

Windows Education security guide: The most secure Windows ever



Welcome

03 /

Introduction

07 /

Windows 11 enables Zero Trust protection

08 /

Windows Education security priorities

Why security matters

The expansion of technology in online and offline learning brings exciting new opportunities to educators and students. Education has transformed, and schools need advanced, affordable, intuitive tools to help all students access instruction and gain future-proof skills, wherever learning happens.

At Microsoft, we're analyzing how this expansion of technology exposes education to cyberthreats—and how to prevent associated risks. According to data from the Microsoft Digital Defense Report 2022, the education sector bore 14 percent of attacks by nation state actors.¹

We're also learning from others' findings: in 2021 alone, the K-12 Security Information Exchange reported 166 breaches in US school districts, including impacts to school budgets and student privacy.²

We recognize that our K-12 customers are tasked with protecting fast-growing data ecosystems in this shifting security landscape, with limited resources—and while managing threat exposure from multiple vendors and apps.

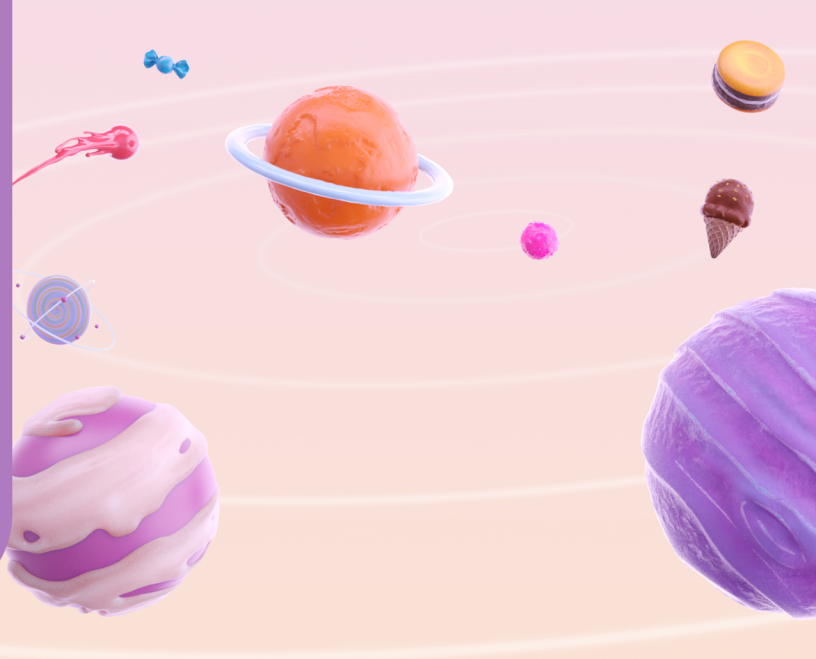
We've designed Windows 11 to help K-12 IT administrators meet these security challenges.

¹[Microsoft Digital Defense Report 2022](#).

²"The State of K-12 Cybersecurity Report 2022," K-12 Security Information Exchange.



“Several needs are clear...
The need for cybersecurity
threat intelligence, guidance,
and best practices **to be
tailored specifically for
the K-12 sector.**”³



Microsoft brings deep insight into cyberthreat tools that help our K-12 customers prevent breaches.



8,500+

Security professionals



1.3 billion

Windows devices in use globally



20 billion+

Invested in security over 5 years⁴



4.3 trillion

Security signals analyzed daily⁵

Windows Education devices leverage the Microsoft security ecosystem.

With Windows 11 and Windows 11 SE devices, you can enable online and offline learning anywhere while advancing security for schools, educators, and students. We designed Windows 11 Education devices for K-12 end users, with Windows 11 SE devices further customized to meet the needs of K-8 students.

³"The State of K-12 Cybersecurity Report 2022," K-12 Security Information Exchange.

⁴"[Microsoft expands on cybersecurity commitments for U.S. government agencies](#)," Microsoft in Business Blogs.

⁵[Microsoft Digital Defense Report 2022](#).

Microsoft offers three editions of Windows Education



Windows 11 Education

Offers the same security capabilities as Windows 11 Enterprise in an experience designed for education customers. This includes the by-default disabling of Cortana and Microsoft Store suggestions. Windows 11 Education is available through volume license subscriptions.

➞ [Learn more about Windows 11 Education](#)

Windows 11 Pro Education

Offers the same security capabilities of Windows 11 Pro in an experience designed for education customers, while also allowing students and teachers to install apps on their devices. This edition comes pre-loaded on devices purchased through the Shape the Future Program academic volume license subscriptions, which guarantees that you receive the best pricing on pre-installed Windows 11 Education devices.

➞ [Learn more about the Shape the Future Program](#)



Windows 11 SE

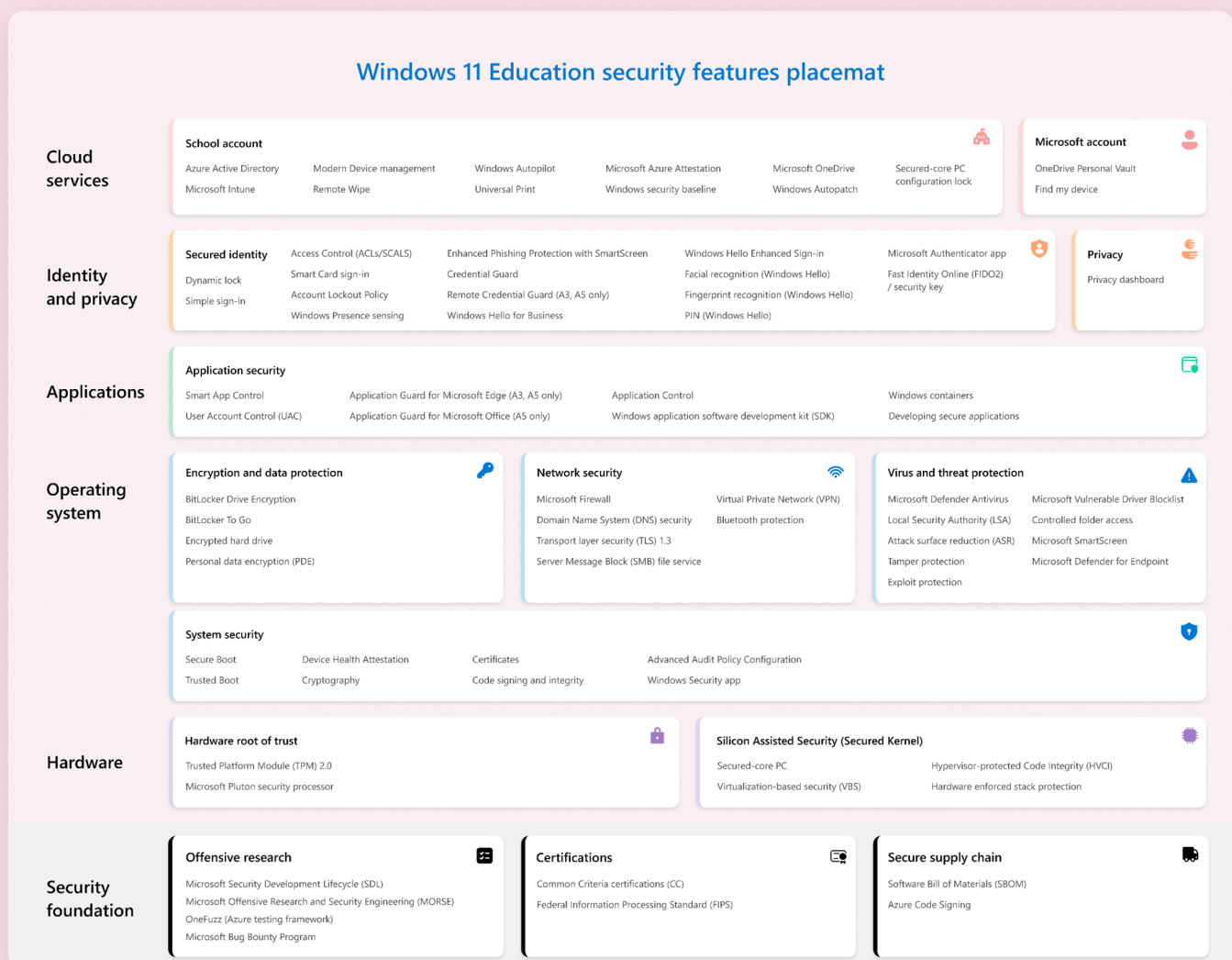
Offers the same security capabilities as Windows 11 Pro. This edition comes preloaded on Windows 11 SE devices, and delivers a **cloud-first, simplified design optimized for educational settings, especially grades K-8**. Students enjoy great educational experiences with fewer tech distractions and IT administrators benefit from unified management tools—all on devices that start at US\$249.

➞ [Learn more about Windows 11 SE](#)

Approximately 80 percent of security decision makers say that software alone is not enough protection from emerging threats.⁶

In Windows 11, hardware and software work together to protect sensitive data from the core of your device all the way to the cloud. The layered, comprehensive protection helps keep your school, teachers, and students secure, no matter where learning happens.

See the layers of protection in this diagram and get a brief overview of our security priorities below.



⁶[Microsoft Security Signals for SDMs, 2021.](#)

“Because Microsoft designed the security model of Windows 11 from the ground up to assume that some component has already been compromised, threat actors will find it orders of magnitude more difficult to remain undetected [and persist] in the environment than in traditional architectures.”

- SANS Institute⁷

Windows 11 enables Zero Trust protection

The Zero Trust model reduces breadth and depth of risk. Instead of trusting access requests from within a district or school firewall, Zero Trust treats every access request as though it originates from an open network. Zero Trust security is based on three principles:



Verify explicitly.

Require verification of data points such as user identity, permissions, location, and device health—for every access request, every time, without exception.



Use least privilege access.

After verification, grant access only to necessary resources, for only the necessary amount of time.



Assume breach.

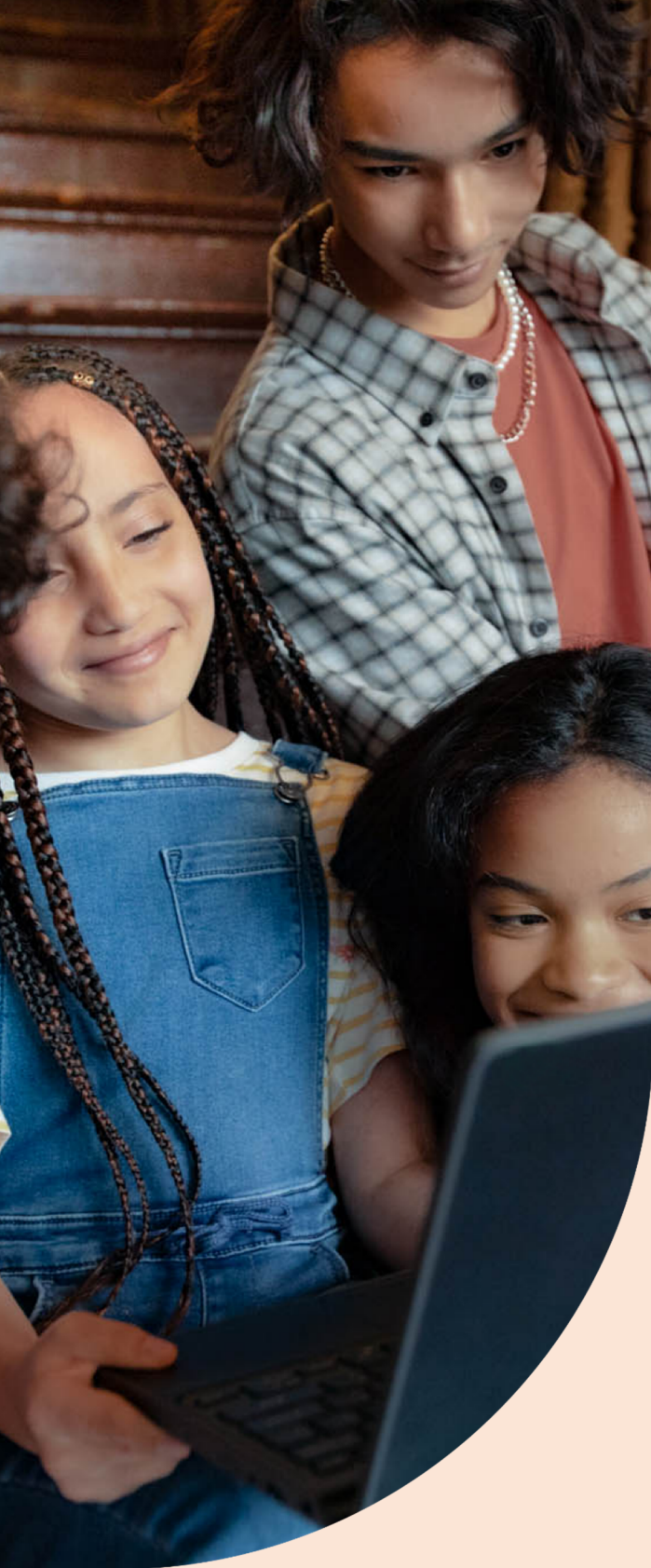
Continuous analytics to detect threats and improve defenses.

On Windows 11, the Zero Trust principles inform our chip-to-cloud security, enabling IT administrators to implement strong authorization and authentication processes, and visibility into device health.

Devices work out-of-the-box with Microsoft Endpoint Manager and Azure Active Directory,⁸ so access decisions and enforcements are seamless and don't interfere with instruction or homework. Plus, IT administrators can easily customize Windows 11 to meet specific requirements for access, privacy, compliance, and more.

⁷[How SMBs Can Benefit from the Security Protections of Windows 11](#), SANS Institute 2022.

⁸Azure Active Directory sold separately.



Windows 11 Education security priorities

Windows 11 raises the security baseline with new requirements for integrated hardware and software protections—from chip to cloud.

Here is some of the ways we're committed to helping schools adapt to technology-enhanced learning while protecting against constantly evolving cyberthreats.

Security from the start

Enhanced hardware & operating system security

Robust application security

Secured identities

Simple Sign-in

Windows Hello

Connecting to cloud services

Security from the start

Schools increasingly gather and store sensitive student and employee data in the cloud. Meanwhile, nearly 90 percent of security decision makers surveyed say outdated hardware leaves organizations more open to attacks and using modern hardware would help protect against future threats.⁹

To help schools stay ahead of evolving threats, we've worked with our partners to build on the innovations of Windows 10. The advanced security requirements for Windows 11 devices support schools' growing reliance on technology, with a foundation that is even more resilient to attacks.



Enhanced hardware and operating system security



With hardware-based isolation security that begins at the chip, Windows 11 stores sensitive data behind additional barriers separated from the operating system. As a result, Windows 11 protects information, including encryption keys and user credentials, from unauthorized access and tampering.

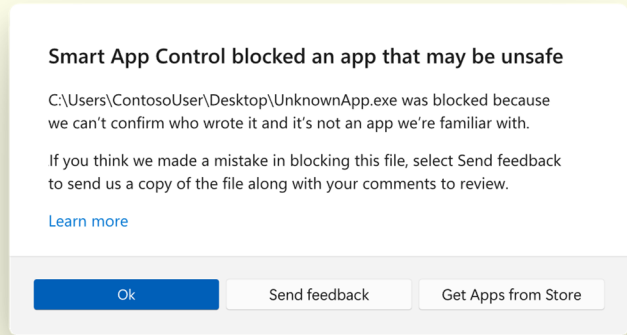
In Windows 11, hardware and software work together to protect the operating system.

For example, new devices come with virtualization-based security (VBS) and Secure Boot built in and enabled by default to contain and limit malware exploits.¹⁰

⁹[Microsoft Security Signals for SDMs, 2021.](#)

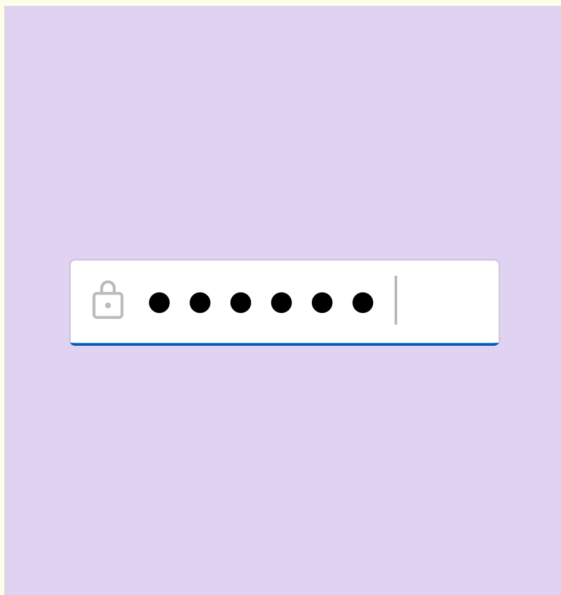
¹⁰Requires compatible hardware with biometric sensors.

Robust application security



To help keep information protected and private for students, teachers, and schools, Windows 11 uses multiple layers of integrated application security—including application isolation and controls, code integrity, privacy controls, and least privilege principles. This approach gives developers the control they need to build in security and privacy, to help prevent breaches and malware.

In Windows 11, Microsoft Defender Application Guard¹¹ uses Hyper-V virtualization technology to isolate untrusted websites and Microsoft Office files in containers, separate from and unable to access the host operating system and enterprise data. To protect privacy, Windows 11 also provides more controls over which apps and features can collect and use data such as the device's location, or access resources like camera and microphone.



Secured identities

Passwords are a top target of cybercriminals. Windows 11 provides powerful protection against credential theft with chip-level hardware security. Credentials are protected by layers of hardware and software security such as TPM 2.0, VBS, and/or Windows Defender Credential Guard, making it harder for attackers to steal credentials from a device. And with Windows Hello, educators can quickly sign in with face, fingerprint, or PIN for passwordless protection.¹²

¹¹Windows 10 Pro and above support Application Guard protection for Microsoft Edge. Microsoft Defender Application Guard for Office requires Windows 10 Enterprise, and Microsoft 365 E5 or Microsoft 365 E5 Security.

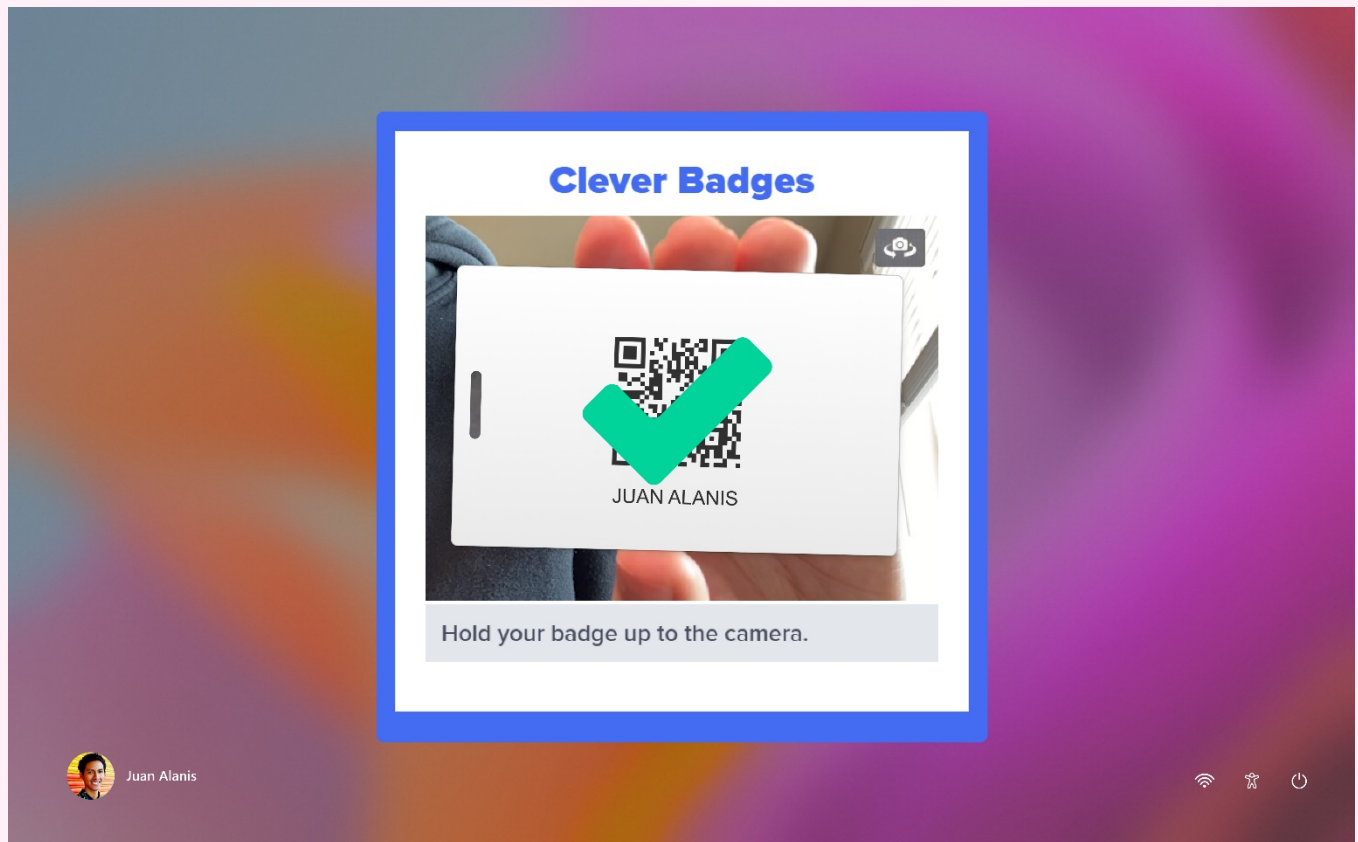
¹²[Get the free Microsoft Authenticator app for Android or iOS](#)

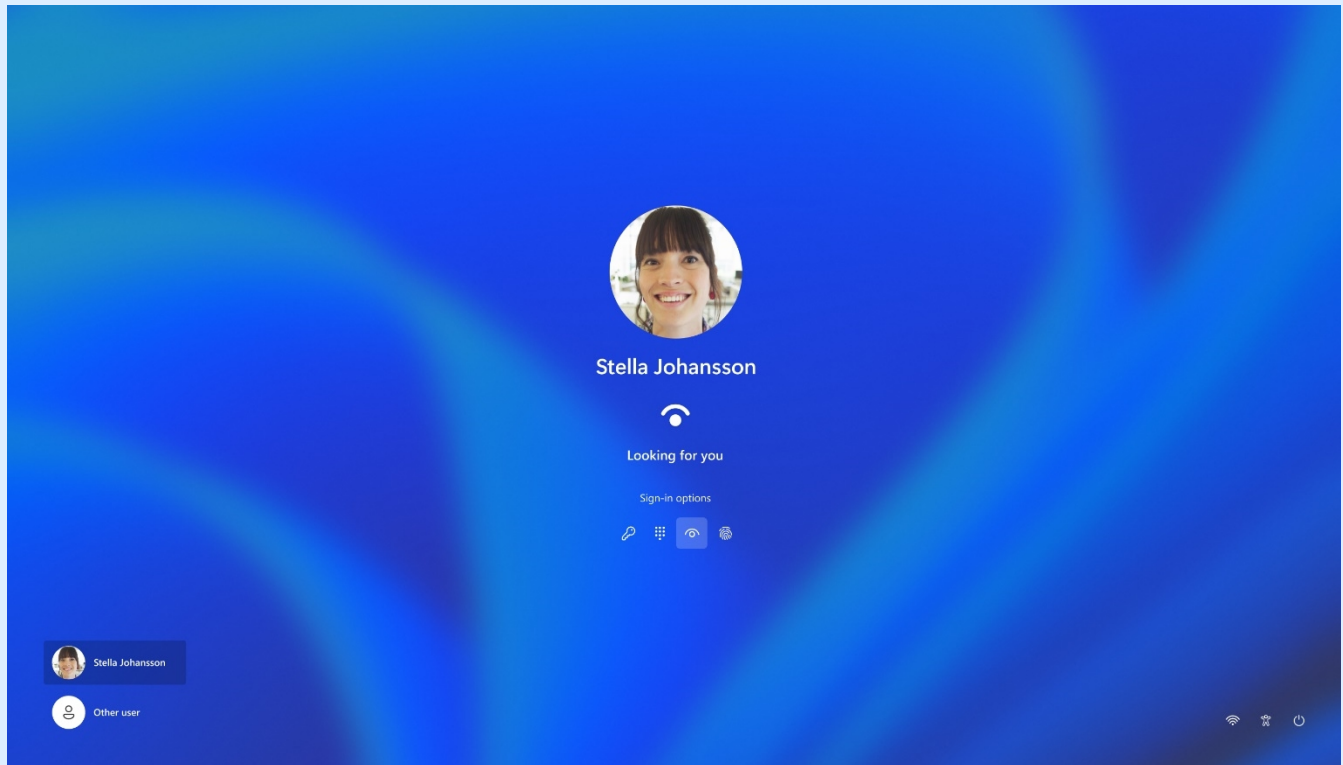


Simple sign-in

On Windows 11 SE, students can quickly and easily sign in using existing third-party providers, such as Google or Clever. This means younger learners can use logins they already know to access their materials.

This reduces the quantity of passwords they must create, track, or remember—to help minimize disruptions and enhance security.





Windows Hello



Windows Hello lets you sign into your devices, apps, online services, and networks using your face, iris, fingerprint, or a PIN.¹³ Even if your Windows device can use Windows Hello biometrics, you don't have to. If it's the right choice for you, you can rest assured that the info that identifies your face, iris, or fingerprint never leaves your device. Windows does not store pictures of your face, iris, or fingerprint on your device or anywhere else. Your biometric data will remain on your device until you remove it.

However, after a significant period of Windows Hello inactivity, you will be prompted to confirm that you want to continue to store your biometric data. You can go to Settings and remove Windows Hello, and any associated biometric identification data, at any time. If you enrolled using an external device, such as a USB fingerprint reader, please connect the device first.

For more information, check out this website: [Learn about Windows Hello and set it up.](#)

¹³Windows Hello supports multi-factor authentication including facial recognition, fingerprint, and PIN. Requires specialized hardware such as fingerprint reader, illuminated IR sensor or other biometric sensors and capable devices. Part No. 20 September 2022.



Connecting to cloud services

Microsoft offers comprehensive cloud services for identity, storage, and access management in addition to the tools needed to attest that Windows 11 devices connecting to your network are trustworthy.

You can also enforce compliance and conditional access with a modern device management (MDM) service such as Microsoft Intune for Education, which works with Azure Active Directory¹⁴ and Microsoft Azure Attestation to control access to applications and data through the cloud.



¹⁴Azure Active Directory sold separately.

Thank you.

Designed for online and offline learning, Windows 11 is the most secure Windows yet with hardware and software working together to provide powerful protection across the device, operating system, identities, applications, and cloud services. We will continue to build on our security foundations with innovations that deliver powerful protection now and in the future.

➞ **Learn how to upgrade to Windows 11 Education now**

For technical information on security features in Windows 11 devices, please visit:

➞ aka.ms/commercialsecuritybook

