, X410c M7	**Enabled**, Disabled	
SHA-1 PCR Bank	The Platform Configuration Register (PCR) is a memory location in the TPM. Multiple PCRs are collectively referred to as a PCR bank. A Secure Hash Algorithm 1 or SHA-1 PCR Bank allows to enable or disable TPM security.	4.2(1), 5.0(1), 5.0(2)	C240 M6, C220 M6, C225 M6, C245 M6, B200 M6, X210c M6, C220 M7, C240 M7, X210c M7, X410c M7	**Enabled**, Disabled	If the Security Device Support is disabled then the entire TPM operation will fail.
SHA256 PCR Bank	The Platform Configuration Register (PCR) is a memory location in the TPM. Multiple PCRs are collectively referred to as a PCR bank. A Secure Hash Algorithm 256-bit or SHA-256PCR Bank allows to enable or disable TPM security.	4.2(1), 5.0(1), 5.0(2)	C240 M6, C220 M6, C225 M6, C245 M6, B200 M6, X210c M6, , C220 M7, C240 M7, X210c M7, X410c M7	**Enabled**, Disabled	If the Security Device Support is disabled then the entire TPM operation will fail.

Name	Description	Supported Attributes			
		Versions	Platforms	Values	Dependencies
SHA384 PCR Bank	The Platform Configuration Register (PCR) is a memory location in the TPM. Multiple PCRs are collectively referred to as a PCR bank. A Secure Hash Algorithm 256-bit or SHA-384PCR Bank allows to enable or disable TPM security.	4.3(3a)	X410c M7, X210c M7, C220 M7, C240 M7	Enabled, **Disabled**	If the Security Device Support is disabled then the entire TPM operation will fail.
Trusted Platform Module State	Whether to enable or disable the TrustedPlatform Module (TPM), which is a component that securely stores artifactsthat are used to authenticate the server.	4.2(1), 5.0(1), 5.0(2)	C240 M6, C220 M6, C225 M6, C245 M6, B200 M6, X210c M6, C220 M7, C240 M7, X210c M7, X410c M7	**Enabled**, Disabled	If the Security Device Support is disabled then the entire TPM operation will fail.
Trust Domain Extension	Whether to enable or disable the Trust Domain Extension (TDX), which protects the sensitive data and applications from unauthorized access.	4.3(3a)	X410c M7, X210c M7, C220 M7, C240 M7	Enabled, **Disabled**	To enable Trust Domain Extension, ensure that: • Total Memory Encryption (TME) is Enabled. • Software Guard Extensions (SGX) is Enabled. • Multikey Total Memory Encryption (MK-TME) is Enabled. • LIMIT CPU PA to 46 Bits token is Disabled.

Name	Description	Supported Attributes			
		Versions	Platforms	Values	Dependencies
TDX Secure Arbitration Mode Loader	Whether to enable or disable the TDX Secure Arbitration Mode (SEAM) Loader, which helps to verify the digital signature on the Intel TDX module and load it into the SEAM-memory range.	4.3(3a)	X410c M7, X210c M7, C220 M7, C240 M7	Enabled, **Disabled**	To enable TDX Secure Arbitration Mode Loader, ensure that: • Total Memory Encryption (TME) is Enabled. • Software Guard Extensions (SGX) is Enabled. • Multikey Total Memory Encryption (MK-TME) is Enabled. • LIMIT CPU PA to 46 Bits token is Disabled. • Trust Domain Extension (TDX) is Enabled.
TPM Pending Operation	Trusted Platform Module (TPM) Pending Operation option allows you to control the status of the pending operation.	4.2(1), 5.0(1), 5.0(2)	C240 M6, C220 M6, C225 M6, C245 M6, B200 M6, X210c M6, C220 M7, C240 M7, X210c M7, X410c M7	**None**, TpmClear	If the Security Device Support is disabled then the entire TPM operation will fail.
TPM Minimal Physical Presence	Whether to enable or disable TPM Minimal Physical Presence, which enables or disables the communication between the OS and BIOS for administering the TPM without compromising the security.	4.2(1)	C240 M6, C220 M6, C225 M6, C245 M6, B200 M6, X210c M6, C220 M7, C240 M7, X210c M7, X410c M7	Enabled, **Disabled**	If the Security Device Support is disabled then the entire TPM operation will fail.
Intel Trusted Execution Technology Support	Whether to enable or disable Intel Trusted Execution Technology (TXT), which provides greater protection for information that is used and stored on the business server.	4.2(1), 5.0(1), 5.0(2)	C240 M6, C220 M6, C225 M6, C245 M6, B200 M6, X210c M6, C220 M7, C240 M7, X210c M7, X410c M7	**Enabled**, Disabled	TPM cannot be disabled unless TXT is disabled.

Name	Description	Supported Attributes			
		Versions	Platforms	Values	Dependencies
Security Device Support	It controls the entire TPM functionality.	4.2(3)	C220M6, C240M6, C225M6, C245M6, B200M6, X210c M6, C220 M7, C240 M7, X210c M7, X410c M7	**Enabled**, Disabled	
DMA Control Opt-In Flag	Enabling this token enables Windows 2022 Kernel DMA Protection feature. The OS treats this as a hint that the IOMMU should be enabled to prevent DMA attacks from possible malicious devices.	4.2(2), 4.2(3)	C220 M6 and C240 M6, B200 M6, X210c M6, C220 M7, C240 M7, X210c M7, X410c M7	Enabled, **Disabled**	
LIMIT CPU PA to 46 Bits	Limits CPU physical address to 46 bits to support the older Hyper-v CPU platform.	4.2(2), 4.2(3)	C220 M6, C240 M6, B200 M6, X210c M6, C220 M7, C240 M7, X210c M7, X410c M7	**Enabled**, Disabled	

Trusted Platform