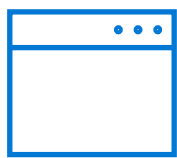
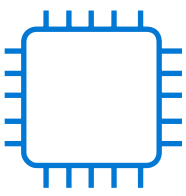


Windows 11 Security Book: Powerful security by design

Table of contents



Introduction

Emerging technologies and evolving business trends bring new opportunities and challenges for organizations of all sizes. As technology and workstyles transform, so does the threat landscape with growing numbers of increasingly sophisticated attacks on organizations and employees.

To thrive, organizations need security to work anywhere. [Microsoft's 2022 Work Trend Index shows](#) "cybersecurity issues and risks" are top concerns for business decision-makers, who worry about issues like malware, stolen credentials, devices that lack security updates, and physical attacks on lost or stolen devices.

In the past, a corporate network and software-based security were the first lines of defense. With an increasingly distributed and mobile workforce, attention has shifted to hardware-based endpoint security. People are now the top target for cybercriminals, with 74% of all breaches due to human error, privilege misuses, stolen credentials, or social engineering. Most attacks are financially motivated, and credential theft, phishing, and exploitation of vulnerabilities are the primary attack vectors. Credential theft is the most prevalent attack vector, accounting for 50% of breaches.¹

At Microsoft, we work hard to help organizations evolve and stay agile while protecting against modern threats. We're committed to helping businesses and their employees get secure—and stay secure. We [synthesize 43 trillion signals daily](#) to understand and protect against digital threats. We have more than 8,500 dedicated security professionals across 77 countries and over 15,000 partners in our security ecosystem striving to increase resilience for our customers.²

Businesses worldwide are moving toward [secure-by-design and secure-by-default strategies](#). With these models, organizations choose products from manufacturers that consider security as a business requirement, not just a technical feature. With a secure-by-default strategy, businesses can proactively reduce risk and exposure to threats across their organization because products are shipped with security features already built in and enabled.

To help businesses transform and thrive in a new era, we built Windows 11 to be secure by design and secure by default. Windows 11 devices arrive with more security features enabled out of the box. In contrast, Windows 10 devices came with many safeguards turned off unless enabled by IT or employees. The default security provided by Windows 11 elevates protection without needing to configure settings. In addition, Windows 11 devices have been shown to increase malware resistance without impacting performance.³

Windows 11 is the most secure Windows ever, built in deep partnership with original equipment manufacturers (OEMs) and silicon manufacturers. Discover why organizations of all sizes, including 90% of Fortune 500 companies, are taking advantage of the powerful default protection of Windows 11.⁴

Security priorities and benefits

Security by design and security by default

Windows 11 is designed with layers of security enabled by default, so you can focus on your work, not your security settings. Out-of-the-box features such as credential safeguards, malware shields, and application protection led to a reported 58% drop in security incidents, including a 3.1x reduction in firmware attacks.⁵

Out-of-the-box features such as credential safeguards, malware shields, and application protection led to a reported 58% drop in security incidents, including a 3.1x reduction in firmware attacks.

In Windows 11, hardware and software work together to shrink the attack surface, protect system integrity, and shield valuable data. New and enhanced features are designed for security by default. For example, Win32 apps in isolation (public preview)⁶, token protection (public preview)⁶, and Microsoft Intune Endpoint Privilege Management⁷ are some of the latest capabilities that help protect your organization and employees against attack. Windows Hello and Windows Hello for Business work with hardware-based features like TPM 2.0 and biometric scanners for credential protection and easier, secure sign-on. Existing security features like BitLocker encryption have also been enhanced to optimize both security and performance.

Protect employees against evolving threats

With attackers targeting employees and their devices, organizations need stronger security against increasingly sophisticated cyberthreats. Windows 11 provides proactive protection against credential theft. Windows Hello and TPM 2.0 work together to shield identities. Secure biometric sign-in virtually eliminates the risk of lost or stolen passwords. And enhanced phishing protection increases safety. In fact, businesses reported 2.8x fewer instances of identity theft with the hardware-backed protection in Windows 11.⁵

Businesses reported 2.8x fewer instances of identity theft with the hardware-backed protection in Windows 11.⁵

Gain mission-critical application safeguards

Help keep business data secure and employees productive with robust safeguards and control for applications. Windows 11 has multiple layers of application security that shield critical data and code integrity. Application protection, privacy controls, and least-privilege principles enable developers to build in security by design. This integrated security protects against breaches and malware, helps keep data private, and gives IT administrators the controls they need. As a result, organizations and regulators can be confident that critical data is protected.

End-to-end protection with modern management

Increase protection and efficiency with Windows 11 and chip-to-cloud security. Microsoft offers comprehensive cloud services for identity, storage, and access management. In addition, Microsoft also provides the tools needed to attest that Windows 11 devices connecting to your network or accessing your data and resources are trustworthy. You can also enforce compliance and conditional access with modern device management (MDM) solutions such as Microsoft Intune⁹ and [Microsoft Entra ID](#) (formerly known as Azure Active Directory).

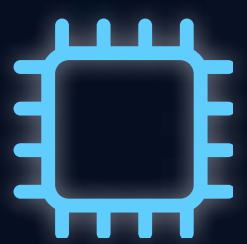
Security by default not only enables people to work securely anywhere, but it also simplifies IT. A streamlined, chip-to-cloud security solution based on Windows 11 has improved productivity for IT and security teams by a reported 25%.⁸

Security by design and default

In Windows 11, hardware and software work together to protect sensitive data from the core of your PC all the way to the cloud. Comprehensive protection helps keep your organization secure, no matter where people work. This simple diagram shows the layers of protection in Windows 11, while each chapter provides a layer-by-layer deep dive into features.



► Learn more: [Windows security features licensing and edition requirements](#)



Hardware Security



Today's ever-evolving threats require strong alignment between hardware and software technologies to keep users, data, and devices protected. The operating system alone cannot defend against the wide range of tools and techniques cybercriminals use to compromise a computer. Once they gain a foothold, intruders can be difficult to detect as they engage in multiple nefarious activities ranging from stealing important data and credentials to implanting malware into low-level device firmware. Once malware is installed in firmware, it becomes difficult to identify and remove.

These new threats call for computing hardware that is secure down to the very core, including the hardware chips and processors that store sensitive business information. With hardware-based protection, we can enable strong mitigation against entire classes of vulnerabilities that are difficult to thwart with software alone. Hardware-based protection can also improve the system's overall security without measurably slowing performance, compared to implementing the same capability in software.

With Windows 11, Microsoft has raised the hardware security bar to design the most secure version of Windows ever from chip to cloud. We have carefully chosen the hardware requirements and default security features based on threat intelligence, global regulatory requirements, and our own Microsoft Security team's expertise. We have worked with our chip and device manufacturing partners to integrate advanced security capabilities across software, firmware, and hardware.

Through a powerful combination of hardware root-of-trust and silicon-assisted security, Windows 11 delivers built-in hardware protection out of the box.

Hardware root-of-trust

A hardware root-of-trust helps protect and maintain the integrity of the system as the device powers on, loads firmware, and then launches the operating system, meeting important system security goals.

For example, the Secure Boot process provides a secure startup environment that allows devices to boot only with software trusted by the original equipment manufacturer (OEM). When the PC starts, the firmware checks the signature of each piece of boot software, including Unified Extensible Firmware Interface (UEFI) firmware drivers (also known as Option ROMs), Extensible Firmware Interface (EFI) applications, and the operating system. If the signatures are valid, the PC boots, and the firmware gives control to the operating system. Rollback protection also prevents the system from rolling back to older versions of firmware.

In addition, hardware root-of-trust provides a highly secure area for storing cryptographic keys, data, and code, isolated from the operating system and applications. This protection helps mitigate attacks against the Windows authentication stack, single sign-on tokens, the Windows Hello biometric stack, and BitLocker volume encryption keys.

Trusted Platform Module (TPM)

Trusted Platform Module (TPM) technology is designed to provide hardware-based, security-related functions. TPMs provide security and privacy benefits for system hardware, platform owners, and users. Windows Hello, BitLocker, System Guard (previously called Windows Defender System Guard), and other Windows features rely on the TPM for capabilities such as key generation, secure storage, encryption, boot integrity measurements, and attestation. These capabilities in turn help organizations strengthen the protection of their identities and data.

The 2.0 version of TPM includes support for newer algorithms, which provides improvements like support for stronger cryptography. To upgrade to Windows 11, existing Windows 10 devices must meet minimum system requirements for CPU, RAM, storage, firmware, TPM, and more. All new Windows 11 devices come with TPM 2.0 built in. With Windows 11, both new and upgraded devices must have TPM 2.0. The requirement strengthens the security posture across all Windows 11 devices and helps ensure that these devices can benefit from future security capabilities that depend on a hardware root-of-trust.

Learn more: [Windows 11 TPM specifications](#)

Learn more: [Enabling TPM 2.0 on your PC](#)

Learn more: [Trusted Platform Module technology overview](#)

Microsoft Pluton

The Microsoft Pluton security processor is the result of Microsoft's close partnership with silicon partners. Pluton enhances the protection of Windows 11 devices, including Secured-core PCs, with a hardware security processor that provides additional protection for cryptographic keys and other secrets. Pluton is designed to reduce the attack surface by integrating the security chip directly into the processor. It can be used as a TPM 2.0 or as a standalone security processor. When a security processor is located on a separate, discrete chip on the motherboard, the communication path between the hardware root-of-trust and the CPU can be vulnerable to physical attack. Embedding Pluton into the CPU makes it harder to exploit the communication path.

Pluton supports the TPM 2.0 industry standard, allowing customers to immediately benefit from enhanced security for Windows features that rely on TPMs, including BitLocker, Windows Hello, and System Guard. Pluton can also support other security functionality beyond what is possible with the TPM 2.0 specification. This extensibility allows for additional Pluton firmware and OS features to be delivered over time via Windows Update.

As with other TPMs, credentials, encryption keys, and other sensitive information cannot be easily extracted from Pluton even if an attacker has installed malware or has complete physical possession of the PC. Storing sensitive data like encryption keys securely within the Pluton processor, which is isolated from the rest of the system, helps ensure that attackers cannot access sensitive data—even if attackers use emerging techniques like speculative execution.

Pluton also solves the major security challenge of keeping its own security processor firmware up to date across the entire PC ecosystem. Today customers receive updates to their security firmware from a variety of different sources, which may make it difficult for customers to get alerts about security updates, keeping systems in a vulnerable state. Pluton provides a flexible, updateable platform for its firmware that implements end-to-end security functionality authored, maintained, and updated by Microsoft. Pluton is integrated with the Windows Update service, benefiting from over a decade of operational experience in reliably delivering updates across over a billion endpoint systems.

Microsoft Pluton is available with select new Windows PCs.

Learn more: [Meet the Microsoft Pluton processor – The security chip designed for the future of Windows PCs](#)

Learn more: [Microsoft Pluton security processor](#)

Silicon assisted security

In addition to a modern hardware root-of-trust, there are numerous other capabilities in the latest chips that harden the operating system against threats by protecting the boot process, safeguarding the integrity of memory, isolating security-sensitive compute logic, and more.

Secured kernel

To secure the kernel we have two key features: virtualization-based security (VBS) and hypervisor-protected code integrity (HVCI). All Windows 11 devices will support HVCI and most new devices will come with VBS and HVCI protection turned on by default.

Virtualization-based security (VBS), also known as core isolation, is a critical building block in a secure system. VBS uses hardware virtualization features to host a secure kernel separated from the operating system. This means that even if the operating system is compromised, the secure kernel is still protected.

The isolated VBS environment protects processes, such as security solutions and credential managers, from other processes running in memory. Even if malware gains access to the main OS kernel, the hypervisor and virtualization hardware help prevent the malware from executing unauthorized code or accessing platform secrets in the VBS environment. VBS implements virtual trust level 1 (VTL1), which has higher privilege than the virtual trust level 0 (VTL0) implemented in the main kernel.

Since more privileged VTLs can enforce their own memory protections, higher VTLs can effectively protect areas of memory from lower VTLs. In practice, this allows a lower VTL to protect isolated memory regions by securing them with a higher VTL. For example, VTL0 could store a secret in VTL1, at which point only VTL1 could access it. Even if VTL0 is compromised, the secret would be safe.

Learn more: [Virtualization-based security \(VBS\)](#)

Hypervisor-protected code integrity (HVCI), also called memory integrity, uses VBS to run Kernel Mode Code Integrity (KMCI) inside the secure VBS environment instead of the main Windows kernel. This helps prevent attacks that attempt to modify kernel-mode code for things like drivers. The KMCI checks that all kernel code is properly signed and hasn't been tampered with before it is allowed to run.

HVCI ensures that only validated code can be executed in kernel mode. The hypervisor leverages processor virtualization extensions to enforce memory protections that prevent kernel-mode software from executing code that has not been first validated by the code integrity subsystem. HVCI protects against common attacks like WannaCry that rely on the ability to inject malicious code into the kernel. HVCI can prevent injection of malicious kernel-mode code even when drivers and other kernel-mode software have bugs.

All Windows 11 devices will support HVCI, and most new devices will come with VBS and HVCI protection turned on by default.

Learn more: [Enable memory integrity](#)

Hardware-enforced stack protection

[Hardware-enforced stack protection](#) integrates software and hardware for a modern defense against cyberthreats like memory corruption and zero-day exploits. Based on Control-flow Enforcement Technology (CET) from Intel and AMD Shadow Stacks, hardware-enforced stack protection is designed to protect against exploit techniques that try to hijack return addresses on the stack.

Application code includes a program processing stack that hackers seek to corrupt or disrupt in a type of attack called stack smashing. When defenses like executable space protection began thwarting such attacks, hackers turned to new methods like return-oriented programming. Return-oriented programming, a form of advanced stack smashing, can bypass defenses, hijack the data stack, and ultimately force a device to perform harmful operations.

To guard against these control-flow hijacking attacks, the Windows kernel creates a separate “shadow stack” for return addresses. Windows 11 extends stack protection capabilities to provide both user mode and kernel mode support.

Kernel Direct Memory Access (DMA) Protection

Windows 11 also provides protection against physical threats such as drive-by Direct Memory Access (DMA) attacks. Peripheral Component Interconnect Express (PCIe) hot-pluggable devices such as Thunderbolt, USB4, and CExpress allow users to attach new classes of external peripherals, including graphics cards or other PCI devices, to their PCs with the plug-and-play ease of USB. Because PCI hot-plug ports are external and easily accessible, PCs are susceptible to drive-by DMA attacks.

Memory access protection (also known as [Kernel DMA Protection](#)) protects against these attacks by preventing external peripherals from gaining unauthorized access to memory.

Drive-by DMA attacks typically happen quickly while the system owner isn’t present. The attacks are performed using simple to moderate attacking tools created with affordable, off-the-shelf hardware and software that do not require the disassembly of the PC.

For example, a PC owner might leave a device for a quick coffee break. Meanwhile, an attacker plugs an external tool into a port to steal information or inject code that gives the attacker remote control over the PCs, including the ability to bypass the lock screen. With memory access protection built in and enabled, Windows 11 is protected against physical attack wherever people work.

Windows 11 Secured-core PCs

The March 2021 [Security Signals](#) report found that more than 80% of enterprises have experienced at least one firmware attack in the past two years. For customers in data-sensitive industries like financial services, government, and healthcare, Microsoft has worked with OEM partners to offer a special category of devices called [Secured-core PCs \(SCPCs\)](#). The devices ship with additional security measures enabled at the firmware layer, or device core, that underpins Windows.

Secured-core PCs help prevent malware attacks and minimize firmware vulnerabilities by launching into a clean and trusted state at startup with a hardware-enforced root-of-trust. Virtualization-based security comes enabled by default. With built-in hypervisor-protected code integrity (HVCI) shielding system memory, Secured-core PCs ensure that all kernel executable code is signed only by known and approved authorities. Secured-core PCs also protect against physical threats such as drive-by Direct Memory Access (DMA) attacks with kernel DMA protection.

Secured-core PC firmware protection

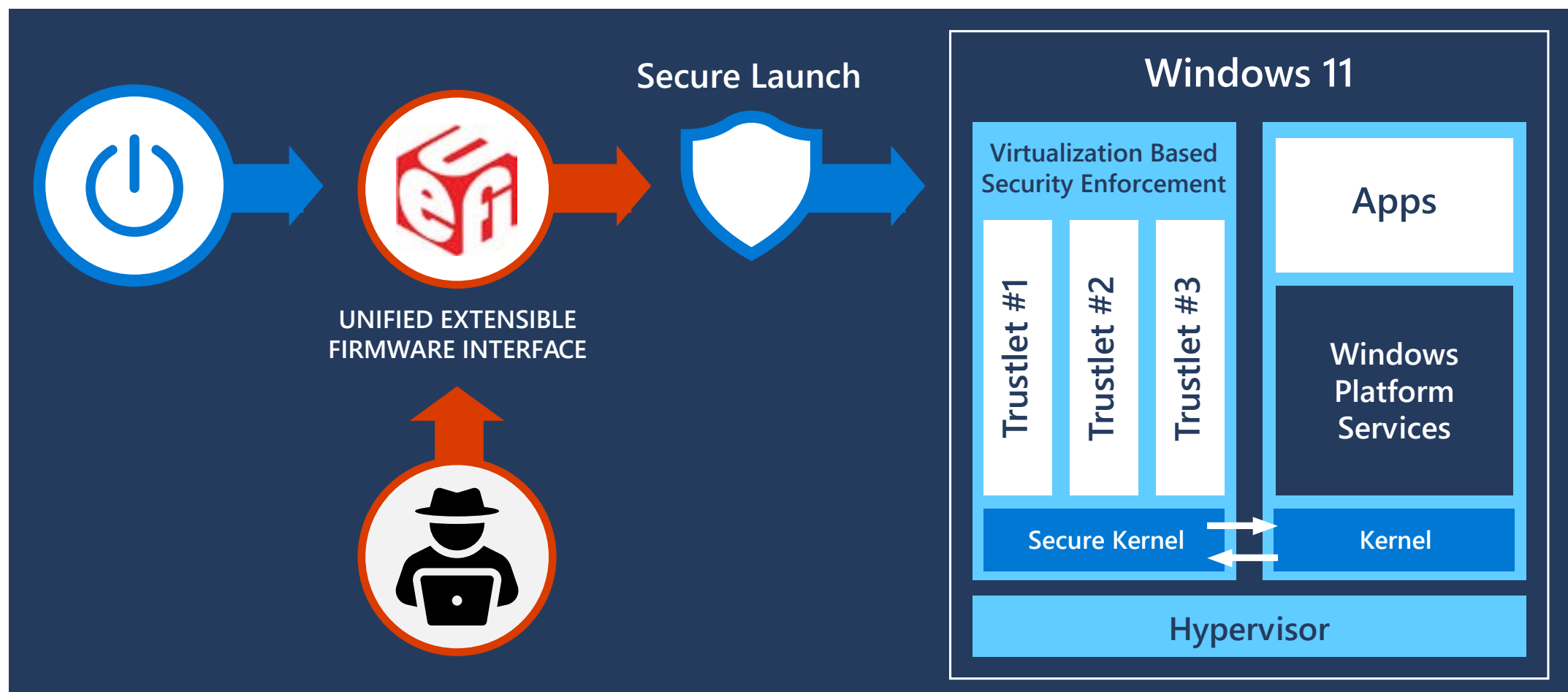
Secured-core PCs provide multiple layers of robust protection against hardware and firmware attacks. Sophisticated malware attacks may commonly attempt to install “bootkits” or “rootkits” on the system to evade detection and achieve persistence. This malicious software may run at the firmware level prior to Windows being loaded or during the Windows boot process itself, enabling the system to start with the highest level of privilege. Because critical subsystems in Windows leverage virtualization-based security, protecting the hypervisor becomes increasingly important. To ensure that no unauthorized firmware or software can start before the Windows bootloader, Windows PCs rely on the Unified Extensible Firmware Interface (UEFI) Secure Boot standard, a baseline security feature of all Windows 11 PCs. Secure Boot helps ensure that only authorized firmware and software with trusted digital signatures can execute. In addition, measurements of all boot components are securely stored in the TPM to help establish a non-repudiable audit log of the boot called the Static Root of Trust for Measurement (SRTM).

Thousands of PC vendors produce numerous device models with diverse UEFI firmware components, which in turn creates an incredibly large number of SRTM signatures and measurements at bootup. Because these signatures and measurements are inherently trusted by Secure Boot, it can be challenging to constrain trust to only what is needed to boot on any specific device. Traditionally, blocklists and allowlists were the two main techniques used to constrain trust, and they continue to expand if devices rely only on SRTM measurements.

In Secured-core PCs, [System Guard Secure Launch](#) protects bootup with a technology known as the Dynamic Root of Trust for Measurement (DRTM). With DRTM, the system initially follows the normal UEFI Secure Boot process. However, before launching, the system enters a hardware-controlled trusted state that forces the CPU(s) down a hardware-secured code path. If a malware rootkit or bootkit has bypassed UEFI Secure Boot and resides in memory, DRTM will prevent it from accessing secrets and critical code protected by the virtualization-

based security environment. [Firmware Attack Surface Reduction \(FASR\) technology](#) can be used instead of DRTM on supported devices such as Microsoft Surface.

System Management Mode (SMM) isolation is an execution mode in x86-based processors that runs at a higher effective privilege than the hypervisor. SMM complements the protections provided by DRTM by helping to reduce the attack surface. Relying on capabilities provided by silicon providers like Intel and AMD, SMM isolation enforces policies that implement restrictions such as preventing SMM code from accessing OS memory. The SMM isolation policy is included as part of the DRTM measurements that can be sent to a verifier like Microsoft Azure Remote Attestation.



Learn more: [Dynamic Root of Trust measure and SMM isolation](#)

Secured-core configuration lock (config lock)

In enterprise organizations, IT administrators enforce policies on their corporate devices to protect the OS and keep devices in a compliant state by preventing users from changing configurations and creating configuration drift. Configuration drift occurs when users with local admin rights change settings and put the device out of sync with security policies. Devices in a non-compliant state can be vulnerable until the next sync, when configuration is reset with the modern device management (MDM) solution.

Secured-core configuration lock (config lock) is a Secured-core PC feature that prevents users from making unwanted changes to security settings. With config lock, the OS monitors the registry keys that are supported and reverts to the IT-desired SCPC state in seconds after detecting a drift.

Learn more: [Windows 11 with config lock](#)



Operating System Security



Windows 11 is the most secure Windows yet with extensive security measures in the operating system designed to help keep devices, identities, and information safe. These measures include built-in advanced encryption and data protection, robust network system security, and intelligent safeguards against ever-evolving viruses and threats.

System security

Trusted Boot (Secure Boot + Measured Boot)

Windows 11 requires all PCs to use Unified Extensible Firmware Interface (UEFI)'s Secure Boot feature. When a Windows 11 device starts, Secure Boot and Trusted Boot work together to prevent malware and corrupted components from loading. Secure Boot provides initial protection, then Trusted Boot picks up the process.

Secure Boot makes a safe and trusted path from the Unified Extensible Firmware Interface (UEFI) through the Windows kernel's Trusted Boot sequence. Malware attacks on the Windows boot sequence are blocked by the signature-enforcement handshakes throughout the boot sequence between the UEFI, bootloader, kernel, and application environments.

To reduce the risk of firmware rootkits, the PC verifies that firmware is digitally signed as it begins the boot process. Then Secure Boot checks the OS bootloader's digital signature as well as all code that runs prior to the operating system starting to ensure the signature and code are uncompromised and trusted by the Secure Boot policy.

Trusted Boot picks up the process that begins with Secure Boot. The Windows bootloader verifies the digital signature of the Windows kernel before loading it. The Windows kernel, in turn, verifies every other component of the Windows startup process, including boot drivers, startup files, and any antimalware product's early-launch antimalware (ELAM) driver. If any of these files have been tampered with, the bootloader detects the problem and refuses to load the corrupted component. Often, Windows can automatically repair the corrupted component, restoring the integrity of Windows and allowing the PC to start normally.

Tampering or malware attacks on the Windows boot sequence are blocked by the signature enforcement handshakes between the UEFI, bootloader, kernel, and application environments.

For more information about these features and how they help prevent rootkits and bootkits from loading during the startup process, see [Secure the Windows boot process](#).

Learn more: [Secure Boot and Trusted Boot](#)

Cryptography

Cryptography is designed to protect user and system data. The cryptography stack in Windows 11 extends from the chip to the cloud, enabling Windows, applications, and services to protect system and user secrets. For example, data can be encrypted so that only a specific reader with a unique key can read it. As a basis for data security, cryptography helps prevent anyone except the intended recipient from reading data, performs integrity checks to ensure data is free of tampering, and authenticates identity to ensure that communication is secure.

Windows 11 cryptography is certified to meet the Federal Information Processing Standard (FIPS) 140. FIPS 140 certification ensures that US government-approved algorithms are correctly implemented.

Learn more: [FIPS 140 validation](#)

Windows cryptographic modules provide low-level primitives such as:

- Random number generators (RNG)
- Support for AES 128/256 with XTS, ECB, CBC, CFB, CCM, and GCM modes of operation; RSA and DSA 2048, 3072, and 4096 key sizes; ECDSA over curves P-256, P-384, P-521
- Hashing (support for SHA1, SHA-256, SHA-384, and SHA-512)
- Signing and verification (padding support for OAEP, PSS, and PKCS1)
- Key agreement and key derivation (support for ECDH over NIST-standard prime curves P-256, P-384, P-521 and HKDF)

Application developers can use these cryptographic modules to perform low-level cryptographic operations (Bcrypt), key storage operations (NCrypt), protect static data (DPAPI), and securely share secrets (DPAPI-NG).

Learn more: [Cryptography and certificate management](#)

Developers can access the modules on Windows through the Cryptography Next Generation API (CNG), which is powered by Microsoft's open-source cryptographic library, SymCrypt. SymCrypt supports complete transparency through its open-source code. In addition, SymCrypt offers performance optimization for cryptographic operations by taking advantage of assembly and hardware acceleration when available.

SymCrypt is part of Microsoft's commitment to transparency, which includes the global Microsoft Government Security Program that aims to provide the confidential security information and resources people need to trust Microsoft's products and services. The program offers controlled access to source code, threat and vulnerability information exchange, opportunities to engage with technical content about Microsoft's products and services, and access to five globally distributed Transparency Centers.

Certificates

To help safeguard and authenticate information, Windows provides comprehensive support for certificates and certificate management.

The built-in certificate management command-line utility (certmgr.exe) or MMC snap-in (certmgr.msc) can be used to view and manage certificates, certificate trust lists (CTLs), and certificate revocation lists (CRLs). Whenever a certificate is used in Windows, we validate that the leaf certificate and all the certificates in its chain of trust have not been revoked or compromised. The CTLs and CRLs on the machine are used as a reference for PKI trust and are updated monthly by the Microsoft Trusted Root program. If a trusted certificate or root is revoked, all global devices will be updated, meaning users can trust that Windows will automatically protect against vulnerabilities in public key infrastructure.

For cloud and enterprise deployments, Windows also offers users the ability to auto-enroll and renew certificates in Active Directory with Group Policy to reduce the risk of potential outages due to certificate expiration or misconfiguration. Additionally, enterprise certificate pinning can be used to help reduce man-in-the-middle attacks by enabling users to protect their internal domain names from chaining to unwanted certificates. A web application's server authentication certificate chain is checked to ensure it matches a restricted set of certificate authorities. Any web application triggering a name mismatch will start event logging and prevent user access from Microsoft Edge.

Code signing and integrity

To ensure that Windows files have not been tampered with, the Windows Code Integrity process verifies the signature of each file in Windows. Code signing is core to establishing the integrity of firmware, drivers, and software across the Windows platform. Code signing creates a digital signature by encrypting the hash of the file with the private key portion of a code-signing certificate and embedding the signature into the file. The Windows code integrity process verifies the signed file by decrypting the signature to check the integrity of the file and confirm that it is from a reputable publisher, ensuring that the file hasn't been tampered with.

The digital signature is evaluated across the Windows environment on Windows boot code, Windows kernel code, and Windows user mode applications. Secure Boot and Code Integrity verify the signature on bootloaders, Option ROMs, and other boot components to ensure that it is trusted and from a reputable publisher. For drivers not published by Microsoft, Kernel Code Integrity verifies the signature on kernel drivers and requires that drivers be signed by Windows or certified by the [Windows Hardware Compatibility Program](#) (WHCP). This program ensures that third-party drivers are compatible with various hardware and Windows and that the drivers are from vetted driver developers.

Device health attestation

The Windows device health attestation process supports a [Zero Trust](#) paradigm that shifts the focus from static, network-based perimeters to users, assets, and resources.

The attestation process confirms the device, firmware, and boot process are in a good state and have not been tampered with before they can access corporate resources. These determinations are made with data stored in the TPM, which provides a secure root-of-trust. The information is sent to an attestation service such as Azure Attestation to verify that the device is in a trusted state. Then a modern device management (MDM) tool like Microsoft Intune⁹ reviews device health and connects this information with Microsoft Entra ID⁹ for conditional access.

Windows includes many security features to help protect users from malware and attacks. However, security components are trustworthy only if the platform boots as expected and is not tampered with. As noted above, Windows relies on Unified Extensible Firmware Interface (UEFI) Secure Boot, ELAM, DRTM, Trusted Boot, and other low-level hardware and firmware security features to protect your PC from attacks. From the moment you power on your PC until your antimalware starts, Windows is backed with the appropriate hardware configurations that help keep you safe. [Measured Boot](#), implemented by bootloaders and BIOS, verifies and cryptographically records each step of the boot in a chained manner. These events are bound to the TPM, that functions as a hardware root-of-trust. Remote attestation is the mechanism by which these events are read and verified by a service to provide a verifiable, unbiased, and tamper-resilient report. Remote attestation is the trusted auditor of your system's boot, allowing reliant parties to bind trust to the device and its security.

A summary of the steps involved in attestation and Zero-Trust on a Windows device are as follows:

- During each step of the boot process—such as a file load, update of special variables, and more—information such as file hashes and signature(s) are measured in the TPM Platform Configuration Register (PCRs). The measurements are bound by a [Trusted Computing Group specification](#) that dictates which events can be recorded and the format of each event. The data provides important information about device security from the moment it powers on.
- Once Windows has booted, the attester (or verifier) requests the TPM get the measurements stored in its PCRs alongside the Measured Boot log. Together, these form the attestation evidence that's sent to the Microsoft Azure Attestation Service.
- The TPM is verified by using the keys or cryptographic material available on the chipset with an [Azure Certificate Service](#).
- The above information is sent to the [Azure Attestation Service](#) to verify that the device is in a trusted state.

Learn more: [Control the health of Windows devices](#)

Windows security policy settings and auditing

Security policy settings are a critical part of your overall security strategy. Windows provides a robust set of security setting policies that IT administrators can use to help protect Windows devices and other resources in your organization. Security policies settings are rules you can configure on a device, or multiple devices, to control:

- User authentication to a network or device.
- Resources that users are permitted to access.
- Whether to record a user or group's actions in the event log.
- Membership in a group.

Security auditing is one of the most powerful tools that you can use to maintain the integrity of your network and assets. Auditing can help identify attacks, network vulnerabilities, and attacks against high-value targets. You can specify categories of security-related events to create an audit policy tailored to the needs of your organization.

All auditing categories are disabled when Windows is first installed. Before enabling them, follow these steps to create an effective security auditing policy:

1. Identify your most critical resources and activities.
2. Identify the audit settings you need to track them.
3. Assess the advantages and potential costs associated with each resource or setting.
4. Test these settings to validate your choices.
5. Develop plans for deploying and managing your audit policy.

Learn more: [Security policy settings](#)

Learn more: [Security auditing](#)

Kiosk Mode (a.k.a. Assigned Access)

With Assigned Access, Windows 11 devices restrict functionality to pre-selected applications depending on the user and keep individual identities separate, which is ideal for public-facing or shared devices. Configuring a device in Kiosk Mode is a straightforward process. You can do this locally on the device or remotely using modern device management.

Learn more: [Kiosk Mode](#)

Config Refresh

With traditional Group Policy, policies were refreshed on a PC when a user signed in and every 90 minutes by default. Administrators could adjust that timing to be shorter to ensure that the PC's policies were compliant with the management settings set by IT.

By contrast, with an MDM solution like Microsoft Intune⁹, policies are refreshed when a user signs in and then at eight-hour intervals by default. But as more available group policies were implemented through MDM, one remaining gap was the longer period between the reapplication of a changed policy.

Config Refresh allows settings in the Policy configuration service provider (CSP) that drift due to misconfiguration, registry edits, or malicious software on a PC to be reset to the value the administrator intended every 90 minutes by default. It is configurable to refresh every 30 minutes if desired. The Policy CSP covers hundreds of settings that were traditionally set with Group Policy and are now set through MDM.

Config Refresh can also be “paused” for a configurable period of time, after which it will be reenabled. This is to support scenarios where a helpdesk technician might need to reconfigure a PC for troubleshooting purposes. It can also be resumed at any time by an administrator.

Windows security settings

Visibility and awareness of device security and health are key to any action taken. The Windows built-in security settings provide an at-a-glance view of the security status and health of your device. These insights help you identify issues and act to make sure you’re protected. You can quickly see the status of your virus and threat protection, firewall and network security, device security controls, and more.

Learn more: [Windows security settings](#)

Learn more: [Windows security](#)

Encryption and data protection

When people travel with their PCs, their confidential information travels with them. Wherever confidential data is stored, it must be protected against unauthorized access, whether through physical device theft or from malicious applications.

BitLocker

[BitLocker Drive Encryption](#) is a data protection feature that integrates with the operating system and addresses the threats of data theft or exposure from lost, stolen, or inappropriately decommissioned computers. BitLocker uses the AES algorithm in XTS or CBC mode of operation with 128-bit or 256-bit key length to encrypt data on the volume. Cloud storage on Microsoft OneDrive or Azure⁹ can be used to save recovery key content. BitLocker can be managed by any MDM solution such as Microsoft Intune⁶ using a [configuration service provider \(CSP\)](#).⁹

BitLocker provides encryption for the OS, fixed data, and removable data drives (BitLocker To Go), leveraging technologies like Hardware Security Test Interface (HSTI), Modern Standby, UEFI Secure Boot, and TPM. Windows consistently improves data protection by expanding existing options and providing new strategies.

Learn more: [BitLocker overview](#)

BitLocker To Go

BitLocker To Go refers to BitLocker Drive Encryption on removable data drives. BitLocker To Go includes the encryption of USB flash drives, SD cards, and external hard disk drives. Drives can be unlocked using a password, certificate on a smart card, or recovery password.

Learn more: [BitLocker FAQ](#)

Device Encryption

Device Encryption is consumer-level device encryption that cannot be managed. Device Encryption is turned on by default for devices with the right hardware components (for example, TPM 2.0, UEFI Secure Boot, Hardware Security Test Interface, and Modern Standby). However, for a commercial scenario, it is possible for commercial customers to disable Device Encryption in favor of BitLocker Drive Encryption. BitLocker Drive Encryption is manageable through MDM.

Encrypted hard drive

Encrypted hard drives are a class of hard drives that are self-encrypted at the hardware level and allow for full-disk hardware encryption while being transparent to the device user. These drives combine the security and management benefits provided by BitLocker Drive Encryption with the power of self-encrypting drives.

By offloading the cryptographic operations to hardware, encrypted hard drives increase BitLocker performance and reduce CPU usage and power consumption. Because encrypted hard drives encrypt data quickly, BitLocker deployment can be expanded across enterprise devices with little to no impact on productivity.

Encrypted hard drives enable:

- Smooth performance: Encryption hardware integrated into the drive controller allows the drive to operate at full data rate without performance degradation.
- Strong security based in hardware: Encryption is always “on,” and the keys for encryption never leave the hard drive. The drive authenticates the user independently from the operating system before it unlocks.
- Ease of use: Encryption is transparent to the user, and the user does not need to enable it. Encrypted hard drives are easily erased using an onboard encryption key. There is no need to re-encrypt data on the drive.

- Lower cost of ownership: There is no need for new infrastructure to manage encryption keys since BitLocker leverages your existing infrastructure to store recovery information. Your device operates more efficiently because processor cycles do not need to be used for the encryption process.

Learn more: [Encrypted hard drive](#)

Personal data encryption

Personal Data Encryption refers to a new user authenticated encryption mechanism used to protect user content. Windows Hello for Business is the modern user authentication mechanism which is used with PDE. Windows Hello for Business, either with PIN or biometrics (face or fingerprint), is used to protect the container which houses the encryption keys used by Personal Data Encryption (PDE). When the user logs in (either after bootup or unlocking after a lock screen), the container gets authenticated to release the keys in the container to decrypt user content.

With the first release of PDE (Windows 11 22H2), the PDE API was available, which when adopted by applications can protect data under the purview of the applications. With the platform release of the next Windows version, PDE for Folders will be released, this feature would require no updates to any applications and protects the contents in the Known Windows Folders from bootup till first login. This reduces the barrier for entry for customers and they will be able to get PDE security as part of the OS.

PDE requires Microsoft Entra ID (previously called Azure AD)⁹.

Learn more: [Personal Data Encryption \(PDE\)](#)

Email encryption

Email encryption enables users to encrypt outgoing email messages and attachments so that only intended recipients with a digital identification (ID)—also called a certificate—can read them.¹⁰ Users can digitally sign a message, which verifies the identity of the sender and ensures the message has not been tampered with.

These encrypted messages can be sent by a user to people within their organization as well as external contacts who have proper encryption certificates.

However, recipients using Windows 11 Mail app can only read encrypted messages if the message is received on their Exchange account and they have corresponding decryption keys. Encrypted messages can be read only by recipients who have a certificate. If an encrypted message is sent to recipients whose encryption certificates are not available, the app will prompt you to remove these recipients before sending the email.

Learn more: [Email encryption](#)

Network security

Windows 11 raises the bar for network security, offering comprehensive protection to help people work with confidence from almost anywhere. To help reduce an organization's attack surface, network protection in Windows prevents people from accessing dangerous IP addresses and domains that may host phishing scams, exploits, and other malicious content. Using reputation-based services, network protection blocks access to potentially harmful, low-reputation domains and IP addresses.

New DNS and TLS protocol versions strengthen the end-to-end protections needed for applications, web services, and Zero Trust networking. File access adds an untrusted network scenario with Server Message Block over QUIC, as well as new encryption and signing capabilities. Wi-Fi and Bluetooth advancements also provide greater trust in connections to other devices. In addition, VPN and Windows Firewall (previously called Windows Defender Firewall) platforms offer new ways to easily configure and debug software.

In enterprise environments, network protection works best with Microsoft Defender for Endpoint, which provides detailed reporting on protection events as part of larger investigation scenarios.

Learn more: [How to protect your network](#)

Transport layer security (TLS)

Transport Layer Security (TLS) is the internet's most deployed security protocol, encrypting data in transit to provide a secure communication channel between two endpoints. Windows defaults to the latest protocol versions and strong cipher suites unless policies are in effect to limit them. There are many extensions available, such as client authentication for enhanced server security and session resumption for improved application performance.

TLS 1.3 is the latest version of the protocol and is enabled by default starting with Windows 11 and Windows Server 2022. TLS 1.3 eliminates obsolete cryptographic algorithms, enhances security over older versions, and encrypts as much of the TLS handshake as possible. The handshake is more performant, with one fewer round trip per connection on average, and supports only five strong cipher suites, which provide perfect forward secrecy and reduced operational risk.

Customers using TLS 1.3 (or Windows components that support it, including HTTP.SYS, WinInet, .NET, MsQuic, and more) will get enhanced privacy and lower latencies for their encrypted online connections. Note that if either the client or server does not support TLS 1.3, Windows will fall back to TLS 1.2.

Legacy protocol versions TLS 1.0 and 1.1 are officially deprecated and will be disabled by default in future OS versions only. This change will come to Windows Insider Preview in September 2023. Organizations and application developers are strongly encouraged to begin to identify and remove code dependencies on TLS 1.0/1.1 if they have not done so already.

Learn more: [TLS/SSL overview \(Schannel SSP\)](#)

Learn more: [TLS 1.0 and TLS 1.1 soon to be disabled in Windows](#)

DNS security

In Windows 11, the Windows DNS client supports DNS over HTTPS and DNS over TLS, two encrypted DNS protocols. These allow administrators to ensure their devices protect their name queries from on-path attackers, whether they are passive observers logging browsing behavior or active attackers trying to redirect clients to malicious sites. In a Zero Trust model where no trust is placed in a network boundary, having a secure connection to a trusted name resolver is required.

Windows 11 provides Group Policy as well as programmatic controls to configure DNS over HTTPS behavior. As a result, IT administrators can extend existing security to adopt new models such as Zero Trust. IT administrators can mandate DNS over HTTPS protocol, ensuring that devices that use insecure DNS will fail to connect to network resources. IT administrators also have the option not to use DNS over HTTPS or DNS over TLS for legacy deployments where network edge appliances are trusted to inspect plain-text DNS traffic. By default, Windows 11 will defer to the local administrator on which resolvers should use encrypted DNS.

Support for DNS encryption integrates with existing Windows DNS configurations such as the Name Resolution Policy Table (NRPT) and the system Hosts file, as well as resolvers specified per network adapter or network profile. The integration helps Windows 11 ensure that the benefits of greater DNS security do not regress existing DNS control mechanisms.

Bluetooth protection

The number of Bluetooth devices connected to Windows 11 continues to increase. Windows users connect their Bluetooth headsets, mice, keyboards, and other accessories and improve their day-to-day PC experience by enjoying streaming, productivity, and gaming. Windows supports all standard Bluetooth pairing protocols, including classic and LE Secure connections, secure simple pairing, and classic and LE legacy pairing. Windows also implements host-based LE privacy. Windows updates help users stay current with OS and driver security features in accordance with the Bluetooth Special Interest Group (SIG) and Standard Vulnerability Reports, as well as issues beyond those required by the Bluetooth core industry standards. Microsoft strongly recommends that Bluetooth accessories' firmware and software are kept up to date.

IT-managed environments have a number of [Bluetooth policies](#) (MDM, Group Policy, and PowerShell) that can be managed through MDM tools such as Microsoft Intune⁹. You can configure Windows to use Bluetooth technology while supporting the security needs of your organization. For example, you can allow input and audio while blocking file transfer, force encryption standards, limit Windows discoverability, or even disable Bluetooth entirely for the most sensitive environments.

Securing Wi-Fi connections

Windows Wi-Fi supports industry-standard authentication and encryption methods when connecting to Wi-Fi networks. WPA (Wi-Fi Protected Access) is a security standard defined by the Wi-Fi Alliance (WFA) to provide sophisticated data encryption and better user authentication.

The current security standard for Wi-Fi authentication is WPA3, which provides a more secure and reliable connection method as compared to WPA2 and older security protocols. Windows supports three WPA3 modes—WPA3 Personal, WPA3 Enterprise, and WPA3 Enterprise 192-bit Suite B.

Windows 11 includes WPA3 Personal with the new H2E protocol and WPA3 Enterprise 192-bit Suite B. Windows 11 also supports WPA3 Enterprise, which includes enhanced server certificate validation and TLS 1.3 for authentication using EAP-TLS authentication.

Opportunistic Wireless Encryption (OWE), a technology that allows wireless devices to establish encrypted connections to public Wi-Fi hotspots, is also included.

5G and eSIM

5G networks use stronger encryption and better network segmentation compared to previous generations of cellular protocols. Unlike Wi-Fi, 5G access is always mutually authenticated. Access credentials are stored in an EAL4-certified eSIM that is physically embedded in the device, making it much harder for attackers to tamper with. Together, 5G and eSIM provide a strong foundation for security.

Learn more: [eSIM configuration of a download server](#)

Windows Firewall

Windows Firewall with Advanced Security (previously called Windows Defender Firewall) is an important part of a layered security model. It provides host-based, two-way network traffic filtering, blocking unauthorized traffic flowing into or out of the local device based on the types of networks the device is connected to.

Windows Firewall in Windows 11 offers the following benefits:

- Reduces the risk of network security threats: Windows Firewall reduces the attack surface of a device with rules that restrict or allow traffic by many properties, such as IP addresses, ports, or program paths. This functionality increases manageability and decreases the likelihood of a successful attack.
- Safeguards sensitive data and intellectual property: By integrating with Internet Protocol Security (IPSec), Windows Firewall provides a simple way to enforce authenticated, end-to-end network communications. It provides scalable, tiered access to trusted network resources, helping to enforce integrity of the data, and optionally helping to protect the confidentiality of the data.
- Extends the value of existing investments: Because Windows Firewall is a host-based firewall that is included with the operating system, there is no additional hardware or software required. Windows Firewall is also designed to complement existing non-Microsoft network security solutions through a documented application programming interface (API).

Windows 11 makes the Windows Firewall easier to analyze and debug. IPSec behavior has been integrated with Packet Monitor (pktmon), an in-box, cross-component network diagnostic tool for Windows. Additionally, the Windows Firewall event logs have been enhanced to ensure an audit can identify the specific filter that was responsible for any given event. This enables analysis of firewall behavior and rich packet capture without relying on third-party tools.

Admins can now configure additional settings through the Firewall and Firewall Rule policy templates in the Endpoint Security node in Microsoft Intune⁹, leveraging the platform support from the [Firewall configuration service provider](#) (CSP) and applying these settings to Windows endpoints.

Learn more: [Windows Firewall with Advanced Security](#)

Virtual private networks (VPN)

Organizations have long relied on Windows to provide reliable, secured, and manageable virtual private network (VPN) solutions. The Windows VPN client platform includes built-in VPN protocols, configuration support, a common VPN user interface, and programming support for custom VPN protocols. VPN apps are available in the Microsoft Store for both enterprise and consumer VPNs, including apps for the most popular enterprise VPN gateways.

In Windows 11, we've integrated the most commonly used VPN controls right into the Windows 11 Quick Actions pane. From the Quick Actions pane, users can see the status of their VPN, start and stop the VPN tunnels, and with one click, go to the modern Settings app for more control.

The Windows VPN platform connects to Microsoft Entra ID⁹ and Conditional Access for single sign-on, including multifactor authentication (MFA) through Microsoft Entra ID. The VPN platform also supports classic domain-joined authentication. It's supported by Microsoft Intune and other modern device management (MDM) providers. The flexible VPN profile supports both built-in protocols and custom protocols. It can configure multiple authentication methods and can be automatically started as needed or manually started by the end user. It also supports split-tunnel VPN and exclusive VPN with exceptions for trusted external sites.

With Universal Windows Platform (UWP) VPN apps, end users never get stuck on an old version of their VPN client. VPN apps from the store will be automatically updated as needed. Naturally, the updates are in the control of your IT admins.

The Windows VPN platform has been tuned and hardened for cloud-based VPN providers like Azure VPN. Features like Microsoft Entra ID authentication, Windows user interface integration, plumbing IKE traffic selectors, and server support are all built into the Windows VPN platform. The integration into the Windows VPN platform leads to a simpler IT admin experience. User authentication is more consistent, and users can easily find and control their VPN.

Learn more: [Windows VPN technical guide](#)

Server Message Block file services

Server Message Block (SMB) and file services are the most common Windows workloads in the commercial and public sector ecosystem. Users and applications rely on SMB to access the files that run organizations of all sizes. In Windows 11, the SMB protocol has significant security updates to meet today's threats, including AES-256 encryption, accelerated SMB signing, Remote Direct Memory Access (RDMA) network encryption, and an entirely new scenario, SMB over QUIC for untrusted networks.

SMB encryption provides end-to-end encryption of SMB data and protects data from eavesdropping occurrences on internal networks. Windows 11 introduces AES-256-GCM and AES-256-CCM cryptographic suites for SMB 3.1.1 encryption. Windows administrators can mandate the use of this more advanced security or continue to use the more compatible and still-safe AES-128 encryption.

In Windows 11 Enterprise, Education, Pro, and Pro Workstation, SMB Direct now supports encryption. For demanding workloads like video rendering, data science, or extremely large files, you can now operate with the same safety as traditional Transmission Control Protocol (TCP) and the performance of RDMA. Previously, enabling SMB encryption disabled direct data placement, making RDMA as slow as TCP. Now, data is encrypted before placement, leading to relatively minor performance degradation while adding packet privacy with AES-128 and AES-256 protection.

Windows 11 also introduces AES-128-GMAC for SMB signing. Windows will automatically negotiate this better-performing cipher method when connecting to another computer that supports it. Signing prevents common attacks like relay and spoofing, and it is required by default when clients communicate with Active Directory domain controllers.

Finally, Windows 11 introduces SMB over QUIC, an alternative to the TCP network transport that provides secure, reliable connectivity to edge file servers over untrusted networks like the internet, as well as highly secure communications on internal networks. QUIC is an Internet Engineering Task Force (IETF)-standardized protocol with many benefits when compared with TCP, but most importantly, it always requires TLS 1.3 and encryption. SMB over QUIC offers an SMB VPN for telecommuters, mobile device users, and high-security organizations. All SMB traffic, including authentication and authorization within the tunnel, is never exposed to the underlying network. SMB behaves normally within the QUIC tunnel, meaning the user experience doesn't change. SMB over QUIC will be a game-changing feature for Windows 11 accessing Windows file servers and eventually Azure Files and third parties.

Newly installed Windows 11 Home editions that contain the February 2023 cumulative update no longer install the SMB 1.0 client by default, meaning the Home edition now operates like all other editions of Windows 11. SMB 1.0 is an unsafe and deprecated protocol that Microsoft superseded by later versions of SMB starting with Windows Vista. Microsoft began uninstalling SMB 1.0 by default in certain Windows 10 editions in 2017. No versions of Windows 11 now install SMB 1.0 by default.

Learn more: [File sharing using the SMB 3 protocol](#)

Virus and threat protection

Today's threat landscape is more complex than ever. This new world requires a new approach to threat prevention, detection, and response. Microsoft Defender Antivirus, along with many other features that are built into Windows 11, is at the frontlines, protecting customers against current and emerging threats.

Microsoft Defender SmartScreen

Microsoft Defender SmartScreen protects against phishing, malware websites and applications, and the downloading of potentially malicious files.

SmartScreen determines whether a site is potentially malicious by:

- Analyzing visited webpages to find indications of suspicious behavior. If it determines a page is suspicious, it will show a warning page advising caution.
- Checking the visited sites against a dynamic list of reported phishing sites and malicious software sites. If it finds a match, SmartScreen warns that the site might be malicious.

SmartScreen also determines whether a downloaded app or app installer is potentially malicious by:

- Checking downloaded files against a list of reported malicious software sites and programs known to be unsafe. If it finds a match, SmartScreen warns that the file might be malicious.
- Checking downloaded files against a list of well-known files. If the file is of a dangerous type and not well-known, SmartScreen displays a caution alert.

With enhanced phishing protection in Windows 11, SmartScreen also alerts people when they are entering their Microsoft credentials into a potentially risky location, regardless of which application or browser is used. IT can customize which notifications appear through Microsoft Intune⁹. This protection runs in audit mode by default, giving IT admins full control to make decisions around policy creation and enforcement.

Because Windows 11 comes with these enhancements already built in and enabled, users have extra security from the moment they turn on their device.

The app and browser control section contains information and settings for Microsoft Defender SmartScreen. IT administrators and IT pros can get configuration guidance in the [Microsoft Defender SmartScreen documentation library](#).

Microsoft Defender Antivirus

Microsoft Defender Antivirus is a next-generation protection solution included in all versions of Windows 10 and Windows 11. From the moment you turn on Windows, Microsoft Defender Antivirus continually monitors for malware, viruses, and security threats. In addition to real-time protection, updates are downloaded automatically to help keep your device safe and protect it from threats. If you have another antivirus app installed and turned on, Microsoft Defender Antivirus will turn off automatically. If you uninstall the other app, Microsoft Defender Antivirus will turn back on.

Microsoft Defender Antivirus includes real-time, behavior-based, and heuristic antivirus protection. This combination of always-on content scanning, file and process behavior monitoring, and other heuristics effectively prevents security threats. Microsoft Defender Antivirus continually scans for malware and threats and also detects and blocks potentially unwanted applications (PUA), applications deemed to negatively impact your device but are not considered malware.

Microsoft Defender Antivirus always-on protection is integrated with cloud-delivered protection, which helps ensure near-instant detection and blocking of new and emerging threats. This combination of local and cloud-delivered technologies provides award-winning protection at home and at work.



Learn more: [Next-generation protection with Microsoft Defender Antivirus](#)

Attack surface reduction

Attack surface reduction rules help prevent software behaviors that are often abused to compromise devices and networks. By reducing the attack surface, you can reduce the overall vulnerability of your organization. Administrators can configure specific attack surface reduction rules to help block certain behaviors, such as:

- Launching executable files and scripts that attempt to download or run files.
- Running obfuscated or otherwise suspicious scripts.
- Performing behaviors that apps don't usually initiate during normal day-to-day work.

For example, an attacker might try to run an unsigned script from a USB drive or have a macro in an Office document make calls directly to the Win32 API. Attack surface reduction rules can constrain these kinds of risky behaviors and improve the defensive posture of the device. For comprehensive protection, follow steps for enabling hardware-based isolation

for Microsoft Edge and reducing the attack surface across applications, folders, device, network, and firewall.

Learn more: [Attack surface reduction](#)

Tamper protection

Attacks like ransomware attempt to disable security features, such as anti-virus protection. Bad actors like to disable security features to get easier access to user's data, to install malware, or otherwise exploit user's data, identity, and devices without fear of being blocked. Tamper protection helps prevent these kinds of activities.

With tamper protection, malware is prevented from taking actions such as:

- Disabling real-time protection.
- Turning off behavior monitoring.
- Disabling antivirus (such as IOfficeAntivirus (IOAV)).
- Disabling cloud-delivered protection.
- Removing security intelligence updates.

Learn more: [Tamper protection](#)

Exploit protection

Exploit protection automatically applies several exploit mitigation techniques to operating system processes and apps. Exploit protection works best with Microsoft Defender for Endpoint⁹, which gives organizations detailed reporting into exploit protection events and blocks as part of typical alert investigation scenarios. You can enable exploit protection on an individual device and then use Group Policy in Active Directory or Microsoft Intune⁹ to distribute the configuration XML file to multiple devices simultaneously.

When a mitigation is encountered on the device, a notification will be displayed from the Action Center. You can customize the notification with your company details and contact information. You can also enable the rules individually to customize which techniques the feature monitors.

You can use audit mode to evaluate how exploit protection would impact your organization if it were enabled.

Windows 11 provides configuration options for exploit protection. You can prevent users from modifying these specific options with Group Policy.

Learn more: [Protecting devices from exploits](#)

Controlled folder access

You can protect your valuable information in specific folders by managing app access to them. Only trusted apps can access protected folders, which are specified when controlled folder access is configured. Typically, commonly used folders, such as those used for documents, pictures, and downloads, are included in the list of controlled folders.

Controlled folder access works with a list of trusted apps. Apps that are included in the list of trusted software work as expected. Apps that are not included in the trusted list are prevented from making any changes to files inside protected folders.

Controlled folder access helps protect user's valuable data from malicious apps and threats such as ransomware.

Learn more: [Controlled folder access](#)

Microsoft Defender for Endpoint

Microsoft Defender for Endpoint⁹ is an enterprise endpoint detection and response solution that helps security teams detect, investigate, and respond to advanced threats.

Organizations can use the rich event data and attack insights Defender for Endpoint provides to investigate incidents. Defender for Endpoint brings together the following elements to provide a more complete picture of security incidents:

- **Endpoint behavioral sensors:** Embedded in Windows, these sensors collect and process behavioral signals from the operating system and send this sensor data to your private, isolated cloud instance of Microsoft Defender for Endpoint.
- **Cloud security analytics:** Behavioral signals are translated into insights, detections, and recommended responses to advanced threats. These analytics leverage big data, device learning, and unique Microsoft optics across the Windows ecosystem, enterprise cloud products such as Microsoft 365⁹, and online assets.
- **Threat intelligence:** Microsoft processes over 43 trillion security signals every 24 hours, yielding a deep and broad view into the evolving threat landscape. Combined with our global team of security experts and cutting-edge artificial intelligence and machine learning, we can see threats that others miss. This threat intelligence helps provide unparalleled protection for our customers. The protections built into our platforms and products blocked attacks that include 31 billion identity threats and 32 billion email threats.

- Rich response capabilities: Defender for Endpoint empowers SecOps teams to isolate, remediate, and remote into machines to further investigate and stop active threats in their environment, as well as block files, network destinations, and create alerts for them. In addition, Automated Investigation and Remediation can help reduce the load on the SOC by automatically performing otherwise manual steps towards remediation and providing detailed investigation outcomes.

Defender for Endpoint is also part of Microsoft 365 Defender, our end-to-end, cloud-native extended detection and response (XDR) solution that combines best-of-breed endpoint, email, and identity security products. It enables organizations to prevent, detect, investigate, and remediate attacks by delivering deep visibility, granular context, and actionable insights generated from raw signals harnessed across the Microsoft 365 environment and other platforms, all synthesized into a single dashboard. This solution offers tremendous value to organizations of any size, especially those that are looking to break away from the added complexity of multiple point solutions, keeping them protected from sophisticated attacks and saving IT and security teams' time and resources.

Learn more: [Microsoft Defender for Endpoint](#)

Learn more: [Microsoft 365 Defender](#)



Application Security



Cybercriminals can take advantage of poorly secured applications to access valuable resources. With Windows 11, IT admins can combat common application attacks from the moment a device is provisioned. For example, IT can remove local admin rights from user accounts so that PCs run with the least amount of privileges to prevent malicious applications from accessing sensitive resources.

In addition, organizations can control which applications run on their devices with App Control for Business (previously called [Windows Defender Application Control](#)).

Application and driver control

Windows 11 offers a rich application platform with layers of security like isolation and code integrity that help protect your valuable data. Developers can also take advantage of these capabilities to build in security from the ground up to protect against breaches and malware.

Smart App Control

Smart App Control prevents users from running malicious applications on Windows devices by blocking untrusted or unsigned applications. Smart App Control goes beyond previous built-in browser protections by adding another layer of security that is woven directly into the core of the OS at the process level. Using AI, our new Smart App Control only allows processes to run if they are predicted to be safe based on existing and new intelligence updated daily.

Smart App Control builds on top of the same cloud-based AI used in App Control for Business to predict the safety of an application so that users can be confident that their applications are safe and reliable on their new Windows devices. Additionally, Smart App Control blocks unknown script files and macros from the web are blocked, greatly improving security for everyday users.

Smart App Control will ship with new devices with Windows 11, version 22H2 installed. Devices running previous versions of Windows 11 will have to be reset with a clean installation of Windows 11, version 22H2 to take advantage of this feature. Smart App Control will be disabled on devices enrolled in enterprise management. We suggest enterprises running line-of-business applications continue to leverage App Control for Business.

Learn more: [Smart App Control](#)

App Control for Business

Your organization is only as secure as the applications that run on your devices. With application control, apps must earn trust to run, in contrast to an application trust model where all code is assumed trustworthy. By helping prevent unwanted or malicious code from running, application control is an important part of an effective security strategy. Many organizations cite application control as one of the most effective means of defending against executable file-based malware.

Windows 10 and above include App Control for Business (previously called Windows Defender Application Control) as well as AppLocker. App Control for Business is the next-generation app control solution for Windows and provides powerful control over what runs in your environment. Customers who were using AppLocker on previous versions of Windows can continue to use the feature as they consider whether to switch to App Control for Business for stronger protection.

Customers using Microsoft Intune⁹ to manage their devices are now able to configure App Control for Business in the admin console, including setting up Intune as a managed installer.

Customers can use some built-in options for App Control for Business or upload their own policy as an XML file for Intune to package and deploy.

Learn more: [Application Control for Windows](#)

User Account Control

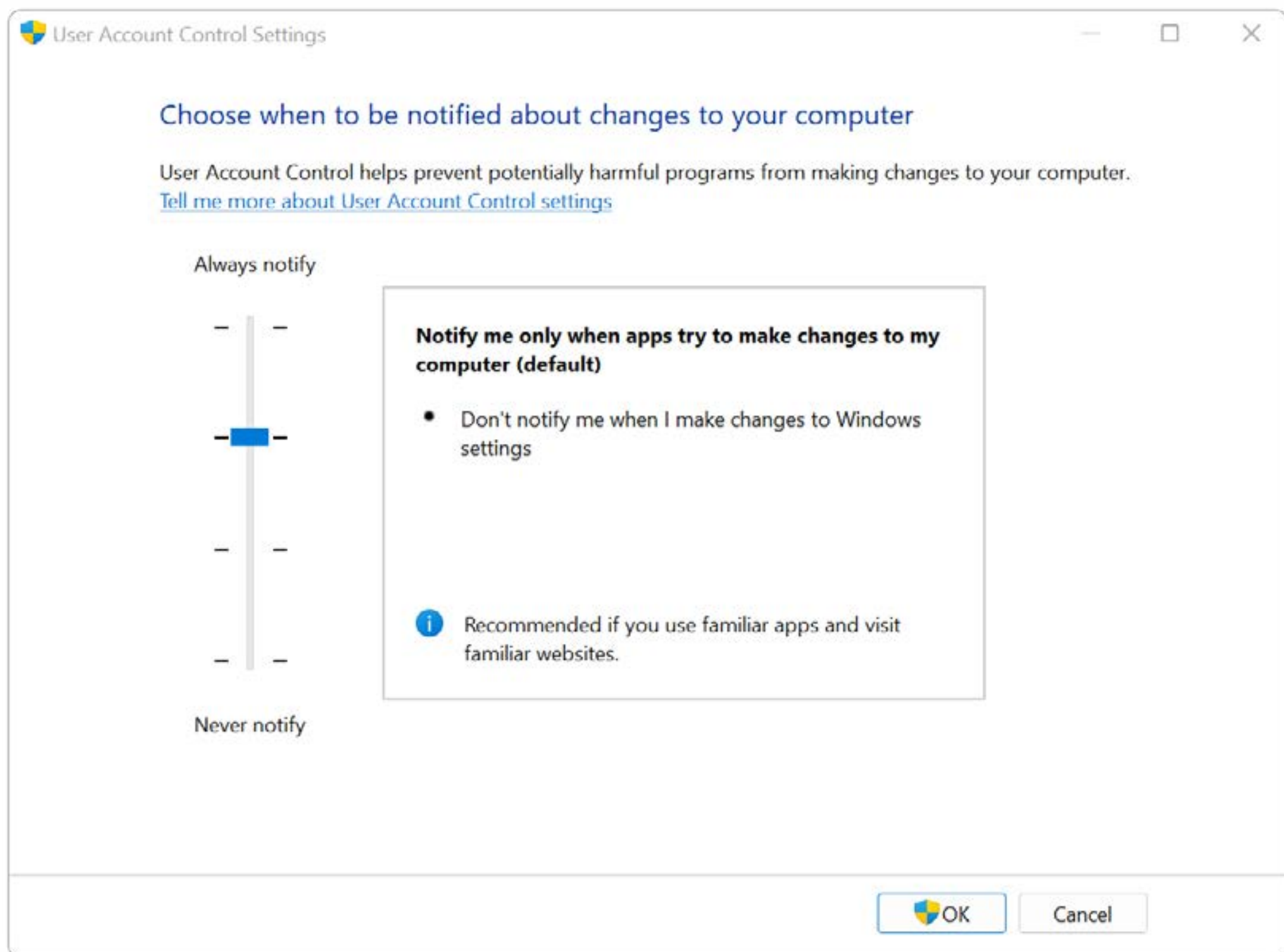
User Account Control (UAC) helps prevent malware from damaging a PC and enables organizations to deploy a better-managed desktop. With UAC, apps and tasks always run in the security context of a non-administrator account unless an administrator specifically authorizes administrator-level access to the system. UAC can block the automatic installation of unauthorized apps and prevent inadvertent changes to system settings.

Organizations can use a modern device management (MDM) solution like Microsoft Intune⁹ to remotely configure UAC settings. Organizations without MDM can change settings directly on the device.

Enabling UAC helps prevent malware from altering PC settings and potentially gaining access to networks and sensitive data. UAC can also block the automatic installation of unauthorized apps and prevent inadvertent changes to system settings.

Users with standard accounts, or those using administrative accounts with UAC enabled, run most programs with limited access rights. This includes the Windows shell and any apps started from the shell, such as Windows Explorer, a web browser, productivity suite, graphics programs, or games.

Some apps require additional permissions and will not work properly (or at all) when running with limited permissions. When an app needs to run with more than standard user rights, UAC allows users to run apps with a “full” administrator token (with administrative groups and privileges) instead of their default user access token. Users continue to operate in the standard user security context while enabling certain executables to run with elevated privileges if needed.



Learn more: [How User Account Control works](#)

Microsoft vulnerable driver blocklist

The Windows kernel is the most privileged software and is therefore a compelling target for malware authors. Since Windows has strict requirements for code running in the kernel, cybercriminals commonly exploit vulnerabilities in kernel drivers to get access. Microsoft works with ecosystem partners to constantly identify and respond to potentially vulnerable kernel drivers. Prior to the Windows 11 2022 Update, Windows enforced a block policy when hypervisor-protected code integrity (HVCI) was enabled to prevent vulnerable versions of drivers from running. Beginning with the Windows 11 2022 Update, the block policy is now on by default for all new Windows PCs, and users can opt in to enforce the policy from the Windows Security app.

Learn more: [Microsoft recommended driver block rules](#)

Application Isolation

Win32 app isolation

Win32 app isolation is a new security feature in public preview designed to be the default isolation standard on Windows clients. It is built on [AppContainer](#), and offers several added security features to help the Windows platform defend against attacks that leverage vulnerabilities in applications or third-party libraries. To isolate their apps, developers can update their applications using the tools provided by Microsoft.

Win32 app isolation follows a two-step process. In the first step, the Win32 application is launched as a low-integrity process using [AppContainer](#), which is recognized as a security boundary by Microsoft. Consequently, the process is limited to a specific set of Windows APIs by default and is unable to inject code into any process operating at a higher integrity level.

In the second step, least privilege is enforced by granting authorized access to Windows securable objects. This access is determined by capabilities that are added to the application manifest through MSIX packaging. Securable objects in this context refer to Windows resources whose access is safeguarded by capabilities. These capabilities enable the implantation of a [Discretionary Access Control List](#) on Windows.

To help ensure that isolated applications run smoothly, developers must define the access requirements for the application via access capability declarations in the application package manifest. The Application Capability Profiler (ACP) simplifies the entire process by allowing the application to run in “learn mode” with low privileges. Instead of denying access if the capability is not present, ACP allows access and logs additional capabilities required for access if the application were to run isolated. For more information on ACP, please refer to the [GitHub documentation page](#).

To create a smooth user experience that aligns with non-isolated, native Win32 applications, two key factors should be taken into consideration:

- Approaches for accessing data and privacy information
- Integrating Win32 apps for compatibility with other Windows interfaces

The first factor relates to implementing methods to manage access to files and privacy information within and outside the isolation boundary ([AppContainer](#)). The second factor involves integrating Win32 apps with other Windows interfaces in a way that helps enable seamless functionality without causing perplexing user consent prompts.

Learn more: [Win32 app isolation](#)

Windows Sandbox

Windows Sandbox provides a lightweight desktop environment to safely run untrusted Win32 applications in isolation using the same hardware-based Hyper-V virtualization technology without fear of lasting impact to the PC. Any untrusted Win32 app installed in Windows Sandbox stays only in the sandbox and cannot affect the host.

Once Windows Sandbox is closed, nothing persists on the device. All the software with all its files and state are permanently deleted after the untrusted Win32 application is closed.

Learn more: [Windows Sandbox](#)

Learn more: [Windows Sandbox is a new lightweight desktop environment tailored for safely running applications in isolation](#)

App containers

In addition to Windows Sandbox for Win32 apps, Universal Windows Platform (UWP) applications run in Windows containers known as app containers. App containers act as process and resource isolation boundaries, but unlike Docker containers, these are special containers designed to run Windows applications.

Processes that run in app containers operate at a low integrity level, meaning they have limited access to resources they do not own. Because the default integrity level of most resources is medium integrity level, the UWP app can access only a subset of the file system, registry, and other resources. The app container also enforces restrictions on network connectivity. For example, access to a local host is not allowed. As a result, malware or infected apps have limited footprint for escape.

Learn more: [Windows and app containers](#)



Identity

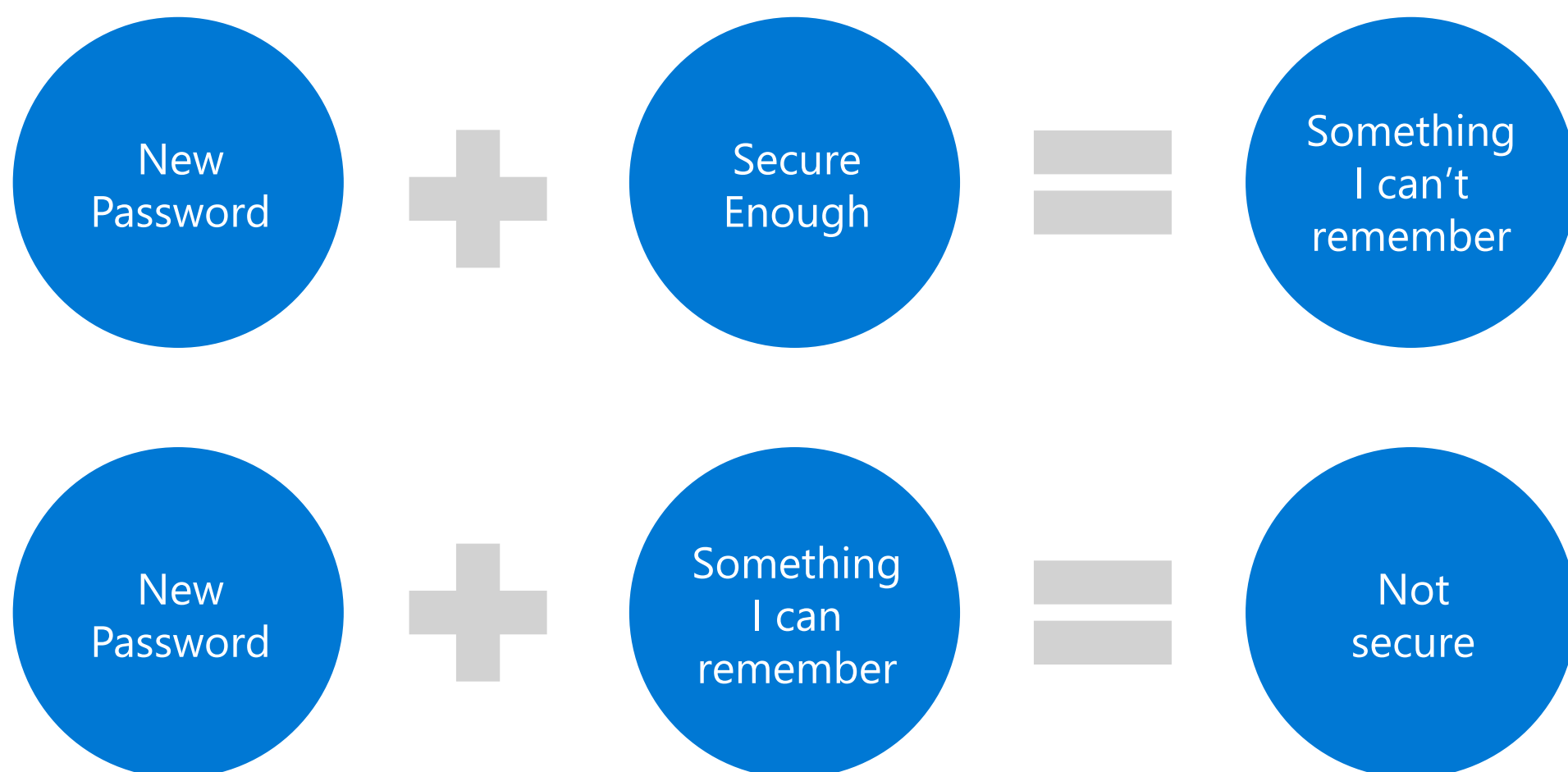


Today's flexible workstyles and the security of your organization depend on secure access to corporate resources, including strong identity protection. Weak or reused passwords, password spraying, social engineering, and phishing are some of the top attack vectors. In the last 12 months, we saw an average of more than 4,000 password attacks per second.¹¹ And phishing threats have increased, making identity a continuous battleground. As Bret Arsenault, Chief Information Security Officer at Microsoft says, "Hackers don't break in, they log in."

Because threats are constantly evolving and often difficult for employees to detect, organizations need proactive protection, including effortlessly secure authentication and features that defend users in real time while they work. Windows 11 is designed with powerful identity protection from chip to cloud, keeping identities and personal and business data safe anywhere people work.

Enabling passwordless sign-in

Passwords are inconvenient to use and prime targets for cybercriminals—and they've been an important part of digital security for years. That changes with the passwordless protection available with Windows 11. After a secure authorization process, credentials are protected behind layers of hardware and software security, giving users secure, passwordless access to their apps and cloud services.



Windows Hello

Too often, passwords are weak, stolen, or forgotten. Organizations are moving toward passwordless sign-in to reduce the risk of breaches, lower the cost of managing passwords, and improve productivity and satisfaction for their employees and customers. Microsoft is committed to helping customers move toward a secure, passwordless future with Windows Hello, a cornerstone of Windows security and identity protection.

[Windows Hello](#) can enable passwordless sign-in using biometric or PIN verification and provides built-in support for the FIDO2 passwordless industry standard. As a result, people no longer need to carry external hardware like a security key for authentication.

The secure, convenient sign-in experience can augment or replace passwords with a stronger authentication model based on a PIN or biometric data such as facial or fingerprint recognition secured by the Trusted Platform Module (TPM). Step-by-step guidance makes setup easy.

Using asymmetric keys provisioned in the TPM, Windows Hello protects authentication by binding a user's credentials to their device. Windows Hello validates the user based on either a PIN or biometrics match and only then allows the use of cryptographic keys bound to that user in the TPM.

PIN and biometric data stay on the device and cannot be stored or accessed externally. Since the data cannot be accessed by anyone without physical access to the device, credentials are protected against replay attacks, phishing, and spoofing as well as password reuse and leaks.

Windows Hello can authenticate users to a Microsoft account (MSA), identity provider services, or the relying parties that also implement the FIDO2 or WebAuthn standards.

Windows Hello for Business

Windows Hello for Business extends Windows Hello to work with an organization's Active Directory⁹ and Microsoft Entra ID⁹ accounts. It provides single sign-on access to work or school resources such as OneDrive for Business, work email, and other business apps. Windows Hello for Business also give IT admins the ability to manage PIN and other sign-in requirements for devices connecting to work or school resources.

Windows Hello for Business Passwordless

Windows 11 devices with Windows Hello for Business can protect user identities by removing the need to use passwords from day one.

IT can now set a policy for Microsoft Entra ID⁹ joined machines so users no longer see the option to enter a password when accessing company resources.¹² Once the policy is set, passwords are removed from the Windows user experience, both for device unlock as well as in-session authentication scenarios via CredUI. However, passwords are not eliminated from the identity directory yet. Users are expected to navigate through their core authentication scenarios using strong, phish-resistant, possession-based credentials like Windows Hello for Business and FIDO2 security keys. If necessary, users can leverage passwordless recovery mechanisms such as Windows Hello for Business PIN reset or Web Sign-in.

During a device's lifecycle, a password may only need to be used once during the provisioning process. After that, people can use a PIN, face, or fingerprint to unlock credentials and sign into the device.

Provisioning methods include:

- Temporary Access Pass (TAP), a time-limited passcode with strong authentication requirements issued through Microsoft Entra ID⁹.
- Existing multifactor authentication with Microsoft Entra ID⁹, including authentication methods like the Microsoft Authenticator app.

Windows Hello for Business replaces the username and password by combining a security key or certificate with a PIN or biometric data and then mapping the credentials to a user account during setup. There are multiple ways to deploy Windows Hello for Business depending on an organization's needs. Organizations that rely on certificates typically use on-premises public key infrastructure (PKI) to support authentication through Certificate Trust. Organizations using key trust deployment require root-of-trust provided by certificates on domain controllers.

Organizations with hybrid scenarios can eliminate the need for on-premises domain controllers and simplify passwordless adoption by using Windows Hello for Business cloud Kerberos trust.¹³ This solution uses security keys and replaces on-premises domain controllers with a cloud-based root-of-trust. As a result, organizations can take advantage of Windows Hello for Business and deploy passwordless security keys with minimal additional setup or infrastructure.

Users will authenticate directly with Microsoft Entra ID⁹, helping speed access to on- premises applications and other resources.

Learn more: [Windows Hello for Business overview](#)

Windows Hello PIN

The Windows Hello PIN, which can only be entered by someone with physical access to the device, can be used for strong multifactor authentication. The PIN is protected by the TPM and, like biometric data, never leaves the device. When a user enters their PIN, an authentication key is unlocked and used to sign a request sent to the authenticating server.

The TPM protects against threats including PIN brute-force attacks on lost or stolen devices. After too many incorrect guesses, the device locks. IT admins can set security policies for PINs, such as complexity, length, and expiration requirements.

Windows Hello biometric sign-in

Windows Hello biometric sign-in enhances both security and productivity with a quick, convenient sign-in experience. There's no need to enter a password every time when a face or fingerprint is the credential.

Windows devices that support biometric hardware such as fingerprint or facial recognition cameras integrate directly with Windows Hello, enabling access to Windows client resources and services. Biometric readers for both face and fingerprint must comply with [Microsoft Windows Hello biometric requirements](#). Windows Hello facial recognition is designed to only authenticate from trusted cameras used at the time of enrollment.

If a peripheral camera is attached to the device after enrollment, that camera will only be allowed for facial authentication after it has been validated by signing in with the internal camera. For additional security, external cameras can be disabled for use with Windows Hello facial recognition.

Windows Hello Enhanced Sign-in Security

Windows Hello biometrics also supports Enhanced Sign-in Security, which uses specialized hardware and software components to raise the security bar even higher for biometric sign-in.

Enhanced Sign-in Security biometrics uses virtualization-based security (VBS) and the TPM to isolate user authentication processes and data and secure the pathway by which the information is communicated.

These specialized components protect against a class of attacks that includes biometric sample injection, replay, and tampering. For example, fingerprint readers must implement Secure Device Connection Protocol, which uses key negotiation and a Microsoft-issued certificate to protect and securely store user authentication data. For facial recognition, components such as the Secure Devices (SDEV) table and process isolation with trustlets help prevent additional attack classes.

Enhanced Sign-in Security is configured by device manufacturers during the manufacturing process and is most typically supported in Secured-core PCs. For facial recognition, Enhanced Sign-in Security is supported by specific silicon and camera combinations—please check with the specific device manufacturer. Fingerprint authentication is available across all processor types. Please reach out to specific OEMs for support details.

Learn more: [Windows Hello Enhanced Sign-in Security](#)

Windows Hello for Business multi-factor unlock

For organizations that need an extra layer of sign-in security, multi-factor unlock enables IT admins to configure Windows by requiring a combination of two unique trusted signals to sign in. Trusted signal examples include a PIN or biometric data (face or fingerprint) combined with either a PIN, Bluetooth, IP configuration, or Wi-Fi.

Multi-factor unlock is useful for organizations who need to prevent information workers from sharing credentials or need to comply with regulatory requirements for a two-factor authentication policy.

Learn more: [Multi-factor unlock](#)

Windows presence sensing

Windows presence sensing¹⁴ provides another layer of data security protection for hybrid workers. Windows 11 devices can intelligently adapt to a user's presence to help them stay secure and productive, whether they're working at home, the office, or a public environment.

Windows presence sensing combines presence detection sensors with Windows Hello facial recognition to sign the user in hands-free and automatically locks the device when the user leaves. With adaptive dimming, the PC dims the screen when the user looks away on compatible devices with presence sensors. It's also easier than ever to configure presence sensors on devices, with easy enablement in the out-of-the-box experience and new links in Settings to help find presence sensing features. Device manufacturers will be able to customize and build extensions for the presence sensor.

Developer APIs and app privacy support for presence sensing

Privacy is top of mind and more important than ever. Customers want to have greater transparency and control over the use of their information. We are pleased to announce new app privacy settings that enable users to allow or block access to their presence sensor information. Users can decide on these settings during the initial Windows 11 setup.

Users can also take advantage of more granular settings to easily enable and disable differentiated presence sensing features like wake on approach, lock on leave, and adaptive dimming. We are also supporting developers with new APIs for presence sensing for third-party applications. Third-party applications can now access user presence information on devices with modern presence sensors.

Learn more: [Presence sensing](#)

Learn more: [Managing presence sensing settings in Windows 11](#)

FIDO support

The FIDO Alliance, the Fast Identity Online industry standards body, was established to promote authentication technologies and standards that reduce reliance on passwords. FIDO Alliance and World Wide Web Consortium (W3C) have worked together to define the Client to Authenticator Protocol (CTAP2) and Web Authentication (WebAuthn) specifications, which are the industry standard for providing strong, phishing-resistant, user friendly, and privacy preserving authentication across the web and apps. FIDO standards and certifications are becoming recognized as the leading standard for creating secure authentication solutions across enterprises, governments, and consumer markets.

Windows 11 can also use passkeys from external FIDO2 security keys for authentication alongside or in addition to Windows Hello and Windows Hello for Business, which is also a FIDO2-certified passwordless solution. As a result, Windows 11 can be used as a FIDO authenticator for many popular identity management services.

Learn more: [Passwordless security key sign-in](#)

Passkeys

Windows 11 makes it much harder for hackers who exploit stolen passwords via phishing attacks by empowering users to replace passwords with passkeys. Passkeys are the cross-platform future of secure sign-in. Microsoft and other technology leaders are supporting passkeys across their platforms and services.

A passkey is a unique, unguessable cryptographic secret that is securely stored on the device. Instead of using a username and password to sign in to a website or application, Windows

11 users will be able to create and use a passkey from Windows Hello, an external security provider, or their mobile device.

Passkeys on Windows 11 will be protected by Windows Hello or Windows Hello for Business. This enables users to sign in to the site or app using their face, fingerprint, or device PIN. Passkeys on Windows work in any browser or app that supports them for sign in. Users will be able to manage passkeys on their device on Windows 11 account settings.

Learn more: [Passkeys \(passkey authentication\)](#)

Microsoft Authenticator

The Microsoft Authenticator app, which runs on iOS and Android devices, helps keep Windows 11 users secure and productive. Microsoft Authenticator can be used to bootstrap Windows Hello for Business, which removes the need for a password to get started on Windows 11.

Microsoft Authenticator also enables easy, secure sign-in for all online accounts using multifactor authentication, passwordless phone sign-in, or password autofill. The accounts in the Authenticator app are secured with a public/private key pair in hardware-backed storage such as the Keychain in iOS and Keystore on Android. IT admins can leverage different tools to nudge their users to setup the Authenticator app, provide them with extra context about where the authentication is coming from, and ensure that they are actively using it.

Individual users can back up their credentials to the cloud by enabling the encrypted backup option in settings. They can also see their sign-in history and security settings for Microsoft personal, work, or school accounts.

Using this secure app for authentication and authorization enables people to be in control of how, where, and when their credentials are used. To keep up with an ever-changing security landscape, the app is constantly updated, and new capabilities are added to stay ahead of emerging threat vectors.

Learn more: [Microsoft Authenticator](#)

Smart cards for Windows service

Organizations also have the option of using smart cards, an authentication method that predates biometric authentication. Smart cards are tamper-resistant, portable storage devices that can enhance Windows security when authenticating users, signing code, securing e-mail, and signing in with Windows domain accounts.

Smart cards provide:

- Ease of use in scenarios such as healthcare where employees need to sign in and out quickly without using their hands or when sharing a workstation.

- Isolation of security-critical computations that involve authentication, digital signatures, and key exchange from other parts of the computer. These computations are performed on the smart card.
- Portability of credentials and other private information between computers at work, home, or on the road

Smart cards can only be used to sign in to domain accounts or Microsoft Entra ID accounts. When a password is used to sign in to a domain account, Windows uses the Kerberos Version 5 (V5) protocol for authentication. If you use a smart card, the operating system uses Kerberos V5 authentication with X.509 V3 certificates. On Microsoft Entra ID joined devices, a smart card can be used with Entra ID certificate-based authentication. Smart cards cannot be used with local accounts.

Learn more: [Smart Card technical reference](#)

Federated sign-in

Windows 11 supports federated sign-in with external education identity management services. For students unable to type easily or remember complex passwords, this capability enables secure sign-in through methods like QR codes or pictures. Additionally, we have added shared device support. It allows multiple students (one at a time) to use the device throughout the school day.

Learn more: [Configure federated sign-in for Windows devices](#)

Advanced credential protection

In addition to adopting passwordless sign-in, organizations can strengthen security for user and domain credentials in Windows 11 with Credential Guard and Remote Credential Guard.

Enhanced phishing protection with Microsoft Defender SmartScreen

As malware protection and other safeguards evolve, cybercriminals look for new ways to circumvent security measures. Phishing has emerged as a leading threat, with apps and websites designed to steal credentials by tricking people into voluntarily entering passwords. As a result, many organizations are transitioning to the ease and security of passwordless sign-in with Windows Hello or Windows Hello for Business.

However, people who are still using passwords can also benefit from powerful credential protection in Windows 11. Microsoft Defender SmartScreen now includes enhanced phishing protection to automatically detect when a user's Microsoft password is entered into any app or website. Windows then identifies if the app or site is securely authenticating to Microsoft and warns if the credentials are at risk. Because the user is alerted at the moment of potential credential theft, they can take preemptive action before the password is used against them or their organization.

Learn more: [Enhanced phishing protection in Microsoft Defender SmartScreen](#)

Local Security Authority (LSA) protection

Windows has several critical processes to verify a user's identity. Verification processes include Local Security Authority (LSA), which is responsible for authenticating users and verifying Windows sign-ins. LSA handles tokens and credentials that are used for single sign-on to a Microsoft account and Azure services.⁹

To help keep these credentials safe, additional LSA protection will be enabled by default on new, enterprise-joined Windows 11 devices. By loading only trusted, signed code, LSA provides significant protection against credential theft. LSA protection also now supports configuration using Group Policy and modern device management.

Learn more: [Configuring additional LSA protection](#)

Credential Guard

Enabled by default in Windows 11 Enterprise, Credential Guard uses hardware-backed, virtualization-based security (VBS) to protect against credential theft. With Credential Guard, the Local Security Authority (LSA) stores and protects Active Directory (AD) secrets in an isolated environment that is not accessible to the rest of the operating system. LSA uses remote procedure calls to communicate with the isolated LSA process.

By protecting the LSA process with virtualization-based security, Credential Guard shields systems from credential theft attack techniques like Pass-the-Hash or Pass-the-Ticket. It also helps prevent malware from accessing system secrets even if the process is running with admin privileges.

Learn more: [Protect derived domain credentials with Credential Guard](#)

Remote Credential Guard

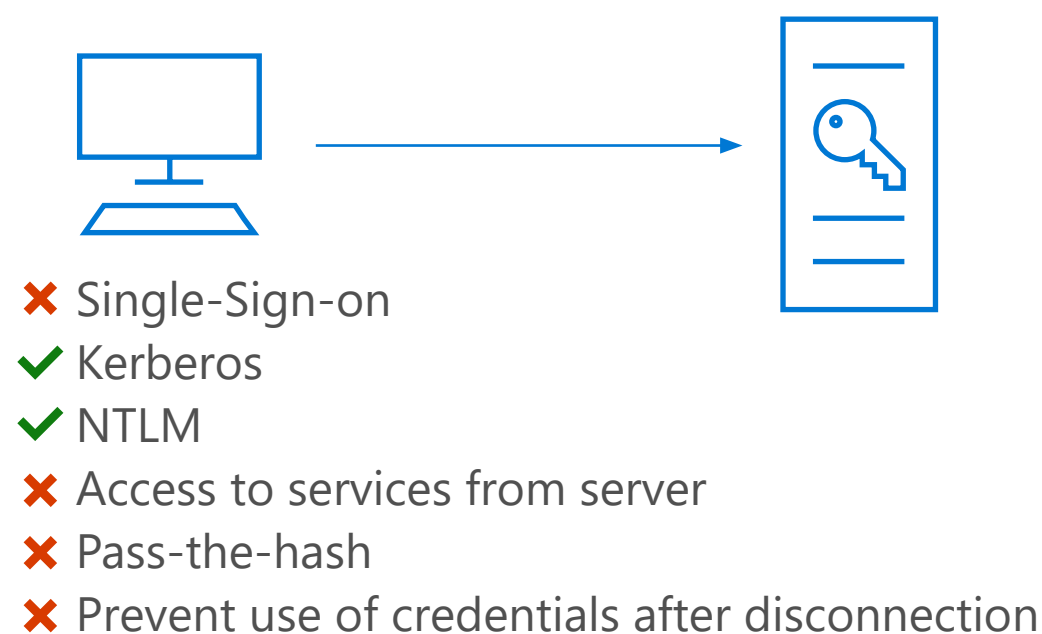
Remote Credential Guard helps organizations protect credentials over a Remote Desktop connection by redirecting the Kerberos requests back to the device that is requesting the connection. It also provides single sign-on experiences for Remote Desktop sessions.

Administrator credentials are highly privileged and must be protected. When Remote Credential Guard is configured and enabled to connect during Remote Desktop sessions, the credential and credential derivatives are never passed over the network to the target device. If the target device is compromised, the credentials are not exposed.

Learn more: [Remote Credential Guard - Windows Security | Microsoft Learn](#)

The following diagram shows how a standard Remote Desktop session to a server without Remote Credential Guard works:

Remote Desktop connection to a server without Remote Credential Guard

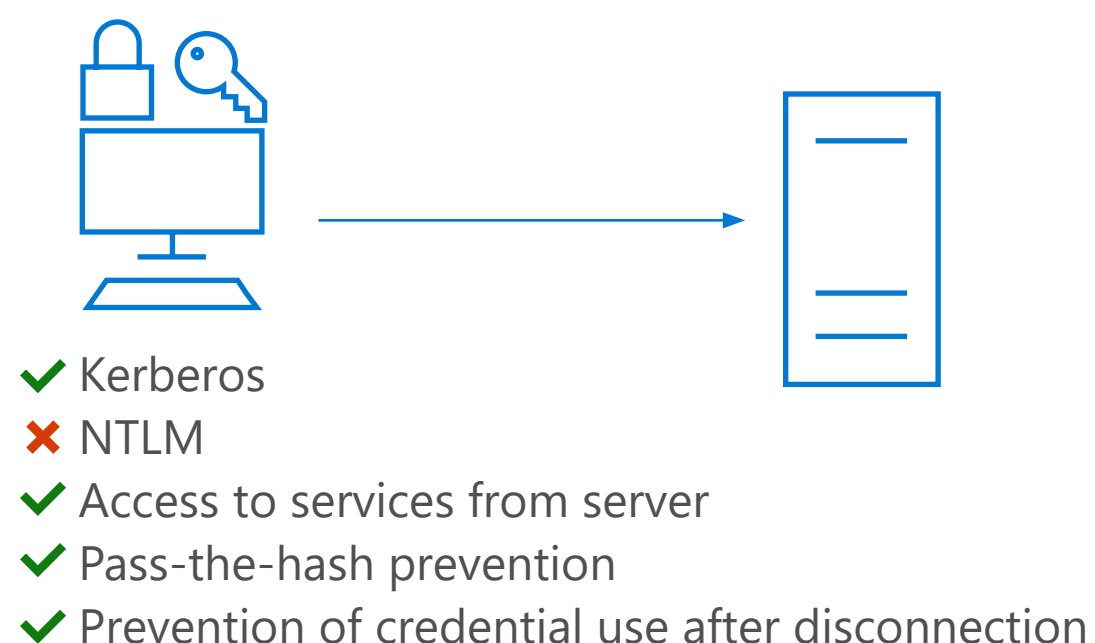


- Credentials are sent to the server.
- Credentials are not protected from attackers on the remote host.
- Attacker can continue to use credentials after disconnection.

 = Credentials

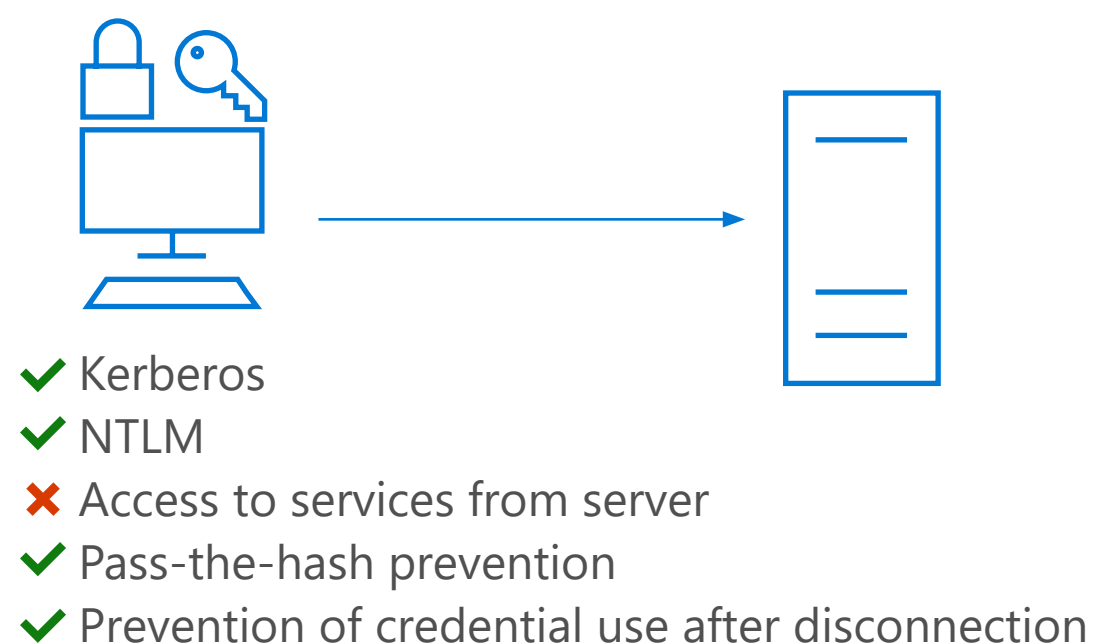
The following diagrams help demonstrate how Windows Defender Remote Credential Guard works, what it helps to protect against, and compares it with the [Restricted Admin mode option](#):

Remote Desktop connection to a server with Windows Defender Remote Credential Guard



- Credentials are protected by Remote Credential Guard.
- Connect to other systems using single sign-on.
- Host must support Remote Credential Guard.

Restricted admin mode



- Credentials used are remote server local admin credentials.
- Connect to other systems using the host's identity.
- Host must support Restricted Admin mode
- Highest protection level provided.
- User account administrator rights are required.

 = Credential protection
 = Credentials

As illustrated, Windows Defender Remote Credential Guard blocks NTLM (allowing only Kerberos), and helping to prevent Pass-the-hash attacks and malicious use of credentials after disconnection.

Token protection

Token protection attempts to reduce attacks using Microsoft Entra ID⁹ token theft. Token protection makes tokens usable only from their intended device by cryptographically binding a token with a device secret. When using the token, both the token and proof of the device secret must be provided. Conditional Access policy can be configured to require token protection when using sign-in tokens for specific services.

Learn more: [Token protection in Entra ID Conditional Access](#)

Sign-in session token protection policy

At the inaugural Microsoft Secure event in March 2023, we announced the public preview of token protection for sign-ins. This feature allows applications and services to cryptographically bind security tokens to the device, restricting attackers' ability to impersonate users on a different device if tokens are stolen.

Learn more: [Conditional Access: Token protection \(preview\)](#)

Account lockout policies

New devices with Windows 11 installed will have account lockout policies that are secure by default. These policies will mitigate brute-force attacks such as hackers attempting to access Windows devices via the Remote Desktop Protocol (RDP).

The account lockout threshold policy is now set to 10 failed sign-in attempts by default, with the account lockout duration set to 10 minutes. The Allow Administrator account lockout is now enabled by default. The Reset account lockout counter after is now set to 10 minutes by default as well.

Learn more: [Account lockout policy](#)

Access management and control

Access control in Windows ensures that shared resources are available to users and groups other than the resource's owner and are protected from unauthorized use. IT administrators can manage users', groups', and computers' access to objects and assets on a network or computer. After a user is authenticated, the Windows operating system implements the second phase of protecting resources by using built-in authorization and access control technologies to determine if an authenticated user has the correct permissions.

Access Control Lists (ACLs) describe the permissions for a specific object and can also contain System Access Control Lists (SACLs). SACLs provide a way to audit specific system level events, such as when a user attempts to access file system objects. These events are essential for tracking activity for objects that are sensitive or valuable and require extra monitoring. Being able to audit when a resource attempts to read or write part of the operating system is critical to understanding a potential attack.

IT administrators can refine the application and management of access to:

- Protect a greater number and variety of network resources from misuse.
- Provision users to access resources in a manner that is consistent with organizational policies and the requirements of their jobs. Organizations can implement the principle of least-privilege access, which asserts that users should be granted access only to the data and operations they require to perform their jobs.
- Update users' ability to access resources on a regular basis as an organization's policies change or as users' jobs change.
- Support evolving workplace needs, including access from hybrid or remote locations, or from a rapidly expanding array of devices, including tablets and mobile phones.
- Identify and resolve access issues when legitimate users are unable to access resources that they need to perform their jobs.

Learn more: [Access control](#)



Privacy

Privacy controls



[Privacy: Your data, powering your experiences, controlled by you.](#) Privacy is becoming top of mind for customers, who want to know who is using their data and why. They also need to know how to control and manage the data that is being collected—so providing transparency and control over this personal data is essential. At Microsoft we are focused on protecting the privacy and confidentiality of your data and will only use it in a way that is consistent with your expectations.

Privacy dashboard and report

Customers can use the [Microsoft Privacy dashboard](#) to view, export, and delete their information, giving them further transparency and control. They can also use the [Microsoft Privacy Report](#) to learn more about Windows data collection and how to manage it. For enterprises we provide a guide for Windows Privacy Compliance that includes additional details on the available controls and transparency.

Privacy transparency and controls

Prominent system tray icons show users when resources and apps like microphones and location are in use. A description of the app and its activity are presented in a simple tooltip that appears when you hover over an icon with your cursor. Apps can also make use of new Windows APIs to support Quick Mute functionality and more.

Privacy resource usage

Every Microsoft customer should be able to use our products secure in the knowledge that we will protect their privacy and give them the information and tools they need to easily make privacy decisions with confidence. Accessed in Settings, the new app usage history feature gives users a seven-day history of resource access for Location, Camera, Microphone, Phone Calls, Messaging, Contacts, Pictures, Videos, Music library, Screenshots, and other apps.

This information helps you determine if an app is behaving as expected so that you can change the app's access to resources as desired.

Windows diagnostic data processor configuration

The Windows diagnostic data processor configuration enables the user to be the controller, as defined by the European Union General Data Protection Regulation (GDPR), for the Windows diagnostic data collected from Windows devices that meet the configuration requirements.

Learn more: [Windows diagnostic data processor configuration](#)



Cloud Services



Today's workforce has more freedom and mobility than ever before, but the risk of data exposure is also at its highest. At Microsoft, we are focused on getting customers to the cloud to benefit from modern hybrid workstyles while improving security management. Built on Zero Trust principles, Windows 11 works with Microsoft cloud services to safeguard sensitive information while controlling access and mitigating threats.

From identity and device management to Office apps and data storage, Windows 11 and integrated cloud services can help improve productivity, security, and resilience anywhere.

Protecting your work information

Microsoft Entra ID

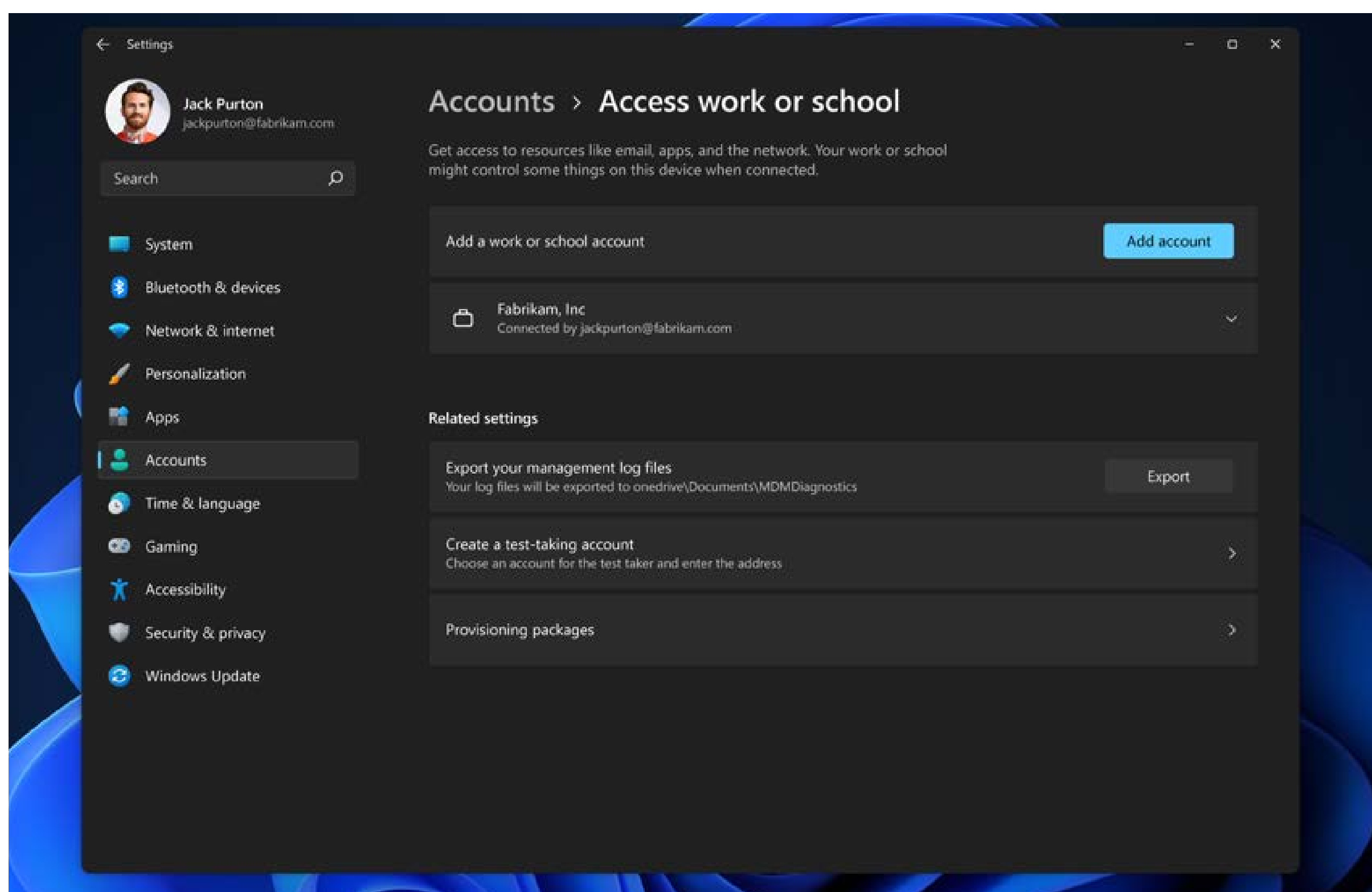
[Microsoft Entra ID⁹ \(formerly Azure Active Directory\)](#) is a comprehensive cloud-based identity management solution that helps enable secure access to applications, networks, and other resources and guard against threats. Microsoft Entra ID can also be used with Windows Autopilot for zero-touch provisioning of devices preconfigured with corporate security policies.

Organizations can deploy Microsoft Entra ID joined devices to enable access to both cloud and on-premises apps and resources. Access to resources can be controlled based on the Microsoft Entra ID account and Conditional Access policies applied to the device. By registering devices with Microsoft Entra ID—also called Workplace joined—IT admins can

support users in bring your own device (BYOD) or mobile device scenarios. Credentials are authenticated and bound to the joined device and cannot be copied to another device without explicit reverification.

To provide more security and control for IT and a seamless experience for end users, Microsoft Entra ID works with apps and services, including on-premises software and thousands of software-as-a-service (SaaS) applications. Microsoft Entra ID protections include single sign-on, multifactor authentication, conditional access policies, identity protection, identity governance, and privileged identity management.

Windows 11 works with Microsoft Entra ID to provide secure access, identity management, and single sign-on to apps and services from anywhere. Windows has built-in settings to add work or school accounts by syncing the device configuration to an Active Directory domain or Microsoft Entra ID tenant.



When a device is Microsoft Entra ID joined and managed with Microsoft Intune⁹, it receives the following security benefits:

- Default managed user and device settings and policies
- Single sign-in to all Microsoft Online Services
- Full suite of authentication management capabilities using Windows Hello for Business
- Single sign-on (SSO) to enterprise and SaaS applications
- No use of consumer Microsoft Account identity

Organizations and users can join or register their Windows devices with Microsoft Entra ID to get a seamless experience to both native and web applications. In addition, users can setup Windows Hello for Business or FIDO2 security keys with Microsoft Entra ID and benefit from greater security with passwordless authentication.

In combination with Microsoft Intune, Microsoft Entra ID offers powerful security control through Conditional Access to restrict access to organizational resources to healthy and compliant devices. Note that Microsoft Entra ID is only supported on Windows Pro and Enterprise editions.

Every Windows device has a built-in local administrator account that must be secured and protected to mitigate any Pass-the-Hash (PtH) and lateral traversal attacks. Many customers have been using our standalone, on-premises Windows Local Administrator Password Solution (LAPS) to manage their domain-joined Windows machines. We heard from many customers that LAPS support was needed as they modernized their Windows environment to join directly to Microsoft Entra ID.

Windows LAPS is available in public preview to Microsoft Entra ID joined and hybrid Microsoft Entra ID joined devices. Additionally, Windows LAPS is now built in to Windows with Windows 10 20H2 and later, Windows 11 21H2 and later, and Windows Server 2019 and later using the most recent security update (released on April 11, 2023).

Learn more: [Windows Local Administrator Password Solution with Microsoft Entra \(Azure AD\)](#)

Learn more: [Microsoft Entra plans and pricing](#)

Modern device management through (MDM)

Windows 11 supports modern device management through mobile device management (MDM) protocols so that IT professionals can manage company security policies and business applications without compromising user privacy on corporate or employee-owned devices. With MDM solutions like Microsoft Intune⁹, IT can manage Windows 11 using industry-standard protocols. To simplify setup for users, management features are built directly into Windows, eliminating the need for a separate MDM client.

Windows 11 built-in management features include:

- The enrollment client, which enrolls and configures the device to securely communicate with the enterprise device management server.
- The management client, which periodically synchronizes with the management server to check for updates and apply the latest policies set by IT.

Learn more: [Mobile device management overview](#)

Microsoft security baselines

Every organization faces security threats. However, different organizations can be concerned with different types of security threats. For example, an e-commerce company may focus on protecting its internet-facing web apps, while a hospital may focus on protecting confidential patient information. The one thing that all organizations have in common is a need to keep their apps and devices secure. These devices must be compliant with the security standards (or security baselines) defined by the organization.

Microsoft Security baseline

A security baseline is a group of Microsoft-recommended configuration settings that explains their security implications. These settings are based on feedback from Microsoft security engineering teams, product groups, partners, and customers.

Learn more: [Windows security baselines you can deploy with Microsoft Intune](#)

MDM security baseline

Windows 11 can be configured with Microsoft's MDM security baseline backed by ADMX policies, which functions like the Microsoft GP-based security baseline. The security baseline enables IT administrators to easily address security concerns and compliance needs for modern cloud-managed devices.

The security baseline includes policies for:

- Microsoft inbox security technology such as BitLocker, Microsoft Defender SmartScreen, virtualization-based security, Exploit Guard, Microsoft Defender Antivirus, and Windows Firewall.
- Restricting remote access to devices.
- Setting credential requirements for passwords and PINs.
- Restricting use of legacy technology.

Learn more: [MDM security baseline](#)

Microsoft Intune

Microsoft Intune¹⁵ is a comprehensive endpoint management solution that helps secure, deploy, and manage users, apps, and devices. Intune brings together technologies like Microsoft Configuration Manager and Windows Autopilot to simplify provisioning, configuration management, and software updates across the organization.

Intune works with Microsoft Entra ID to manage security features and processes, including multifactor authentication.

Organizations can cut costs while securing and managing remote PCs through the cloud in compliance with company policies.¹⁶ For example, organizations save time and money by provisioning preconfigured devices to remote employees using Windows Autopilot for zero-touch deployment.

Windows 11 enables IT professionals to move to the cloud while consistently enforcing security policies. Windows 11 provides expanded support for Group Policy administrative templates (ADMX-backed policies) in MDM solutions like Microsoft Intune, enabling IT professionals to easily apply the same security policies to both on-premises and remote devices.

Endpoint Privilege Management (EPM): Intune Endpoint Privilege Management supports organizations' Zero Trust journeys by helping them achieve a broad user base running with least privilege, while still permitting users to run tasks allowed by the organization to remain productive.

Local Administrator Password (LAPs): Local Administrator Password solution was a key consideration for many customers when deciding to make the transition from on-premises to cloud-managed devices using Intune. With LAPS (available in preview), organizations can automatically manage and back up the password of a local administrator account on Microsoft Entra ID joined or hybrid Microsoft Entra ID joined devices.

Mobile Application Management (MAM): With Intune, organizations can also extend MAM App Config, MAM App Protection, and App Protection Conditional Access capabilities to Windows. This enables people to access protected organizational content without having the device managed by IT. The first application to support MAM for Windows is Microsoft Edge.

Customers have asked for App Control for Business (previously called Windows Defender Application Control) to manage Installer support for a long time. Now customers will be able to enable allowlisting of Win32 apps within their enterprise to proactively reduce the number of malware infections.

Finally, Config Refresh helps organizations move to cloud from on-premises by protecting against settings deviating from the admin's intent.

Learn more: [Windows LAPS overview](#)

Microsoft Intune also has policies and settings to configure and manage the flow of operating system updates to devices, working with WUfB and WUfB-DS and giving admins great control over their deployments

With Intune, organizations can also extend MAM App Config, MAM App Protection, and App Protection Conditional Access capabilities to Windows. This enables people to access protected organizational content without having the device managed by IT. The first application to support MAM for Windows is Microsoft Edge.

Learn more: [What is Microsoft Intune](#)

Remote Wipe

When a device is lost or stolen, IT administrators might want to remotely wipe data stored in memory and hard disks. A helpdesk agent might also want to reset devices to fix issues encountered by remote workers. A remote wipe can also be used to prepare a previously used device for a new user.

Windows 11 supports the Remote Wipe configuration service provider (CSP) so that MDM Solutions⁹ can remotely initiate any of the following operations:

- Reset the device and remove user accounts and data.
- Reset the device and clean the drive.
- Reset the device but persist user accounts and data.

Learn More: [Remote Wipe CSP](#)

Microsoft Azure Attestation Service

Remote attestation helps ensure that devices are compliant with security policies and are operating in a trusted state before they are allowed to access resources. Microsoft Intune⁹ integrates with [Microsoft Azure Attestation Service](#) to review Windows device health comprehensively and connect this information with Microsoft Entra ID⁹ Conditional Access.

Attestation policies are configured in the Microsoft Azure Attestation Service which can then:

- Verify the integrity of evidence provided by the Windows Attestation component by validating the signature and ensuring the Platform Configuration Registers (PCRs) match the values recomputed by replaying the measured boot log.
- Verify that the TPM has a valid Attestation Identity Key issued by the authenticated TPM.
- Verify that security features are in the expected states.

Once this verification is complete, the attestation service returns a signed report with the security features state to the relying party—such as Microsoft Intune—to assess

the trustworthiness of the platform relative to the admin-configured device compliance specifications. Conditional access is then granted or denied based on the device's compliance.

Learn more: [Azure Attestation overview](#)

Windows Update for Business deployment service

The Windows Update for Business deployment service, a core component of the Windows Update for Business product family, is a cloud-based solution that transforms the way update management is handled. Complementing existing [Windows Update for Business](#) policies and [Windows Update for Business reports](#), the service provides control over the approval, scheduling, and safeguarding of updates—delivered straight from Windows Update to managed devices.

The Windows Update for Business deployment service powers Windows Update management via Microsoft Intune⁹ and Autopatch. The deployment services currently allows the management of [drivers and firmware](#), expedited [quality updates](#) and [feature updates](#).

For an in-depth understanding of this service, including its benefits and prerequisites for use, practical guides on specific capabilities, Microsoft Graph training, and a behind-the-scenes look at how the deployment service functions, read [here](#).

Learn more: [Windows Update for Business - Windows Deployment](#)

Windows Autopatch

Cybercriminals often target outdated or unpatched software to gain access to networks. Keeping endpoints up to date is critical in closing existing vulnerabilities, but planning, monitoring, and reporting on update compliance can take IT resources away from other important tasks.

Available as part of Windows Enterprise E3 and E5, Windows Autopatch automates update management for Windows, drivers, firmware, Microsoft 365, Edge, and Teams apps. The service can even manage the upgrade to Windows 11. While the service is designed to be simple by default, admins can customize the service to reflect their business organization with Autopatch groups. This allows custom content or deployment schedules to be applied to different populations of devices.

From a technical standpoint, Windows Autopatch configures the policies and deployment service of Windows Update for Business to deliver updates, all within Microsoft Intune.⁹ The results for IT admins: up-to-date endpoints and detailed reports to demonstrate compliance or help identify issues. The goal is to help IT teams be more secure and update more efficiently with less effort.

There's a lot more to learn about Windows Autopatch: this [Forrester study commissioned by Microsoft](#) analyzes the impact of Windows Autopatch on real customers, [regular IT pro blogs](#) provide updates and background on Autopatch features and the future of the service, and

the [community](#) allows IT professionals to get answers to questions from their peers and the Autopatch team.

Learn more: [Windows Autopatch documentation](#)

Windows Autopilot and zero-touch deployment

Traditionally, IT professionals spend significant time building and customizing images that will later be deployed to devices. Windows Autopilot introduces a new approach with a collection of technologies used to set up and preconfigure new devices, getting them ready for productive use and ensuring they are delivered locked down and compliant with corporate security policies.

- From a user perspective, it only takes a few simple operations to get their device ready for use.
- From an IT professional perspective, the only interaction required from the end user is to connect to a network and verify their credentials. Setup is automated after that point.

Windows Autopilot enables you to:

- Automatically join devices to Microsoft Entra ID⁹ or Active Directory⁹ via hybrid Microsoft Entra ID Join. For more information about the differences between these two join options, see [Introduction to device management in Microsoft Entra ID](#).
- Auto-enroll devices into MDM services such as Microsoft Intune (requires an Microsoft Entra ID Premium subscription for configuration).
- Automatic upgrade to Enterprise Edition if required.
- Restrict administrator account creation.
- Create and auto-assign devices to configuration groups based on a device's profile.
- Customize Out of Box Experience (OOBE) content specific to the organization.

Existing devices can also be quickly prepared for a new user with [Windows Autopilot Reset](#). The reset capability is also useful in break/fix scenarios to quickly bring a device back to a business-ready state.

Learn more: [Windows Autopilot](#)

Enterprise State Roaming with Azure

Available to any organization with a Microsoft Entra ID Premium⁹ or Enterprise Mobility + Security (EMS)⁹ license, Enterprise State Roaming provides users with a unified Windows Settings experience across their Windows devices and reduces the time needed for configuring a new device.

Learn more: [Enterprise State Roaming FAQ](#)

Universal Print

Universal Print eliminates the need for on-premises print servers. It also eliminates the need for print drivers from the users' Windows devices and makes the devices secure, reducing the malware attacks that typically exploit vulnerabilities in driver model. It enables Universal Print-ready printers (with native support) to connect directly to the Microsoft Cloud. All major printer OEMs have these [models](#). It also supports existing printers by using the connector software that comes with Universal Print.

Unlike traditional print solutions that rely on Windows print servers, Universal Print is a Microsoft-hosted cloud subscription service that supports a Zero Trust security model when using the Universal Print-ready printers. Customers can enable network isolation of printers, including the Universal Print connector software, from the rest of the organization's resources. Users and their devices do not need to be on the same local network as the printers or the Universal Print connector.

Universal Print supports Zero Trust security by requiring that:

- Each connection and API call to Universal Print cloud service requires authentication validated by Microsoft Entra ID⁹. A hacker would have to have knowledge of the right credentials to successfully connect to the Universal Print service.
- Every connection established by the user's device (client), the printer, or another cloud service to the Universal Print cloud service uses SSL with TLS 1.2 protection. This protects network snooping of traffic to gain access to sensitive data.
- Each printer registered with Universal Print is created as a device object in the customer's Microsoft Entra ID tenant and issued its own device certificate. Every connection from the printer is authenticated using this certificate. The printer can access only its own data and no other device's data.
- Applications can connect to Universal Print using either user, device, or application authentication. To ensure data security, it is highly recommended that only cloud applications use application authentication.
- Each acting application must register with Microsoft Entra ID and specify the set of permission scopes it requires. Microsoft's own acting applications—for example, the Universal Print connector—are registered with the Microsoft Entra ID service. Customer administrators need to provide their consent to the required permission scopes as part of onboarding the application to their tenant.
- Each authentication with Microsoft Entra ID from an acting application cannot extend the permission scope as defined by the acting client app. This prevents the app from requesting additional permissions if the app is breached.

Additionally, Windows 11 and Windows 10 include MDM support to simplify printer setup for users. With initial support from Microsoft Intune⁹, admins can now configure policies to provision specific printers onto the user's Windows devices.

Universal Print stores the print data in cloud securely in Office Storage, the same storage used by other Microsoft Office products. More information about Universal Print data residency and encryption can be found [here](#).

More information about handling of Microsoft 365 data (this includes Universal Print data) can be found [here](#).

The Universal Print secure release platform ensures user privacy, secures organizational data, and reduces print wastage. It eliminates the need for people to rush to a shared printer as soon as they send a print job to ensure that no one sees the private or confidential content. Sometimes, printed documents are picked up by another person or not picked up at all and discarded. Detailed support and configuration information can be found [here](#).

Universal Print has integrated with Administrative Units in Microsoft Entra ID to enable customers to assign a Printer Administrator role to their local IT team in the same way customers assign User Administrator or Groups Administrator roles. The local IT team can configure only the printers that are part of the same Administrative Unit. Detailed configuration information can be found [here](#).

Learn more: [Universal Print](#)

For customers who want to stay on Print Servers, we recommend using the Microsoft IPP Print driver. For features beyond what's covered in the standard IPP driver, use Print Support Applications (PSA) for Windows from the respective printer OEM.

Learn more: [Print support app design guide](#)

OneDrive for work or school

Data in OneDrive for work or school is protected both in transit and at rest.

When data transits either into the service from clients or between datacenters, it's protected using transport layer security (TLS) encryption. OneDrive only permits secure access. Authenticated connections are not allowed over HTTP and instead redirect to HTTPS.

There are several ways that OneDrive for work or school is protected at rest:

- Physical protection: Microsoft understands the importance of protecting customer data and is committed to securing the datacenters that contain it. Microsoft datacenters are designed, built, and operated to strictly limit physical access to the areas where customer data is stored. Physical security at datacenters is in alignment with the defense-in-depth principle. Multiple security measures are implemented to reduce the risk of unauthorized users accessing data and other datacenter resources. Learn more [here](#).

- Network protection: The networks and identities are isolated from the corporate network. Firewalls limit traffic into the environment from unauthorized locations.
- Application security: Engineers who build features follow the security development lifecycle. Automated and manual analyses help identify possible vulnerabilities. [The Microsoft Security Response Center](#) helps triage incoming vulnerability reports and evaluate mitigations. Through the [Microsoft Cloud Bug Bounty Terms](#), people across the world can earn money by reporting vulnerabilities.
- Content protection: Each file is encrypted at rest with a unique AES-256 key. These unique keys are encrypted with a set of master keys that are stored in Azure Key Vault.

Learn more: [How OneDrive safeguards data in the cloud](#)

MDM enrollment certificate attestation

When a device is enrolled into device management, the administrator assumes that the device will enroll and receive appropriate policies to secure and manage the PC as they expect. In some circumstances, enrollment certificates can be removed by malicious actors and then used on unmanaged PCs to appear as though they are enrolled, but without the security and management policies the administrator intended. With MDM enrollment certificate attestation, the certificate and keys are bound to a specific machine through the use of the Trusted Platform Module (TPM) to ensure that they can't be lifted from one device and applied to another. This capability has existed for physical PCs since Windows 11 22H2 and is now being extended to Windows 11-based Cloud PCs and Azure Virtual Desktop VMs.

Learn more: [Configuration Service Provider - Windows Client Management](#)

Protecting your personal information

Microsoft Account

Your Microsoft Account (MSA) gives you access to Microsoft products and services with just one login, allowing you to manage everything all in one place. Keep tabs on your subscriptions and order history, update your privacy and security settings, track the health and safety of your devices, and get rewards. Everything stays with you in the cloud, across devices, and between OS ecosystems, including iOS and Android.

You can even go passwordless with your Microsoft Account by removing the password from your MSA and using the Microsoft Authenticator app on your mobile Android or iOS phone.

Learn more: [What is a Microsoft account?](#)

User reauthentication before password disablement

Windows provides greater flexibility for users to balance ease of use with security. Users can choose the interval that the machine remains idle before it automatically signs the user out. To avoid a security breach and prevent users from accidentally making settings changes, Windows reauthenticates the user before they are allowed to change the setting to not sign out the user even after the device remains idle indefinitely.

This setting is available on the Sign-in options page in Settings and is available on Windows 11 and onward for MSA users worldwide.

Find my device

When location services and Find my device settings are turned on, basic system services like time zone and Find my device will be allowed to use the device's location. When enabled, Find my device can be used by the admin on the device to help recover lost or stolen Windows devices to reduce security threats that rely on physical access.

Learn more: [How to set up, find, and lock a lost Windows device using a Microsoft Account](#)

OneDrive for personal

Microsoft OneDrive¹⁷ for personal provides additional security, backup, and restore options for important personal files. OneDrive stores and protects files in the cloud, allowing users to access them from laptops, desktops, and mobile devices. Plus, OneDrive provides an excellent solution for backing up folders. If a device is lost or stolen, the user can quickly recover all their important files from the cloud.

Learn more: [OneDrive](#)

In the event of a ransomware attack, OneDrive can enable recovery. And if backups are configured in OneDrive, users have additional options to mitigate and recover from a ransomware attack.

Learn more: [How to recover from a ransomware attack using Microsoft 365](#)

Learn more: [How to restore from OneDrive](#)

OneDrive Personal Vault

OneDrive Personal Vault⁹ also provides protection for the most important or sensitive files and photos without sacrificing the convenience of anywhere access. Protect digital copies of important documents in OneDrive Personal Vault. Files will be secured by identity verification yet are still easily accessible across devices.

Learn how to [set up a Personal Vault](#) with a strong authentication method or a second step of identity verification, such as fingerprint, face, PIN, or a code sent via email or SMS.



Security Foundation

Microsoft is committed to continuously investing in improving our software development process, building highly secure-by-design software, and addressing security compliance requirements. At Microsoft, we embed security and privacy considerations from the earliest lifecycle phases of all our product design and software development processes. We build in security from the ground up for powerful defense in today’s threat environment and have the infrastructure to protect and react quickly to future threats.

Every component of the Windows 11 technology stack, from chip-to-cloud, is purposefully built secure by design. Windows 11 meets the modern threats of today’s flexible work environments by delivering hardware-based isolation, end-to-end encryption, and advanced malware protection.

With Windows 11, organizations can improve productivity and gain intuitive new experiences without compromising security.



Offensive research

Microsoft Security Development Lifecycle (SDL)

The Microsoft Security Development Lifecycle (SDL) introduces security best practices, tools, and processes throughout all phases of engineering and development.

OneFuzz service

A range of tools and techniques—such as threat modeling, static analysis, fuzz testing, and code quality checks—enable continued security value to be embedded into Windows by every engineer on the team from day one. Through the SDL practices, Microsoft engineers are continuously provided with actionable and up-to-date methods to improve development workflows and overall product security before the code has been released.

Microsoft is dedicated to working with the community and our customers to continuously improve and tune our platform and products to help defend against the dynamic and sophisticated threat landscape. Project OneFuzz—an extensible fuzz testing framework used by Microsoft Edge, Windows, and teams across Microsoft—is now available to developers around the world through GitHub as an open-source tool.

Learn more: [Project OneFuzz framework, an open source developer tool to find and fix bugs at scale](#)

Learn more: [OneFuzz on GitHub](#)

Microsoft Offensive Research and Security Engineering

[Microsoft Offensive Research and Security Engineering](#) performs targeted design reviews, audits, and deep penetration testing of Windows features using Microsoft's open-source OneFuzz platform as part of their development and testing cycle.

Windows Insider and Bug Bounty program

As part of our secure development process, the Microsoft Windows Insider Preview bounty program invites eligible researchers across the globe to find and submit vulnerabilities that reproduce in the latest Windows Insider Preview (WIP) Dev Channel.

The goal of the Windows Insider Preview bounty program is to uncover significant vulnerabilities that have a direct and demonstrable impact on the security of customers using the latest version of Windows.

Through this collaboration with researchers across the globe, our teams identify critical vulnerabilities that were not previously found during development and quickly fix the issues before releasing our final Windows.

Learn more: [Windows Insider Program](#)

Learn more: [Microsoft bounty programs](#)

Certification

Microsoft is committed to supporting product security standards and certifications, including FIPS 140 and Common Criteria, as an external validation of security assurance.

Federal Information Processing Standard (FIPS)

The Federal Information Processing Standard (FIPS) Publication 140 is a US government standard that defines the minimum security requirements for cryptographic modules in IT products. Microsoft maintains an active commitment to meeting the requirements of the FIPS 140 standard, having validated cryptographic modules against FIPS 140-2 since it was first established. Microsoft products, including Windows 11, Windows 10, Windows Server, and many cloud services, use these cryptographic modules.

Common Criteria (CC)

Common Criteria (CC) is an international standard currently maintained by national governments who participate in the Common Criteria Recognition Arrangement. Common Criteria defines a common taxonomy for security functional requirements, security assurance requirements, and an evaluation methodology used to ensure products undergoing evaluation satisfy the functional and assurance requirements.

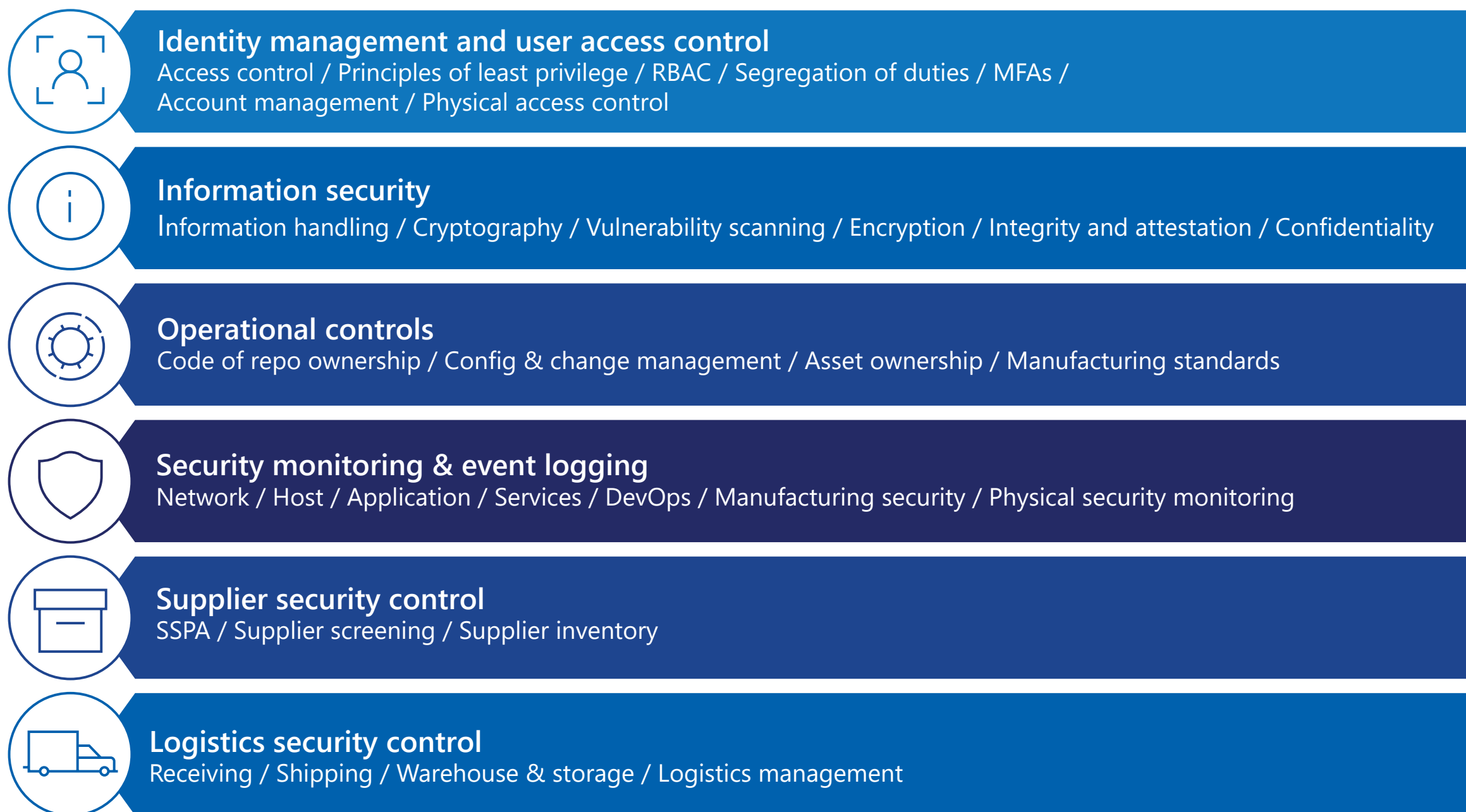
Microsoft ensures that products incorporate the features and functions required by relevant Common Criteria Protection Profiles and completes Common Criteria certifications of Microsoft Windows products.

Microsoft publishes the list of FIPS 140 and Common Criteria certified products at [Federal Information Processing Standard \(FIPS\) 140 Validation](#) and [Common Criteria Certifications](#).

Secure supply chain

The end-to-end Windows 11 supply chain is complex, extending from the entire development process to components such as chips, firmware, drivers, operating system, and apps from other organizations, manufacturing, and security updates. Microsoft invests significantly in Windows 11 supply chain security, as well as the security of features and components. In 2021, the United States issued an executive order on enhancing the nation's cybersecurity. The executive order, along with various attacks like SolarWinds and WannaCry, elevated the urgency and importance of ensuring a secure supply chain.

Microsoft requires the Windows 11 supply chain to comply with controls including:



Software bill of materials (SBOM)

In addition to following the above supply chain security controls, SBOMs are leveraged to provide the transparency and provenance of the content as it moves through various stages of the Windows supply chain. This enables trust between each supply chain segment, ensures that tampering has not taken place during ingestion and along the way, and provides a provable chain of custody for the product that we ship to customers.

Code-signing software is the best way to guarantee application integrity and authenticity and helps users distinguish between trusted applications and malware before downloading or installing. Code signing proprietary applications and software from other organizations greatly reduces the complexity of creating and managing application control policies. Code signing enables the creation and deployment of certificate chain-based application control policies, which can then be cryptographically enforced.

Traditionally, code signing has been a difficult undertaking due to the complexities involved in obtaining certificates, securely managing those certificates, and integrating a proper signing process into the development and continuous integration and continuous deployment (CI/CD) pipelines.

Windows App software development kit (SDK)

Developers can design highly secure applications that benefit from the latest Windows 11 safeguards using the Windows App SDK. The SDK provides a unified set of APIs and tools for developing secure desktop apps for Windows 11 and Windows 10. To help create apps that are up to date and protected, the SDK follows the same security standards, protocols, and compliance as the core Windows operating system.

If you are a developer, you can find security best practices and information at [Windows application development—best practices](#). You can get started with [Windows App SDK Samples on GitHub](#). For an example of the continuous security process in action with the Windows App SDK, see the [most recent release](#).

Conclusion



Conclusion

We will continue to bring you new features to protect against evolving threats, simplify management, and securely enable new workstyles. With Windows 11 devices, organizations of all sizes can benefit from the security and performance to thrive anywhere.

For the latest information and version of this document see windows.com/business/windows-11-security.

What's new

New

[Config Refresh](#)

[5G and eSIM](#)

[Win32 apps in isolation \(public preview\)](#)

[Passkey](#)

[Sign-in Session Token Protection](#)

[Windows Local Administrator Password Solution \(LAPS\) \(public preview\)](#)

[Microsoft Intune Suite Endpoint Privilege Management \(EPM\)](#)

[Microsoft Intune Suite Endpoint Privilege Management \(EPM\)](#)

Enhanced

[Hardware security user experience](#)

[BitLocker to go](#)

[Device encryption](#)

[Windows Firewall](#)

[Server Message Block direct](#)

[Smart App Control \(SAC\) going into Enforcement mode](#)

[Application Control for Business](#)

[Enhanced Sign-in security \(ESS\)](#)

[Windows Hello for Business](#)

[Presence Detection](#)

[Wake on approach, lock on leave](#)

[Universal Print](#)

[Lockout policies for local admin](#)

[Enhanced Phishing protection](#)

Document revision history

Date	Summary
November 2021	Link updates and formatting
February 2022	Revisions to Hardware root-of-trust, Virus and threat protection, and Windows Hello for Business content.
April 2022	Added Upcoming features section
September 2022	Updates with Windows 11 2022 Update features and enhancements. See What's new (LINK to section)
April 2023	Minor edits and updates to edition availability
September 2023	Updates with Windows 11 2023 Update features and enhancements

Endnotes

1. "2023 Data Breach Investigations Report," Verizon, 2023.
2. "Microsoft Digital Defense Report 2022," Microsoft, 2022.
3. Compared to Windows 10 devices. "Improve your day-to-day experience with Windows 11 Pro laptops," Principled Technologies, February 2023.
4. Based on Monthly Active Device data. "Earnings Release FY23 Q3," Microsoft, April 2023.
5. Windows 11 results are in comparison with Windows 10 devices. "Windows 11 Survey Report," Techaisle, February 2022.
6. Requires developer enablement.
7. Requires Microsoft Entra ID (formerly AAD) and Microsoft Intune or other modern device management solution product required; sold separately.
8. Commissioned study delivered by Forrester Consulting. "The Total Economic Impact™ of Windows 11 Pro Devices", December 2022. Note, quantified benefits reflect results over three years combined into a single composite organization that generates \$1 billion in annual revenue, has 2,000 employees, refreshes hardware on a four-year cycle, and migrates the entirety of its workforce to Windows 11 devices.
9. Sold separately
10. Email encryption is supported on products such as Microsoft Exchange Server and Microsoft Exchange Online.
11. Microsoft internal data.
12. Microsoft Entra ID Basic is included with Microsoft Azure and Microsoft 365 subscriptions, and other commercial services subscriptions.
13. Requires Microsoft Entra ID (formerly AAD) Premium; sold separately.
14. Hardware dependent.
15. Microsoft 365 E3 or E5 required; sold separately.
16. The Total Economic Impact™ of Windows Pro Device, Forrester study commissioned by Microsoft, June 2020.
17. All users with a Microsoft Account get 5GB of OneDrive storage free, and all Microsoft 365 subscriptions include 1TB of OneDrive storage. Additional OneDrive storage is sold separately.

The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.

This paper is for informational purposes only. Microsoft makes no warranties, express or implied, in this document.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in, or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

© 2023 Microsoft Corporation. All rights reserved.

Microsoft, list Microsoft trademarks used in your white paper alphabetically are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Part No. September 2023