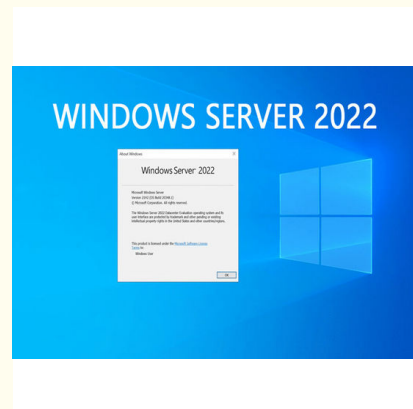


TPM 2.0 VBS Microsoft Windows Server 2022 OEM Online Activation 4GHz

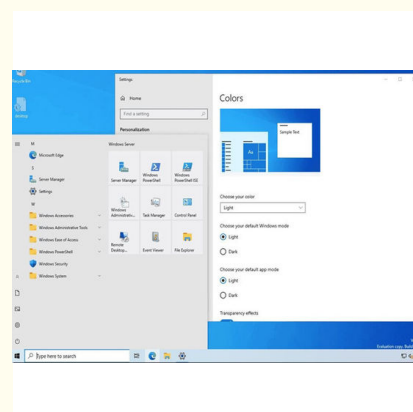
Basic Information

- Place of Origin: Ireland
- Brand Name: Microsoft
- Certification: Microsoft Certified
- Model Number: Windows server 2022
- Minimum Order Quantity: 5 pieces
- Price: Negotiable
- Packaging Details: Factory Sealed Retail box / OEM
- Delivery Time: 48 hours
- Payment Terms: T/T, Western Union, MoneyGram,
- Supply Ability: 5000 pieces/week



Product Specification

- Processor: 4GHz 64-bit Processor
- Language: English
- Optical Storage: DVD Drive
- Package: OEM
- RAM: 512 MB
- Disk Space: 32 GB
- Highlight: **VBS Microsoft Windows Server 2022, TPM 2.0 Microsoft Windows Server 2022, 4GHz Windows Server Key License**



Our Product Introduction

for more products please visit us on computersoftware-systems.com

Product Description

Microsoft Windows Server 2022 Standard OEM Win Server 2022 Datacenter Online Activation Key License

Product description:

Win Server 2022 Standard is the new leading server operating system, and it has several unique features that will make your business prosper. Not only does Win Server 2022 provides fast performance as a reliable workhorse for all types of businesses, but also offers specific benefits to industries, too.

Win Server 2022 is the most recent version of Microsoft's cloud-ready operating system. It comes with technologies that allow it easier for you to migrate your workloads when you're ready. furthermore, this plan ovides a budget-friendly choice so you can save money while still running the programs and applications your business depends on each day.

Features:

Feature	Standard edition	Datacenter edition
Core Windows Server functionality	Feature available	Feature available
Hybrid integration	Feature available	Feature available
Windows Server containers	Unlimited	Unlimited
Storage Replica	Limited feature	Feature available
Software-defined networking	Feature not available	Feature available
Software-defined storage	Feature not available	Feature available

What's new in Windows Server 2022?

Security

The new security capabilities in Windows Server 2022 combine other security capabilities in Windows Server across multiple areas to provide defense-in-depth protection against advanced threats. Advanced multi-layer security in Windows Server 2022 provides the comprehensive protection that servers need today.

Secured-core server

Certified Secured-core server hardware from an OEM partner provides additional security protections that are useful against sophisticated attacks. This can provide increased assurance when handling mission critical data in some of the most data sensitive industries. A Secured-core server uses hardware, firmware, and driver capabilities to enable advanced Windows Server security features. Many of these features are available in Windows Secured-core PCs and are now also available with Secured-core server hardware and Windows Server 2022.

Hardware root-of-trust

Trusted Platform Module 2.0 (TPM 2.0) secure crypto-processor chips provide a secure, hardware-based store for sensitive cryptographic keys and data, including systems integrity measurements. TPM 2.0 can verify that the server has been started with legitimate code and can be trusted by subsequent code execution. This is known as a hardware root-of-trust and is used by features such as BitLocker drive encryption.

Virtualization-based security (VBS)

Secured-core servers support virtualization-based security (VBS) and hypervisor-based code integrity (HVCI). VBS uses hardware virtualization features to create and isolate a secure region of memory from the normal operating system, protecting against an entire class of vulnerabilities used in cryptocurrency mining attacks. VBS also allows for the use of Credential Guard, where user credentials and secrets are stored in a virtual container that the operating system cannot access directly.

Firmware protection

Firmware executes with high privileges and is often invisible to traditional anti-virus solutions, which has lead to a rise in the number of firmware-based attacks. Secured-core server processors support measurement and verification of boot processes with Dynamic Root of Trust for Measurement (DRTM) technology and isolation of driver access to memory with Direct Memory Access (DMA) protection.

HVCI uses VBS to significantly strengthen code integrity policy enforcement, including kernel mode integrity which checks all kernel mode drivers and binaries in a virtualized environment before they are started, preventing unsigned drivers or system files from being loaded into system memory.

Secure connectivity

Transport: HTTPS and TLS 1.3 enabled by default on Windows Server 2022

Secure connections are at the heart of today's interconnected systems. Transport Layer Security (TLS) 1.3 is the latest version of the internet's most deployed security protocol, which encrypts data to provide a secure communication channel between two endpoints. HTTPS and TLS 1.3 is now enabled by default on Windows Server 2022, protecting the data of clients connecting to the server. It eliminates obsolete cryptographic algorithms, enhances security over older versions, and aims to encrypt as much of the handshake as possible. Learn more about supported TLS versions and about supported cipher suites.

Server Message Block (SMB): SMB AES-256 encryption for the most security conscious

Windows Server now supports AES-256-GCM and AES-256-CCM cryptographic suites for SMB encryption and signing. Windows will automatically negotiate this more advanced cipher method when connecting to another computer that also supports it, and it can also be mandated through Group Policy. Windows Server still supports AES-128 for down-level compatibility.

Secure DNS: Encrypted DNS name resolution requests with DNS-over-HTTPS

DNS Client in Windows Server 2022 now supports DNS-over-HTTPS (DoH) which encrypts DNS queries using the HTTPS protocol. This helps keep your traffic as private as possible by preventing eavesdropping and your DNS data being manipulated. Learn more about configuring the DNS client to use DoH.

SMB: East-West SMB encryption controls for internal cluster communications

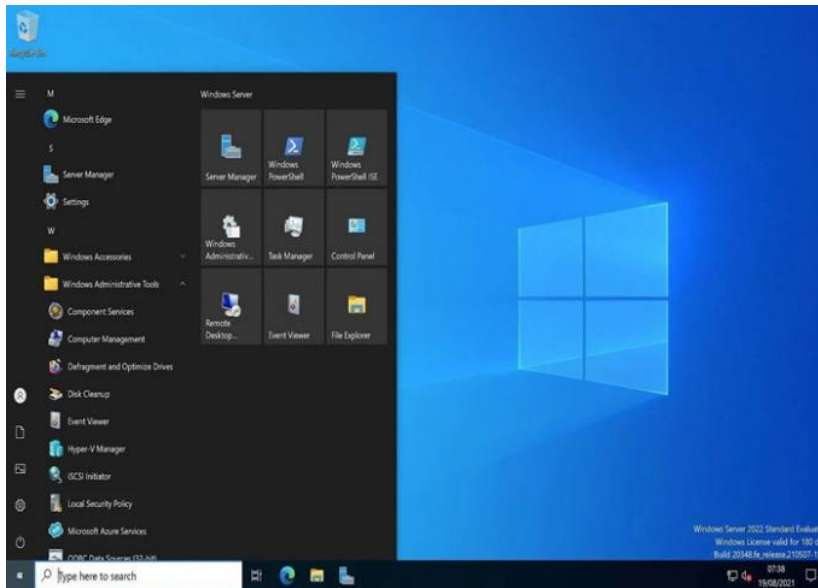
Windows Server failover clusters now support granular control of encrypting and signing intra-node storage communications for Cluster Shared Volumes (CSV) and the storage bus layer (SBL). This means that when using Storage Spaces Direct, you can decide to encrypt or sign east-west communications within the cluster itself for higher security.

SMB Direct and RDMA encryption

SMB Direct and RDMA supply high bandwidth, low latency networking fabric for workloads like Storage Spaces Direct, Storage Replica, Hyper-V, Scale-out File Server, and SQL Server. SMB Direct in Windows Server 2022 now supports encryption. Previously, enabling SMB encryption disabled direct data placement; this was intentional, but seriously impacted performance. Now data is encrypted before placement, leading to far less performance degradation while adding AES-128 and AES-256 protected packet privacy.

SMB over QUIC

SMB over QUIC updates the SMB 3.1.1 protocol in Windows Server 2022 Datacenter: Azure Edition and supported Windows clients to use the QUIC protocol instead of TCP. By using SMB over QUIC along with TLS 1.3, users and applications can securely and reliably access data from edge file servers running in Azure. Mobile and telecommuter users no longer need a VPN to access their file servers over SMB when on Windows. More information can be found at the [SMB over QUIC documentation](#).



Minko Software Service Co. LTD



86-13539872669



sales@hkminko.com



computersoftware-systems.com

Huaqiang North ,Futian district,Shenzhen City,China