Microsoft Surface

Modern device deployment and management across school settings

Cookbook for Windows 11 + Surface Laptop SE + Microsoft 365 Education + Intune for Education

Contents

Why read this cookbook?

Microsoft 365 solutions for Education empower education professionals to unlock creativity, promote teamwork, and provide a simple and safe experience for everyone—all in a comprehensive and affordable cloud offering. This cookbook introduces the tools and services available from Microsoft for deploying and managing devices in schools, thereby enabling modern device management across the school environment. The cookbook is intended for education professionals responsible for these efforts, including:

- System or school leaders
- IT administrators
- Teachers
- Microsoft partners

In the cookbook, we provide a comprehensive path for schools to enroll, deploy, and manage new Surface Laptop SE and Windows 11 SE devices. Specifically, we include step-by-step guidance on the deployment, management, and resetting of the new Surface Laptop SE and Windows 11 SE operating system for education. At multiple steps, we also highlight resources available on Microsoft Docs to help with your rollout. Note that depending on your school setup scenario, you may not need to implement all steps.

New expectations for education technology

Microsoft recognizes that the education landscape continues to change rapidly and dramatically. To better equip students for success, it's essential for schools to stay up to date with technology and tools for teaching and learning. The Microsoft cloud management solution is flexible, affordable, and scalable—helping to ensure that devices are easily updated and students always have what they need, whether they're learning in person or remotely, synchronously or asynchronously. Microsoft also delivers exceptional standards of security and privacy to keep students safer as the hybrid learning model evolves.

Below are some additional key ways that Microsoft addresses expectations for modern device management in school environments:

- **Maximize learning time.** Schools expect lower boot times for an enhanced user experience for students and staff, all on a device optimized for the classroom. They also expect devices to always be up to date with policies that update silently and outside of class time. Intune for Education enables automatic updates to all school devices and software at optimal times you choose.

- **Designed for learning environments.** Schools need identity-based management for secure app delivery and simple device management. They also need to ensure that the right apps are delivered at the right time. With Azure Active Directory (Azure AD) and Intune for Education, you can enable profile-based app delivery with the ability to manage device policies, settings, and apps. You can also save time setting up devices with more apps and policies preinstalled and preconfigured than ever before—simply enroll and go.
- **Simplify deployment and management.** End-to-end guidance and support from Microsoft and partners can help schools streamline both deployment and cloud migration. With Intune for Education and Surface SE devices, education professionals can deploy apps to users and apply device settings that create a great classroom experience in just a few simple steps.
- **Cost-effective remote management.** Intune for Education enables a modern IT environment—complete with remote management—in school settings. This helps to provide reduced and more predictable IT costs, along with better performance, availability, and security. Intune for Education also enables a predictable and stable software as a service (SaaS) model, which eliminates spending spikes from upgrading hardware and software.

The powerful simplicity of Microsoft education technology

Our innovative approach to education technology is built on the idea of *powerful simplicity* and combines the unparalleled user experience and security features of Surface Laptop Student Edition (SE), Windows 11 SE, and Microsoft 365 Education. Students can unlock learning and develop new skills with Surface Laptop SE, which seamlessly runs Windows 11 SE—our new, cloud-first operating system—and Microsoft 365 Education. Surface Laptop SE comes preloaded with widely used apps like Microsoft Teams, Word, PowerPoint, Excel, and OneNote, so students are ready to learn right from the start. Likewise, teachers will appreciate how easy it is to develop and deploy their lessons and enrichment experiences, while IT administrators will save time, money, and frustration with comprehensive modern device management.

Device lifecycle management

Historically, school IT administrators and educators have struggled to find a simple, flexible, and secure way to manage the lifecycle of the devices in their schools. In response, Microsoft has developed integrated suites of products for streamlined, cost-effective device lifecycle management.

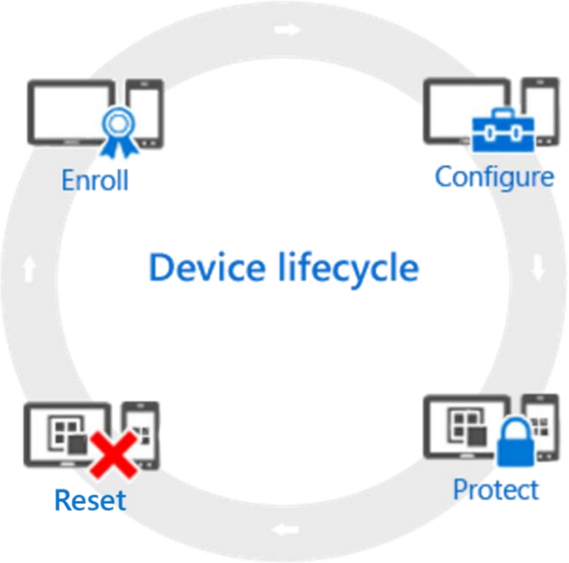
Microsoft 365 Education provides tools and services that enable simplified management of all devices through Microsoft Endpoint Manager (MEM). This gives IT administrators the flexibility to support diverse scenarios, including both school-owned devices and bring-your-own devices. MEM services include Microsoft Intune, Microsoft Intune for Education, Configuration Manager, Desktop Analytics, Windows Autopilot, and Surface Management Portal. These services are part of the Microsoft 365 stack to help secure access, protect data, and manage risk.

Why Intune for Education?

Surface Laptop SE with Windows 11 SE can be managed with Intune for Education, enabling simplified management of multiple devices from a single point. With the Set Up School PCs app, you can select Windows 11 SE as the operating system and then create a simple provisioning package. You can also use Windows Autopilot to set up Windows 11 SE devices across your schools. Similarly, Intune for Education provides simple avenues for resetting devices at the end of the school year so that they can be reused the following year.

From enrollment, through configuration and protection, to resetting, Intune for Education helps school IT administrators manage and optimize the devices across school settings:

- **Enroll.** To enable remote device management as the IT administrator, you need to enroll devices through an account in your tenant. Some methods require you to initiate enrollment, while others require students to complete the initial device setup process. This cookbook discusses the facets of various device enrollment methods.
- **Configure.** With Intune for Education, it's easy to register, prepare, and configure Surface Laptop SE devices. Intune for Education ensure that these devices are secure and compliant with school standards and policies. Moreover, as the IT administrator, you can easily configure these policies and settings to control the features and capabilities of all managed devices. In this cookbook, we highlight the "what and how" of policy configuration for IT administrators, along with the end-user deployment experience.
- **Protect.** In addition to its configuration capabilities, Intune for Education helps protect managed devices from unauthorized access or malicious attacks. For example, adding an extra layer of authentication with Windows Hello can make devices more secure. Policies are available that let you control settings for Windows Firewall, Endpoint Protection, and software updates.
- **Reset.** When it's time to repurpose a device, Intune for Education offers several methods, including resetting the device, removing it from management, and wiping it of school data. In this cookbook, we cover these and other device return and exchange scenarios.



For more information, see [Overview of the Microsoft Intune MDM lifecycle](#).

Four pillars of modern device management

In the remainder of this cookbook, we will discuss the key concepts and benefits of modern device management with Microsoft 365 solutions for education. The cookbook is organized around the four main pillars of modern device management:

Identity management. Setting up and configuring the identity system, with Microsoft 365 Education and Azure Active Directory as the foundation for user identity and authentication.

Initial setup. Setting up the Intune for Education environment for managing updates, applications, and settings.

Device enrollment. Setting up Windows 11 SE devices for deployment and enrolling them in Intune for Education.

Device reset. Resetting managed devices with Intune for Education.

Identity management

The Microsoft platform for education simplifies the management of devices and apps with Windows 11, Intune for Education, and Microsoft 365 Education. The first and most essential step is configuring the identity infrastructure to manage user access and permissions for your school.

Microsoft 365 Education uses Azure Active Directory, a cloud-based service included with the Microsoft 365 Education subscription, to manage user identities and authentication. Azure AD provides authentication and authorization for access to a resource. Identity objects exist for human identities like students and teachers, as well as non-human identities like devices and applications. Azure AD identities are assigned Microsoft 365 licenses, providing users with access to apps and resources within the tenant. With Microsoft 365 Education on Surface Laptop SE, you can issue cloud identities for teachers and students, assign licenses to devices and users, and create groups for classrooms and clubs—all more seamlessly and safely than ever before.

Setting up a Microsoft 365 Education tenant

In this section, you will create and configure a Microsoft 365 tenant and explore the Microsoft 365 admin center.

Create a Microsoft 365 tenant account

If you don’t already have a Microsoft 365 tenant account, you will need to create one. For more information, see Create your Office 365 tenant account, and then return to this document to continue with the steps below.

Set up the tenant

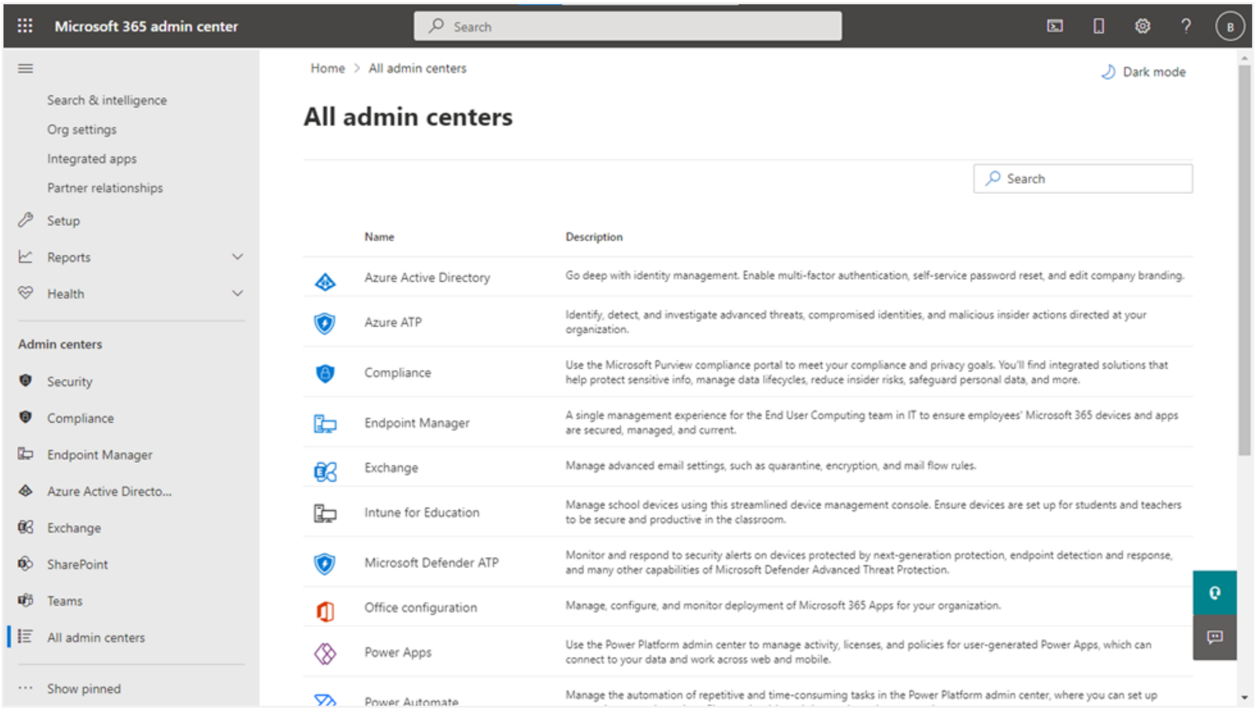
To set up the Microsoft 365 tenant for your school, follow this interactive demo. Then, return to this document to continue with the steps below.

Explore the Microsoft 365 admin center

The Microsoft 365 admin center is the hub for all administrative consoles for the Microsoft 365 cloud. To access the Microsoft 365 admin center:

1. Go to admin.microsoft.com.
2. Sign in with the global administrator you used when creating your Microsoft 365 tenant account.

As shown below, you can access the admin centers for Azure Active Directory, Microsoft Endpoint Manager, Intune for Education, and others through the Microsoft 365 admin center. For more information, see Overview of the Microsoft 365 admin center, and then return to this document to continue with the steps below.



All admin centers

Name	Description
Azure Active Directory	Go deep with identity management. Enable multi-factor authentication, self-service password reset, and edit company branding.
Azure ATP	Identify, detect, and investigate advanced threats, compromised identities, and malicious insider actions directed at your organization.
Compliance	Use the Microsoft Purview compliance portal to meet your compliance and privacy goals. You'll find integrated solutions that help protect sensitive info, manage data lifecycles, reduce insider risks, safeguard personal data, and more.
Endpoint Manager	A single management experience for the End User Computing team in IT to ensure employees' Microsoft 365 devices and apps are secured, managed, and current.
Exchange	Manage advanced email settings, such as quarantine, encryption, and mail flow rules.
Intune for Education	Manage school devices using this streamlined device management console. Ensure devices are set up for students and teachers to be secure and productive in the classroom.
Microsoft Defender ATP	Monitor and respond to security alerts on devices protected by next-generation protection, endpoint detection and response, and many other capabilities of Microsoft Defender Advanced Threat Protection.
Office configuration	Manage, configure, and monitor deployment of Microsoft 365 Apps for your organization.
Power Apps	Use the Power Platform admin center to manage activity, licenses, and policies for user-generated Power Apps, which can connect to your data and work across web and mobile.
Power Automate	Manage the automation of repetitive and time-consuming tasks in the Power Platform admin center, where you can set up

NOTE: Setting up your school's basic cloud infrastructure does not require you to complete the rest of the Microsoft 365 setup. For this reason, we will skip directly to adding students and teachers as users in the Microsoft 365 tenant.

Adding users, creating groups, and assigning licenses

With the Microsoft 365 tenant in place, it's time to add users, create groups, and assign licenses. All students and teachers need a user account before they can sign in and access Microsoft 365. There are multiple ways to do this, including using School Data Sync (SDS) to add users to the tenant; integrating on-premises Active Directory to work with Microsoft 365 and provision cloud identities; or manually assigning users, groups, and licenses.

NOTE: Synchronizing your SIS with School Data Sync is the preferred way to add students and teachers as users in a Microsoft 365 Education tenant. However, if you want to integrate an on-premises directory and synchronize accounts to the cloud, skip directly to Azure Active Directory sync below.

School Data Sync

School Data Sync imports and synchronizes SIS data to create classes in Microsoft 365, such as Microsoft 365 groups and class teams in Microsoft Teams. SDS can be used to create new, cloud-only identities or to evolve existing identities. Existing users evolve into "students" and "teachers" and are associated with a "grade," "school," and other education-specific attributes and associations. For more information, see Overview of School Data Sync.

Configure and deploy School Data Sync

To get started with School Data Sync, follow the Microsoft School Data Sync demo, which provides detailed steps to access, configure, and deploy School Data Sync for your Microsoft 365 Education subscription. For additional deployment guidance, see Choose a deployment method. Then, return to this document to continue with the steps below.

NOTE: You can perform a test deployment by cloning or downloading sample SDS CSV school data from the O365-EDU-Tools GitHub site. Remember that you should typically deploy test SDS data (users, groups, and so on) in a separate test tenant, not your school production environment.

Azure Active Directory sync

To integrate an on-premises directory with Azure Active Directory, you can use Azure AD Connect to synchronize users, groups, and other objects. Azure AD Connect lets you configure the authentication method appropriate for your school, including password hash synchronization, pass-through authentication, or federation integration with Active Directory Federation Services (AD FS) or a non-Microsoft SAML identity provider. For more information, see Set up directory synchronization for Microsoft 365, and then return to this document to continue with the steps below.

Manual assignment

In addition to the above methods, you can manually add users and groups and assign licenses through the Microsoft 365 admin center.

Add users manually

There are two options for adding users manually—either individually or in multiples:

(**Option 1**) To add students and teachers as users in Microsoft 365 Education individually:

- Go to admin.microsoft.com to access the Microsoft 365 admin center.
- Select **Users** → **Active users**, and then select **Add a user**.
- For more information, see Add users and assign licenses at the same time.

(Option 2) To add *multiple* users to Microsoft 365 Education:

- In the Microsoft 365 admin center, select **Users** → **Active users**, and then select **Add multiple users**.
- Follow the **Import multiple users** panel to assign accounts.
- For more information, see Add multiple users in the Microsoft 365 admin center.

Create groups

To organize users, create groups:

- In the Microsoft 365 admin center, select **Groups**, and then ensure you are in **All groups**.
- Select **New group**.
- On the **Choose a group type** page, select **Microsoft 365**, and then select **Next**.
- For more information, see Create a group in the Microsoft 365 admin center.

Assign licenses

The recommended way to assign licenses is through group-based licensing. With this method, Azure AD ensures that licenses are assigned to all members of the group. Any new members who join the group are assigned the appropriate licenses, and when members leave, their licenses are removed. To assign a license to each user account:

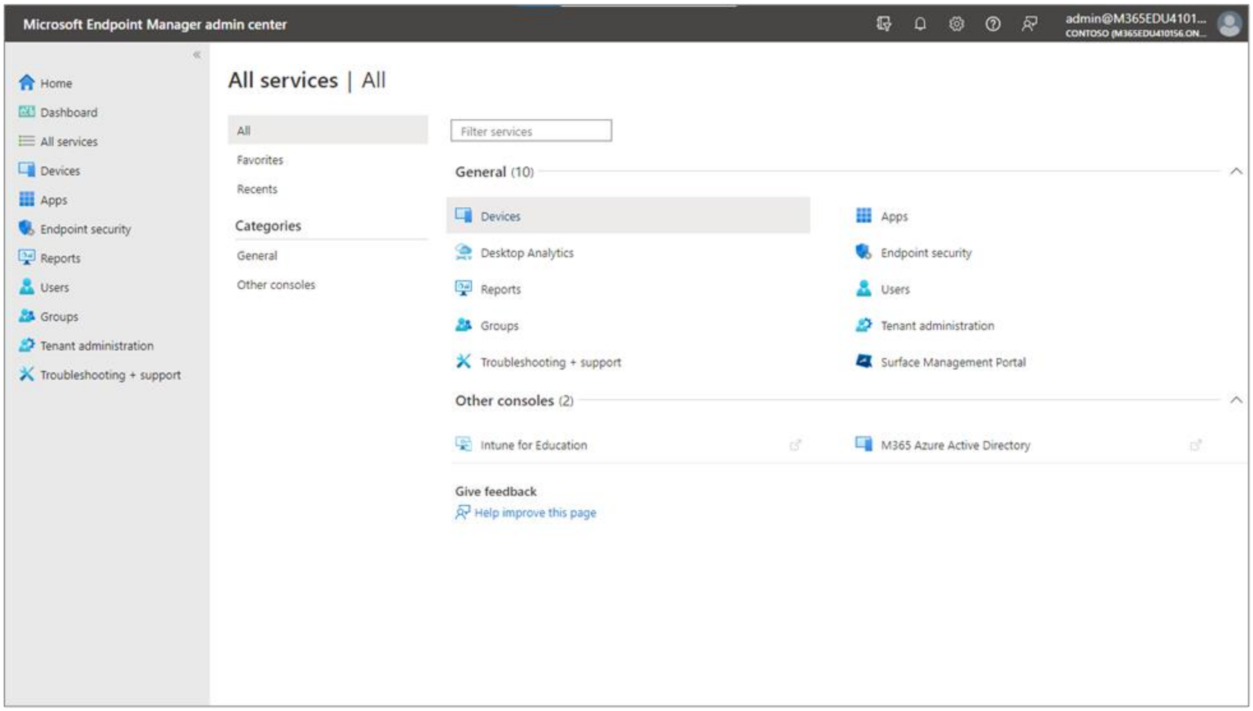
- Go to portal.azure.com.
- Select **Azure Active Directory** → **Licenses**.
- Under **All products**, select the required licensing, and then select **Assign**.
- Add the group to which the licenses should be assigned.
- For more information, see Assign a license to a group in Azure Active Directory.

NOTE: You can also use the Azure Active Directory admin center for group-based licensing. For more information, see Group-based licensing using Azure AD admin center.

UP NEXT: With users and groups created, assigned, and licensed for Microsoft 365 Education, we are ready to set up and manage students' and teachers' devices. To do this, we need to configure Microsoft Intune for Education.

Initial setup

This section of the cookbook focuses on how to set up the device management environment. Managing hundreds of devices across a school environment can be complex and time-consuming without the proper tools and resources. Microsoft Endpoint Manager provides a collection of cloud-based device management services that can help to eliminate this complexity. Intune for Education is one such service provided by Microsoft Endpoint Manager for managing and configuring students' and teachers' devices.



Cloud-based device management

Microsoft Intune for Education is a cloud-based mobile device management service for schools. It is designed to enable common education scenarios and settings, such as the need for shared devices. Intune for Education supports an entire device lifecycle that begins when a device is enrolled and progresses through additional phases until the device is no longer used. IT administrators can easily manage classroom devices with bulk enrollment and streamlined deployment. At the end of the school year, they can also reset devices, wipe them, and prepare them for next year. For more information, see Intune for Education documentation, and then return to this document to continue with the steps below.

Configuring management settings

With Intune for Education, you can configure group settings to manage how users and devices will interact in your school. Settings assigned to users will apply regardless of what devices they use. Similarly, settings assigned to devices will apply regardless of who is using them. There are two ways to manage group settings in Intune for Education:

- **Express Configuration.** Configure a selection of settings that are most used in school environments.
- **Group settings.** Configure all settings for any group of devices or users.

NOTE: Express Configuration is ideal when you are just getting started. Settings are preconfigured to Microsoft-recommended values but can be changed to fit your school's policies. We recommend using Express Configuration to set up your Windows devices.

Prerequisites

Before configuring settings with Intune for Education, consider these prerequisites:

- **Microsoft subscription.** In most scenarios, Microsoft 365 may be the best option, as it provides Enterprise Mobility + Security (EMS), Microsoft Endpoint Manager, and common productivity apps. Intune for Education is included in Microsoft 365 Education A1 for Devices, A3, and A5. For more information, see this this comparison sheet, which includes a table detailing the Microsoft Modern Work Plan for Education.
- **Intune subscription.** Intune is licensed in three ways—as a standalone Azure service, as part of EMS, and included with Microsoft 365. (For more information, see Intune licensing.) You can also sign up for a free trial account.
- **Supported device platform.** School devices running Windows 10 (1709 and later), Windows 11, Windows 11 SE, iOS (11.0 and later), and iPad OS (13.0 and later) are supported.
- **Optional requirements.** Microsoft 365 Education, Azure Active Directory Connect, School Data Sync, Set Up School PCs app, Windows Configuration Designer, and Windows Autopilot.

Configure settings with Express Configuration

With Express Configuration, you can get Intune for Education up and running in just a few steps, all from a single console. You can select a group of Windows 11 SE devices or users, pick the specific apps that you want available, and choose key configuration settings from those most often used in schools.

The Intune for Education portal provides a step-by-step walkthrough of how to use Express Configuration; you can access the demo from the home page. For more information, see Express Configuration in Intune for Education, and then return to this document to continue with the steps below.

Configure group settings

Groups are used to manage users and devices with similar management needs, allowing you to apply changes to many devices or users at once. To review the available group settings:

1. Go to the Intune for Education portal, and then select the **Groups** tile.
2. On the **Choose settings** screen, select **Group**.
3. Select the reverse caret to expand the group and review information about individual settings.

For more information, see Set up Intune for Education, and then return to this document to continue with the steps below.

NOTE: For a fully interactive demo, see the Microsoft Education Interactive Demos site. The Intune for Education demo shows how IT administrators can deploy apps and policies designed for classroom directly from the cloud. It also explains how using Intune for Education helps to ensure that the right apps are delivered to the right devices at the right time.

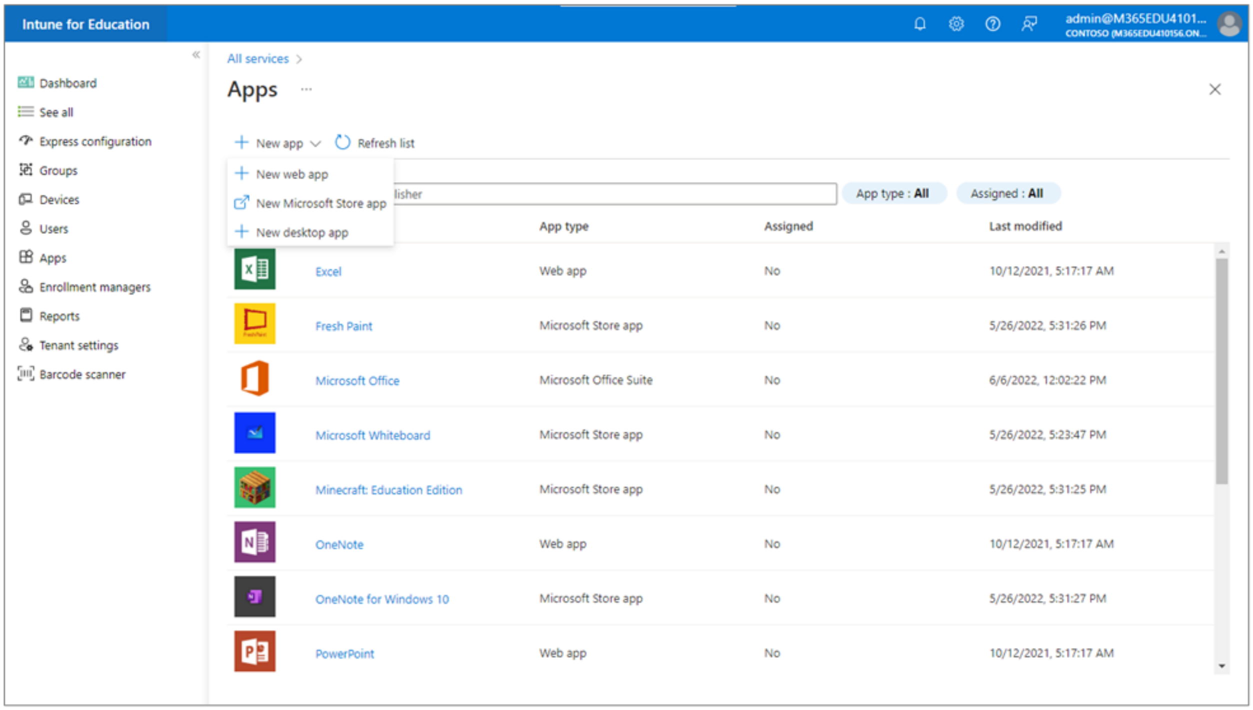
Managing Windows 11 SE apps

Windows 11 SE supports all web applications and a set of native applications. These apps can be deployed using the Intune for Education portal. For the list of available desktop apps, see Available apps. If the apps you need aren't included, anyone in your school district can submit an application request at aka.ms/eduapprequest. For more information, see Windows 11 SE for Education.

Intune for Education supports two types of Windows apps: web apps and desktop apps. For more information, see Add desktop apps and Add web apps.

NOTE: You can prepare and add an app to Microsoft Intune as a Win32 app from the approved app list in Windows 11 SE.

With Intune for Education, you can specify the groups for which apps should be installed. Specifically, apps can be deployed by assigning them to security groups. If you select a security group containing users, the apps will be installed on any managed device that the user signs into. If you select a security group containing devices, the apps will be installed on those devices and available to any user who signs in. For more information, see Install apps for all users, and then return to this document to continue with the steps below.



	App type	Assigned	Last modified
Excel	Web app	No	10/12/2021, 5:17:17 AM
Fresh Paint	Microsoft Store app	No	5/26/2022, 5:31:26 PM
Microsoft Office	Microsoft Office Suite	No	6/6/2022, 12:02:22 PM
Microsoft Whiteboard	Microsoft Store app	No	5/26/2022, 5:23:47 PM
Minecraft: Education Edition	Microsoft Store app	No	5/26/2022, 5:31:25 PM
OneNote	Web app	No	10/12/2021, 5:17:17 AM
OneNote for Windows 10	Microsoft Store app	No	5/26/2022, 5:31:27 PM
PowerPoint	Web app	No	10/12/2021, 5:17:17 AM

NOTE: For additional details about setting up the device management environment and managing devices using Intune for Education, see Appendix: Device Management – Level 2 in this cookbook.

UP NEXT: After setting up the device management environment, it’s time to start enrolling devices.

Device enrollment

Enrolling large numbers of Windows 11 SE devices to Azure Active Directory and Intune for Education can help save time, effort, and cost. There are four methods for setting up Windows 11 SE devices and enrolling them in your education tenant:

- **Windows Autopilot.** Uses cloud-based technologies and services to set up and configure Windows devices with a zero-touch deployment approach. Windows Autopilot helps simplify the Windows device lifecycle, from initial deployment to end of life, for both IT administrators and end users. For more information, see Overview of Windows Autopilot.

  NOTE: There are some limitations to Windows Autopilot in Windows 11 SE. For more information, see Device settings.
- **Set Up School PCs app.** Configures devices with the apps and features students need, removing those they do not need. You create a provisioning package with the app and then automatically install the package to enroll devices into Intune for Education. For more information, see Use the Set Up School PCs app.
- **Windows Configuration Designer.** Configures end-user devices without imaging. Using Windows provisioning, you can specify the desired configuration for enrollment and then apply those settings to target devices in minutes. Windows Configuration Designer is best suited for small to medium schools with deployments that range from tens to a few hundred computers. It is offered as an app in the Microsoft Store. For more information, see Install Windows Configuration Designer.
- **Manual out-of-the-box experience (OOBE).** Requires the user's school credentials. This experience happens when a user first opens a new device preinstalled with Windows 11 SE. It enables the user to customize certain functionality before reaching the desktop. Keep in mind that when using the manual OOBE, there is a lack of support for the Device Firmware Configuration Interface (DFCI). In addition, users going through this flow will automatically become local administrators on their devices, which can cause management issues.

Choosing the best method

In this section of the cookbook, we review four methods for device enrollment. While all will work, Windows Autopilot and the Set Up School PCs app are usually easier, faster, and more efficient for school environments. There are various points to consider when choosing between Windows Autopilot and the Set Up School PCs app. This table describes the ideal scenarios for using either method. We recommend reviewing the table when making your enrollment and deployment plan. Also, note that DFCI management is not supported with Set Up School PCs enrollment.

Windows Autopilot

Windows Autopilot is especially useful in scenarios where devices are handed out to users without the need to build, maintain, and apply custom operating system images. These devices will be enrolled as school-owned devices.

A cloud-based provisioning technology, Windows Autopilot can be used to set up and preconfigure devices at the start of the school year. There's no need to wipe devices or use custom OS images. The device must be preregistered, and the enrollment profile created and assigned in Intune for Education. When users sign in with their school account, they are automatically enrolled.

NOTE: A fix for the known TPM attestation issue can now be addressed by using the latest Bare Metal Recovery (BMR) with 5b CU. For more information, see Support tip: Recovering from Windows Autopilot error code 0x81039023 on Windows 11 SE.

Prerequisites

Before setting up Windows Autopilot, consider these prerequisites:

- **Software requirements.** Ensure your school and devices meet the software, networking, licensing, and configuration requirements for Windows Autopilot.
- **Devices ordered and registered.** Ensure your school IT administrator or Microsoft partner has ordered the devices from an original equipment manufacturer (OEM) and registered them for the Autopilot deployment service. We recommend that you connect with a partner through the Microsoft Partner Center and work with them to register your devices.
- **Intune for Education tenant.** Ensure your tenant for Intune for Education is set up. We recommend configuring your tenant with School Data Sync, as this method automatically creates Student and Teacher groups for each school, as well as a combined Teacher and Student group. It also creates tenant-wide All Teachers and All Student groups.
- **Networking requirements.** Ensure students know to connect to the school network during OOBE setup. For more information on managing devices behind firewalls and proxy servers, see Network endpoints for Microsoft Intune.

NOTE: Where not explicitly specified, both HTTPS (443) and HTTP (80) must be accessible. If you are auto-enrolling your devices into Microsoft Intune or deploying Microsoft Office, follow the networking guidelines for Microsoft Intune and Microsoft 365.

Register devices to Windows Autopilot

Before deployment, devices must be registered with the Windows Autopilot deployment service. Each device's unique hardware identity (known as a *hardware hash*) is captured and uploaded to the Autopilot service, and the device is associated with an Azure tenant ID. There are three main ways to register devices to Autopilot:

- **Complete the OEM registration process.** When you purchase devices from an OEM, that company can automatically register them with Windows Autopilot. Before an OEM can register devices, your school must grant permission. The OEM begins this process with approval granted by an Azure AD global administrator from the school. For Microsoft Surface registration, collect the details shown in this documentation table before submitting the request to Microsoft Support. You can make requests using the Microsoft Devices Autopilot Support form.
- **Manually register devices with Windows Autopilot.** To manually register a device, you must first capture its hardware hash. Once this process has been completed, the hardware hash can be uploaded to the Windows Autopilot service using Microsoft Intune, Partner Center, Microsoft 365 Business & Office 365 Admin, or the Microsoft Store.

  NOTE: Windows 11 SE devices do not support the use of Windows PowerShell or Microsoft Configuration Manager to capture hardware hashes. Hardware hashes can only be captured manually. We recommend working with an OEM, partner, or device reseller to register devices. For more information, see Set up devices with Autopilot.
- **Allow a Cloud Solution Provider (CSP) to register devices.** Surface devices can be registered by device resellers (with active CSP partner status) as part of the ordering process. As with OEMs, CSP partners must be granted permission to register devices for a school. For more information, see this Microsoft Partner Center clickable demo. Then, return to this document to continue with the steps below.

Set up the devices

It's easy to set up Windows 11 SE devices with Windows Autopilot and Microsoft Endpoint Manager. First, you create a dynamic device group, and then you apply a Windows Autopilot deployment profile to each device in this group. Deployment profiles determine the deployment mode and customize the OOBE for your end users.

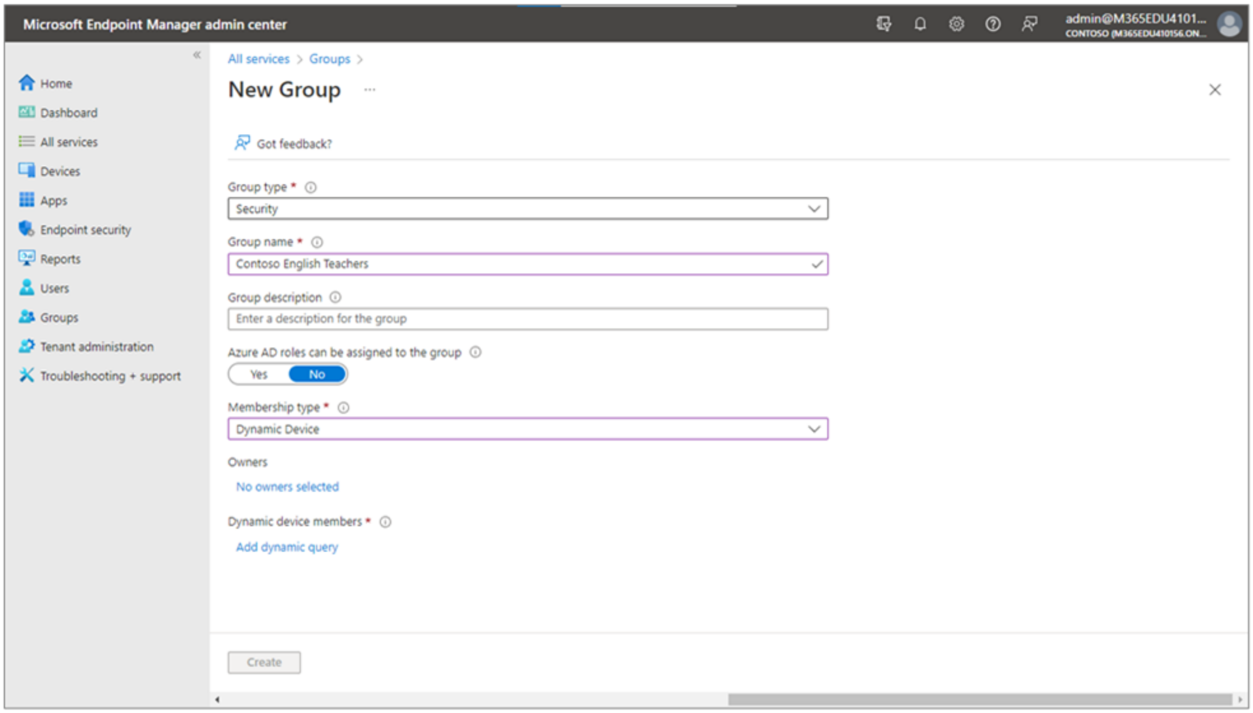
Create a dynamic device group

Dynamic groups reference rules that you create to assign devices to groups. The criteria for a rule are specified during initial group creation and can be edited afterward. A device group is required to assign a Windows Autopilot deployment profile. You can create a group with a dynamic membership rule using Autopilot device attributes. Autopilot devices that meet these rules are automatically added to the group.

The steps for creating a dynamic device group are completed in Microsoft Endpoint Manager:

1. Go to the Microsoft Endpoint Manager admin center, and then select **Groups** → **New Group**.
2. Configure the following properties:

   - **Group type**: Select **Security**.
   - **Group name/Group description**: Enter a valid name and description for your group.
   - **Azure AD roles can be assigned to the group**: Select **Yes**. This allows Azure AD roles to be assigned to the group you are creating. Once set, the group is permanent and always allowed to be assigned Azure AD roles. For more information, see Use Azure AD groups to manage role assignments.
   - **Membership type**: Select **Dynamic Device**. This property allows you to choose how devices become members of this group. For more information, see Add groups to organize users and devices.
   - **Owners**: Select users who own this group. Owners can also delete the group.
   - **Dynamic device members**: Select **Add dynamic query** → **Add expression**.



New Group

Group type *
Security

Group name *
Contoso English Teachers

Group description
Enter a description for the group

Azure AD roles can be assigned to the group
Yes [✓ No]

Membership type *
Dynamic Device

Owners
No owners selected

Dynamic device members *
Add dynamic query

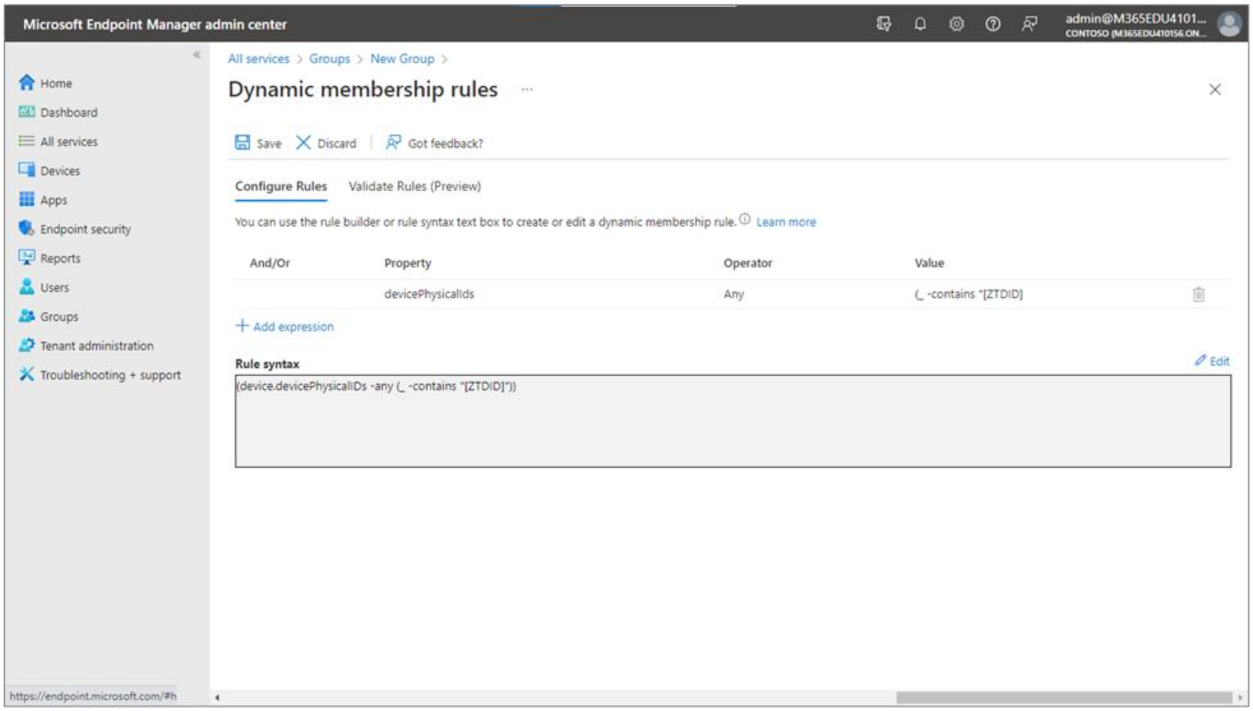
Create rules using Autopilot device attributes

Autopilot devices that meet the rules are automatically added to the group. Note that creating an expression using non-Autopilot attributes does not guarantee that devices included in the group are registered to Autopilot.

The following steps will create a dynamic device group that uses the query expression defined in the rule.

1. Create expressions, as desired:

   - To create a group that includes all your Autopilot devices, enter **(device.devicePhysicalIDs -any (_ -contains "[ZTDID]"))**.
   - The Intune group tag field maps to the OrderID attribute on Azure AD devices. To create a group that includes all Autopilot devices with a specific group tag (the Azure AD device OrderID), enter **(device.devicePhysicalIds -any (_ -eq "[OrderID]:179887111881"))**.
   - To create a group that includes all your Autopilot devices with a specific Purchase Order ID, enter **(device.devicePhysicalIds -any (_ -eq "[PurchaseOrderId]:76222342342"))**.



Dynamic membership rules

You can use the rule builder or rule syntax text box to create or edit a dynamic membership rule.

And/Or	Property	Operator	Value
	devicePhysicallds	Any	(_ -contains "[ZTDID]

Rule syntax

```
(device.devicePhysicalIDs -any (_ -contains "[ZTDID]"))
```

2. Save your expressions.
3. Select **Create**.

Create an Autopilot deployment profile

Once the dynamic device group is created, it can be used for assigning Windows Autopilot deployment profiles. These profiles are used to configure Autopilot devices.

1. In the Microsoft Endpoint Manager admin center, choose **Devices** → **Windows** → **Windows enrollment** → **Deployment Profiles** → **Create Profile** → **Windows PC**.

2. On the **Basics** page:

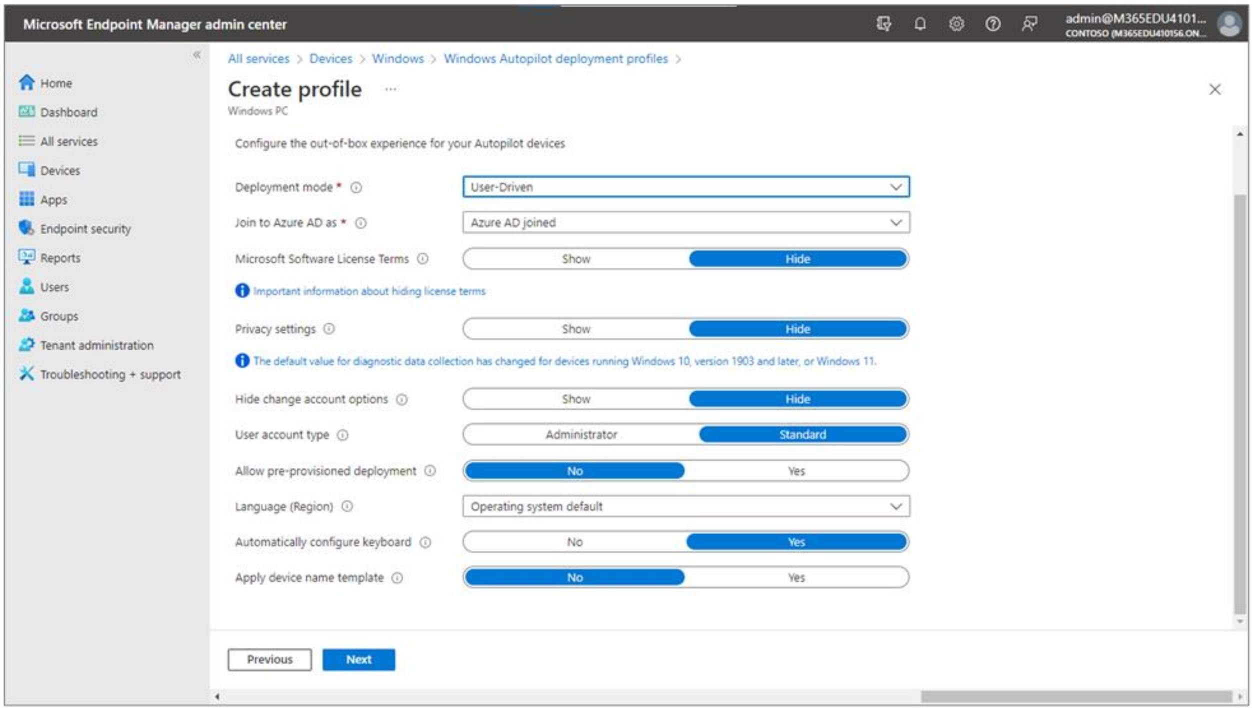
   - Enter a **Name** and optional **Description**.
   - If you want all devices in the assigned groups to convert to Autopilot automatically, for **Convert all targeted devices to Autopilot**, select **Yes**.

3. On the **Out-of-box experience** page, for **Deployment** mode, choose one option:

   - **User-driven**: Devices with this profile are associated with the user enrolling the device. User credentials are required to enroll the device.
   - **Self-deploying**: Devices with this profile are not associated with the user enrolling the device. User credentials are not required to enroll the device. When a device has no user associated with

it, user-based compliance policies do not apply. When using self-deploying mode, only compliance policies targeting the device will be applied.

4. In the **Join to Azure AD** field, choose **Azure AD joined**.


Microsoft Endpoint Manager admin center
admin@M365EDU4101...
CONTOSO (M365EDU410156.ON...
Home
Dashboard
All services
Devices
Apps
Endpoint security
Reports
Users
Groups
Tenant administration
Troubleshooting + support
All services > Devices > Windows > Windows Autopilot deployment profiles >
Previous
Next

Create profile

Windows PC

Configure the out-of-box experience for your Autopilot devices

Deployment mode * : User-Driven

Join to Azure AD as * : Azure AD joined

Microsoft Software License Terms: Show [✓ Hide]

Important information about hiding license terms

Privacy settings: Show [✓ Hide]

The default value for diagnostic data collection has changed for devices running Windows 10, version 1903 and later, or Windows 11.

Hide change account options: Show [✓ Hide]

User account type: Administrator [✓ Standard]

Allow pre-provisioned deployment: [✓ No] Yes

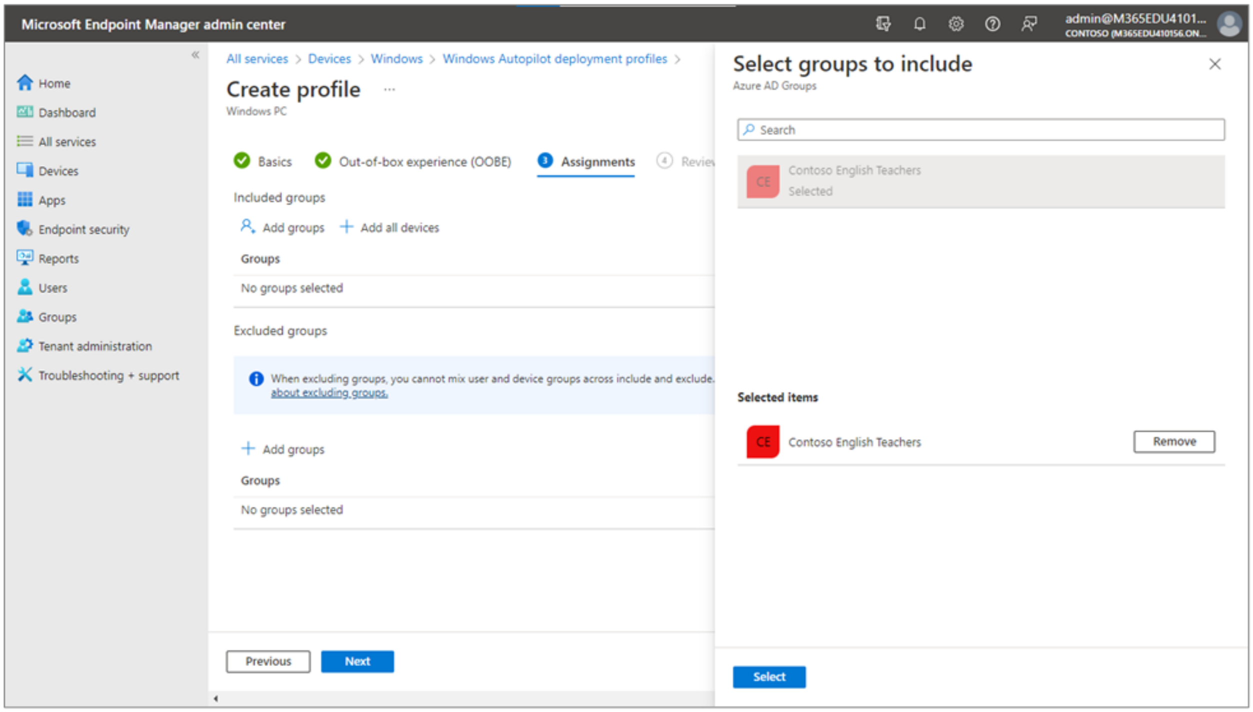
Language (Region): Operating system default

Automatically configure keyboard: No [✓ Yes]

Apply device name template: [✓ No] Yes

5. On the **Assignments** page:

- Choose **Select groups to include**, and then choose the groups you want to include in this profile.
- If a group is not showing in the group list, select **Add groups**, and then select the desired group. In this case, you will select the dynamic device group you created above in Create a dynamic device group.



When excluding groups, you cannot mix user and device groups across include and exclude. about excluding groups.

6. On the **Review + create** page, select **Create** to generate the profile.

For more information, see Configure Autopilot profiles, and then return to this document to continue with the steps below.

Set up the Enrollment Status Page

With the deployment profile completed, you're ready to define the Enrollment Status Page (ESP), which is a greeting page for users signing in and enrolling Windows 11 SE devices. The ESP displays provisioning progress and shows app and profile installation status during device setup. Only Windows 11 SE-approved apps should be included as part of the ESP configuration and targeted to Windows 11 SE devices.

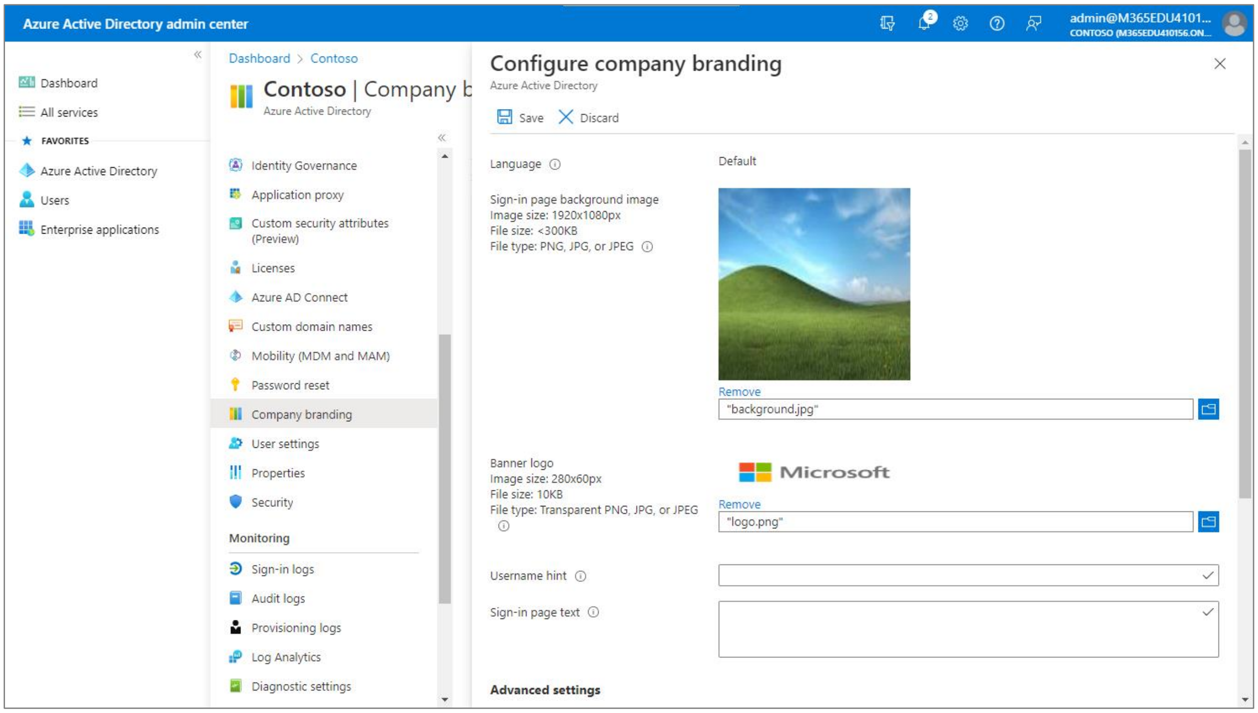
To deploy the ESP to devices, you need to create an ESP profile in Microsoft Endpoint Manager. For a complete list of steps on setting up the ESP in Intune for Education, see Set up the Enrollment Status Page, and then return to this document to continue with the steps below.

Configure school branding

Configuring your school branding helps customize the look and feel of the Autopilot process, which makes the experience more familiar to students and teachers. For your school branding to appear during OOBE, you need to configure it in Azure Active Directory. For more information, see Add branding to your directory.

To configure your school branding:

1. In the Azure Active Directory admin center, select **Azure Active Directory → Company branding → Configure**. You can specify brand settings like background image, banner logo, square logo, and square logo dark.



Configure company branding
Azure Active Directory

Language: Default

Sign-in page background image
Image size: 1920x1080px
File size: <300KB
File type: PNG, JPG, or JPEG
"background.jpg"

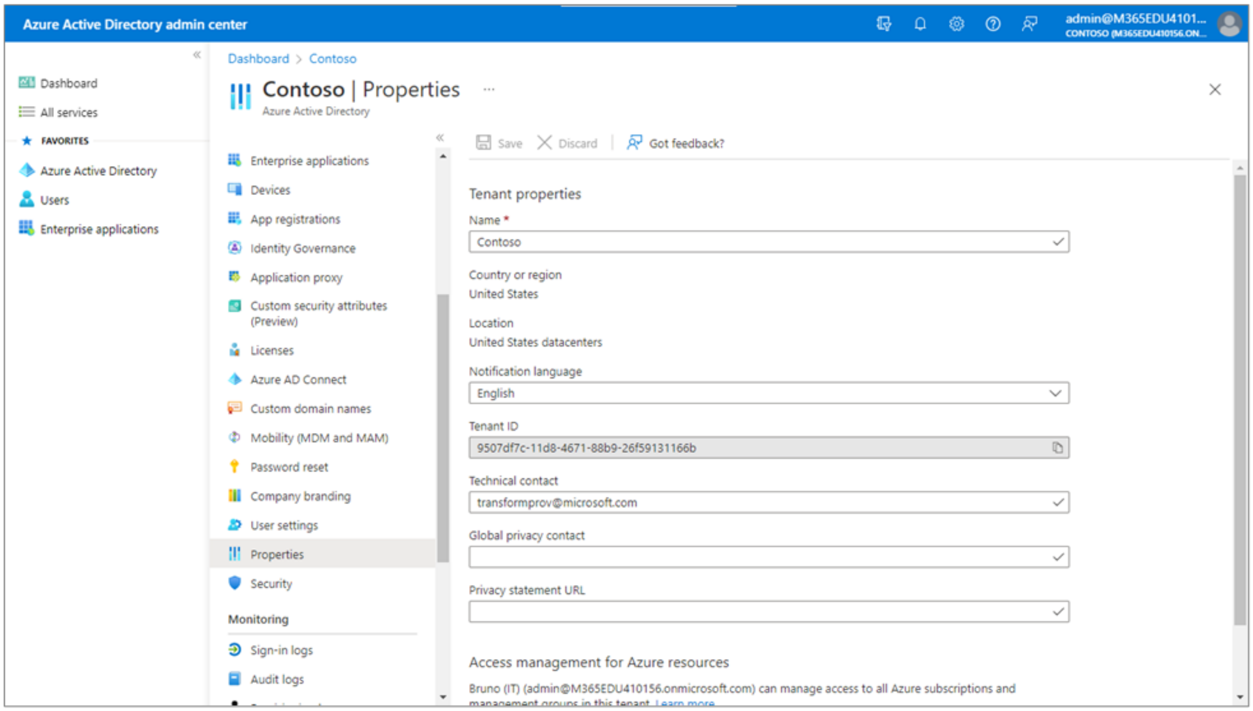
Banner logo
Image size: 280x60px
File size: 10KB
File type: Transparent PNG, JPG, or JPEG
"logo.png"

Username hint

Sign-in page text

Advanced settings

2. To adjust the school tenant's name displayed during OOBE, select **Azure Active Directory → Properties**.
3. In the **Name** field, enter the tenant's name, and then select **Save**.



Tenant properties

Name *: Contoso

Country or region: United States

Location: United States datacenters

Notification language: English

Tenant ID: 9507df7c-11d8-4671-88b9-26f59131166b

Technical contact: transformprov@microsoft.com

Global privacy contact:

Privacy statement URL:

Access management for Azure resources

Bruno (IT) (admin@M365EDU410156.onmicrosoft.com) can manage access to all Azure subscriptions and management groups in this tenant. Learn more

Autopilot end-user experience

Once configuration is complete and devices are distributed, students and teachers are able to complete device setup with Autopilot. They can set up their devices at home, at school, or wherever there is a reliable network. After a user turns on the device and signs in with their school account, enrollment automatically starts.

When a Windows 11 SE device is turned on for the first time, the end-user experience with Windows Autopilot using a Wi-Fi connection is as follows:

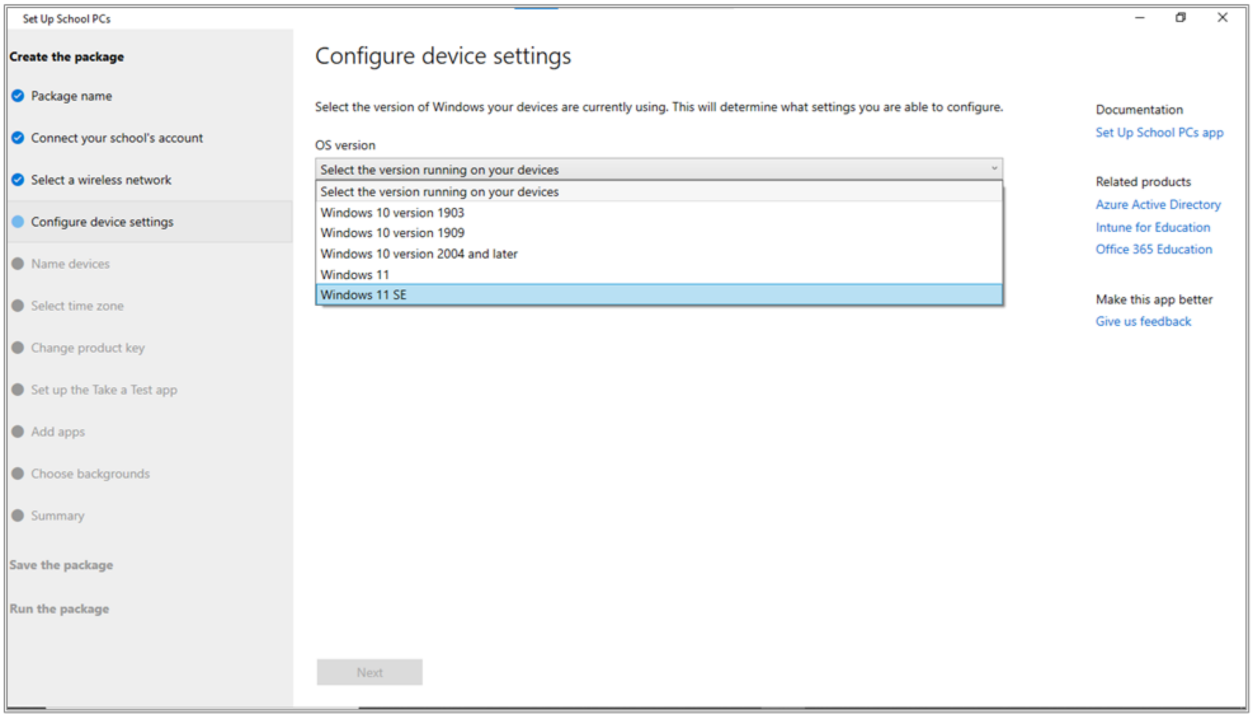
1. Identify the language and region.
2. Select the keyboard layout and decide on the option for a second keyboard layout.
3. Connect to the internet. Windows will verify network connectivity to the internet. If connecting through Wi-Fi, the user will be prompted to connect to a wireless network. If the device is connected through an ethernet cable, Windows will skip this step.
4. Wait for detection. Windows will detect that the device has an Autopilot profile assigned and belongs to your school.
5. Enter the email address and password associated with your school account.
6. Apply updates. Once connected, the Windows 11 SE device will look for and apply required updates.
7. Sign in on the school-branded welcome screen. Users need only their school account credentials. No local administrator permissions are required.

Set Up School PCs app

The Set Up School PCs app is especially useful in scenarios where large numbers of school-owned devices need to be enrolled. The app helps you configure Surface Laptop SE devices with the features students need, remove those they do not need, and enroll the devices into Intune for Education. With the Set Up School PCs app, you create a provisioning package to enroll devices using a USB drive. For more information on prerequisites, configuration, and recommendations, see Use the Set Up School PCs app. Then, return to this document to continue with the steps below.

Create the provisioning package

The Set Up School PCs app guides you through configuration choices for school-owned devices. Review the Set Up School PCs demo to step through how to create provisioning packages and save them to USB.



Configure device settings

Select the version of Windows your devices are currently using. This will determine what settings you are able to configure.

OS version

Select the version running on your devices

- Select the version running on your devices
- Windows 10 version 1903
- Windows 10 version 1909
- Windows 10 version 2004 and later
- Windows 11
- Windows 11 SE

NOTE: Importantly, for **Configure device settings → OS version**, you must select **Windows 11 SE**.

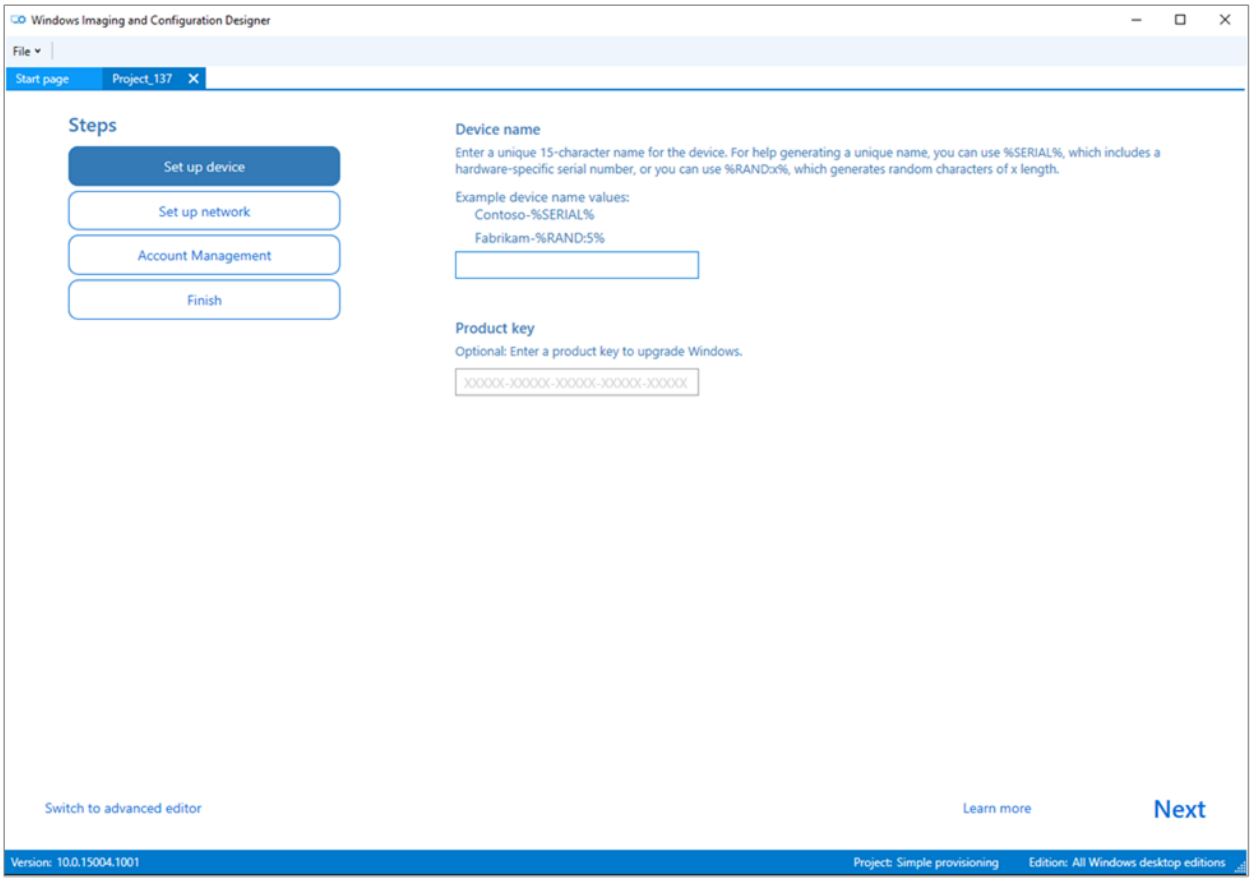
The devices will be joined to Azure Active Directory and automatically enrolled in Intune. Note that the Set Up School PCs app will configure many settings, allowing you to optimize devices for shared use and other scenarios.

Provision devices with USB

To provision Surface Laptop SE devices with USB, insert the provisioning package saved to USB during manual OOBE. For more information, see Run package - Install package on PC, which steps through running and installing the provisioning package.

Windows Configuration Designer

Windows Configuration Designer is especially useful in scenarios where a school needs to provision packages for both bring-you-own devices and school-owned devices. Ideal for small-to-medium schools that manage up to a few hundred devices, Windows Configuration Designer lets you configure devices without imaging. For more information, see Install Windows Configuration Designer, which provides details about the app, its provisioning process, and considerations for its use.



Device name

Enter a unique 15-character name for the device. For help generating a unique name, you can use %SERIAL%, which includes a hardware-specific serial number, or you can use %RAND:x%, which generates random characters of x length.

Example device name values:
Contoso-%SERIAL%
Fabrikam-%RAND:5%

Product key

Optional: Enter a product key to upgrade Windows.

XXXXX-XXXXX-XXXXX-XXXXX-XXXXX

Version: 10.0.15004.1001 Project: Simple provisioning Edition: All Windows desktop editions

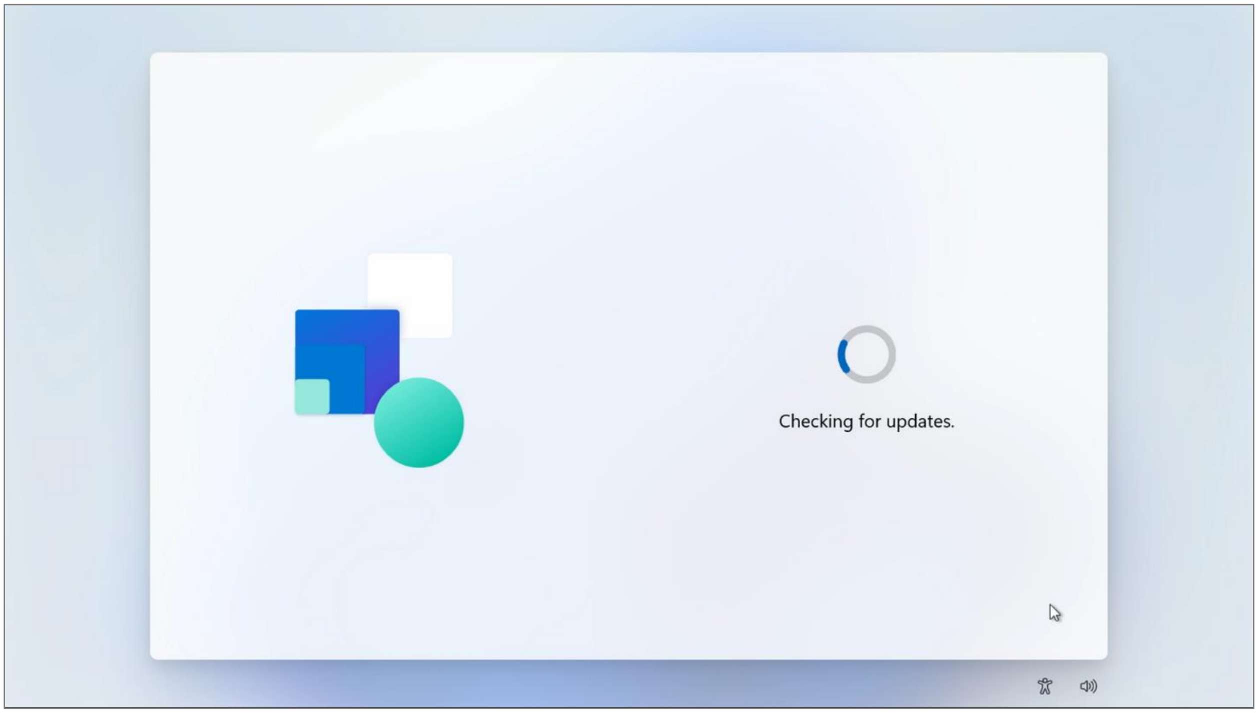
Manual OOBE

If you are setting up a Windows 11 SE device individually and network bandwidth is not an issue, you can use the out-of-the-box, first-run setup experience to configure the device, join it to your school's Azure Active Directory account, and enroll it in Intune.

Configure, join, and enroll devices

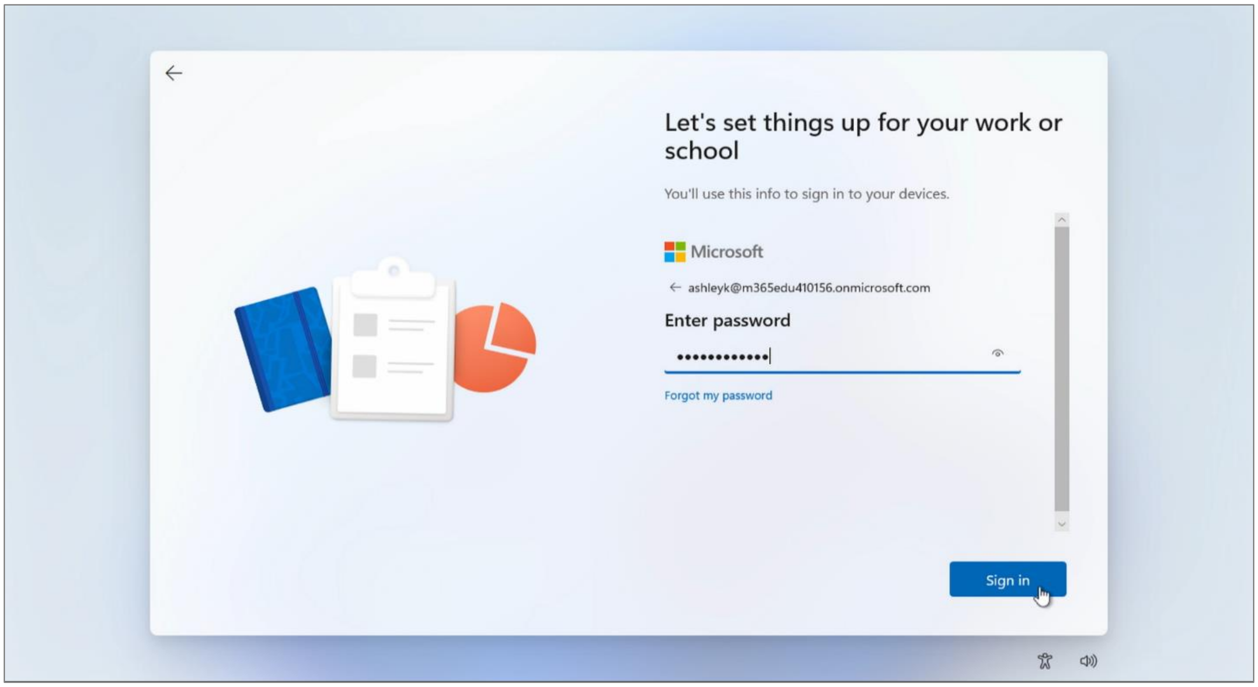
When using OOBE, no advance preparation is needed:

1. Follow the on-screen prompts for region selection, keyboard selection, and network connection.
2. Wait for updates. If any updates are available, they will be installed at this time.



Checking for updates.

3. When prompted, select **Work or School Account**. This will deploy Windows 11 SE to the device within a few minutes.



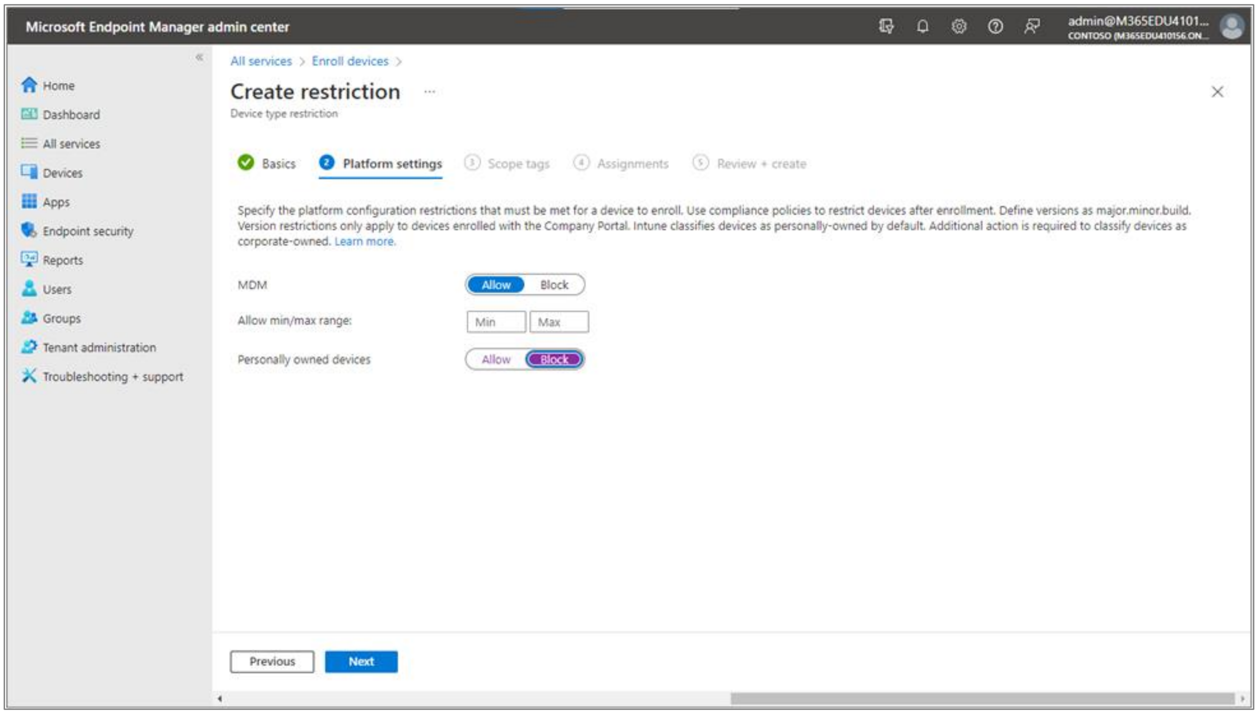
Let's set things up for your work or school

You'll use this info to sign in to your devices.

Set enrollment restrictions for personally owned devices

To block personally owned devices from enrolling, use restrictions for device platform and OS version.

1. In the Microsoft Endpoint Manager admin center, select **Devices** → **Enroll devices** → **Enrollment device platform restrictions**.
2. Select the Windows tab you are configuring, and then select **Create restriction**.
3. On the **Basics** page, give the restriction a name and optional description.
4. On the **Platform settings** page, in the **Personally owned devices** field, select **Block**.



Create restriction

Device type restriction

Specify the platform configuration restrictions that must be met for a device to enroll. Use compliance policies to restrict devices after enrollment. Define versions as major.minor.build. Version restrictions only apply to devices enrolled with the Company Portal. Intune classifies devices as personally-owned by default. Additional action is required to classify devices as corporate-owned. Learn more.

MDM: [✓ Allow] Block

Allow min/max range: Min Max

Personally owned devices: Allow [✓ Block]

5. Optionally, on the **Scope tags** page, add scope tags to the restriction.
6. On the **Assignments** page, select **Add groups**, and then use the search box to find and choose groups.
7. To assign the restriction to all device users, select **Add all users**.
8. On the **Review + create**, select **Create** to save the restriction.

For more information, see [Create a device platform restriction](#).

Device reset

When a device is lost, stolen, or needs to be replaced, or when a user moves to another position, it is usually time to wipe or reset the device. There are several ways you can do this—including resetting the device, removing it from management, or wiping the personal and school data on it. In scenarios where a device needs to be exchanged or returned, additional steps are required to prepare the device and then send it for repair. With Intune, IT administrators can remotely execute all these actions for device reset.

Resetting a device

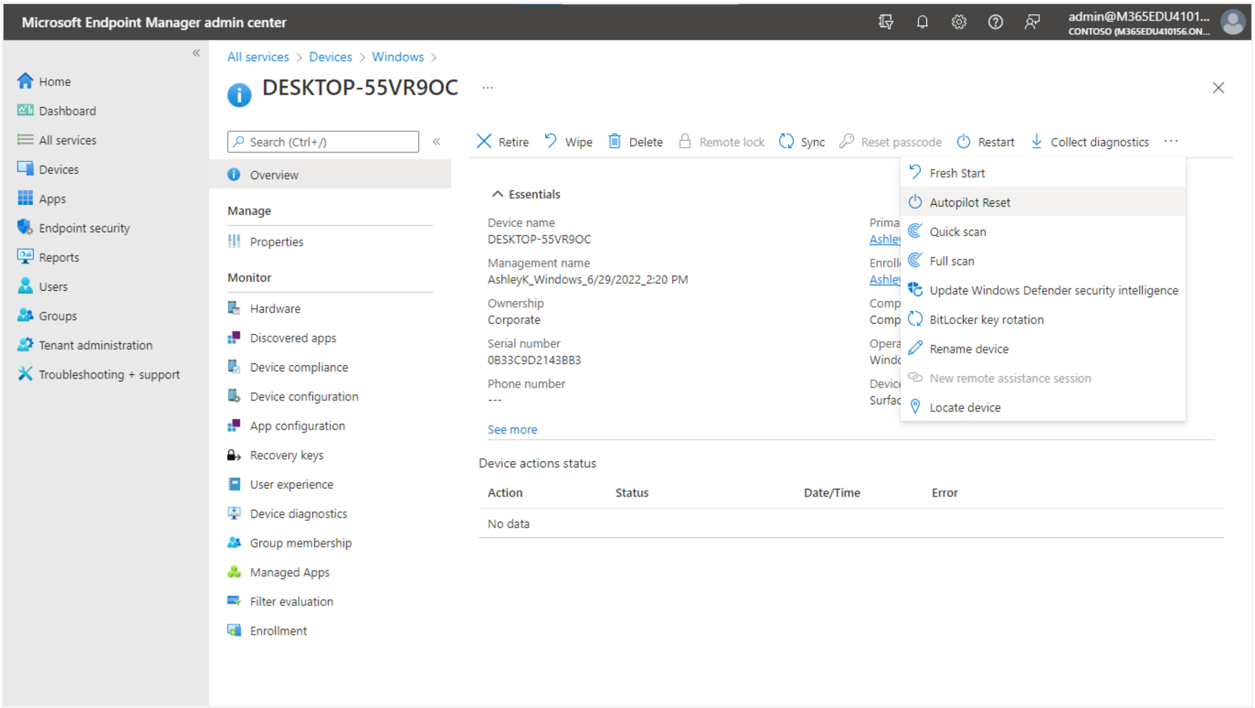
Two Reset Device actions can be used to reset and deregister student devices in preparation for next year: Autopilot Reset and factory reset. With Autopilot Reset, you return the device to a fully configured or known IT-approved state. With factory reset, you wipe all personal and school data and settings from the device, returning it to the default factory settings.

Autopilot Reset

This reset action is ideal when all data on a device needs to be wiped, but the device will remain enrolled in your school. You can use Autopilot Reset to remove personal files, apps, and settings; reset Windows 11 SE devices from the lock screen; and apply original Intune settings and management enrollment (Azure Active Directory and device management).

With Intune for Education, wiping can be performed remotely:

1. In Intune for Education, choose **Groups** → **Choose a device group**.
2. Choose a device, and then select **Autopilot Reset**.
3. To confirm the reset, select **Autopilot Reset** again. A message appears when the reset is initiated. The device will reset the next time it connects to the Internet.



Device name
DESKTOP-55VR9OC

Management name
AshleyK_Windows_6/29/2022_2:20 PM

Ownership
Corporate

Serial number
0B33C9D2143BB3

Phone number

Device actions status

Action	Status	Date/Time	Error
No data			

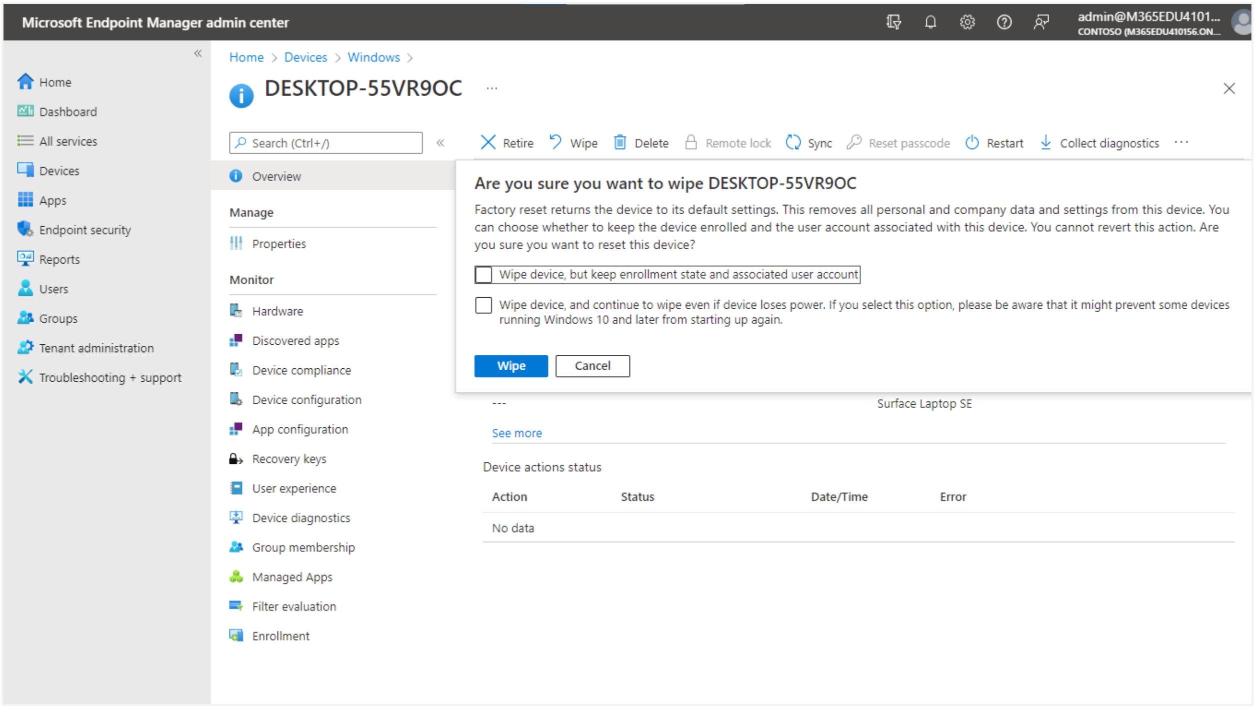
Factory reset (wipe)

A factory reset, or a wipe, reverts a device to the original settings when it was purchased. All apps and data installed on the device after purchase are removed. The device is also removed from Intune management, and all data and settings are wiped from the device.

To perform a factory reset:

1. In Microsoft Endpoint Manager, go to **Devices** → **Windows devices** to view all enrolled devices.
2. Choose the device you want to reset, and on the next screen, select **Wipe**.

   NOTE: We recommend keeping the enrollment state and associated user account. This option ensures that the Wipe action cannot be circumvented by turning off the device.
3. Select **Yes** to reset the device to its factory defaults and delete the Intune object.



Are you sure you want to wipe DESKTOP-55VR9OC

Factory reset returns the device to its default settings. This removes all personal and company data and settings from this device. You can choose whether to keep the device enrolled and the user account associated with this device. You cannot revert this action. Are you sure you want to reset this device?

☐ Wipe device, but keep enrollment state and associated user account

☐ Wipe device, and continue to wipe even if device loses power. If you select this option, please be aware that it might prevent some devices running Windows 10 and later from starting up again.

Wipe | Cancel

Device actions status

Action	Status	Date/Time	Error
No data			

Wiping and removing a device

With this action, a device's data is wiped, and the device is removed from the school deployment. This action should only be performed for devices that are no longer going to be used. To completely remove a device, you need to perform two actions:

1. Perform a factory reset (wipe) on the device.
2. Complete one of the following actions, depending on Intune enrollment:

   - If the device is not enrolled in Intune, delete it from Autopilot.
   - If the device is enrolled in Intune, delete it from Microsoft Endpoint Manager. (This removes device records from Intune, Azure AD, and Autopilot).

Delete a device from Autopilot

To delete Autopilot devices that are not enrolled in Intune:

1. In Windows Autopilot, go to **Devices** → **Windows** → **Windows enrollment**.
2. Under Windows Autopilot Deployment Program, select **Devices**.
3. Choose the device you want to delete, and then select **Delete**. Note that device deletion can take a few minutes to complete.

Delete a device using Intune

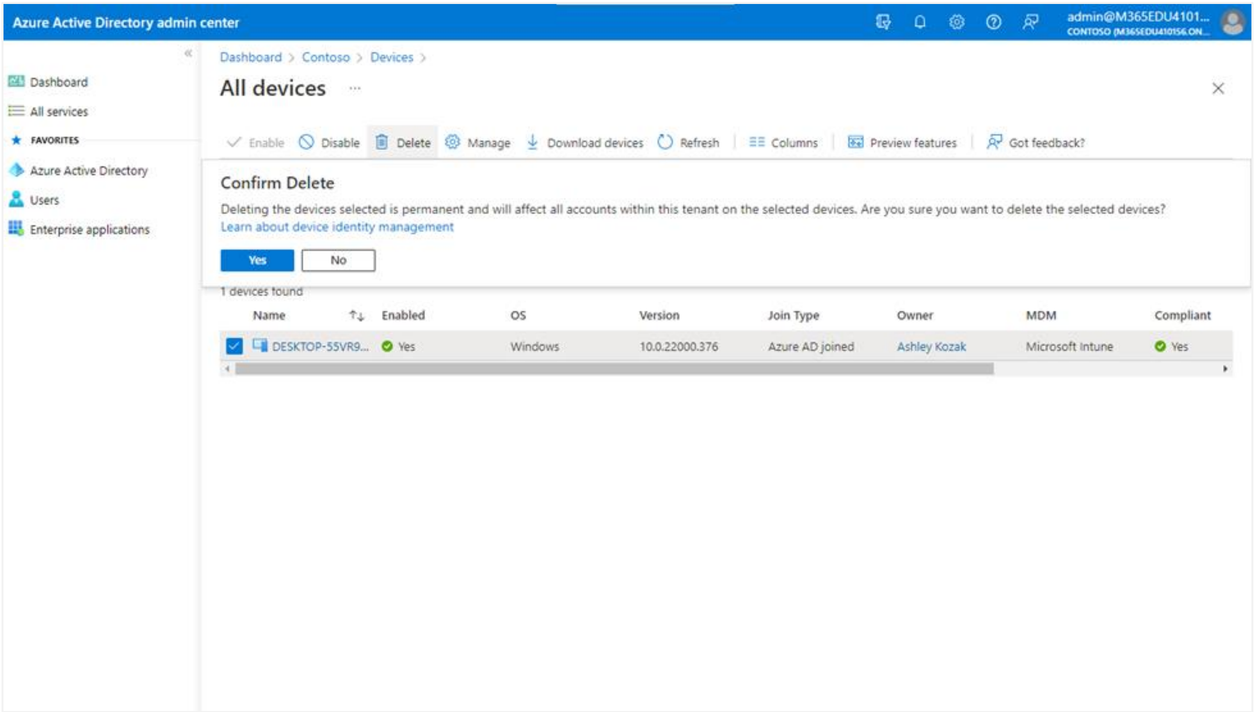
To delete devices that are enrolled in Intune:

1. Delete the device from the **All devices** blade in Microsoft Endpoint Manager:

   - Sign in to the Microsoft Endpoint Manager admin center.
   - Select **Devices** → **All devices**.
   - Choose the device you want to delete, and then select **Delete**.

2. Delete the device from Azure Active Directory:

   - From the Azure portal, sign in to Azure Active Directory.
   - Select **Devices** → **Azure AD devices**.
   - Follow the steps outlined in Delete devices from the Azure Active Directory portal.



All devices

Confirm Delete

Deleting the devices selected is permanent and will affect all accounts within this tenant on the selected devices. Are you sure you want to delete the selected devices?
Learn about device identity management

1 devices found

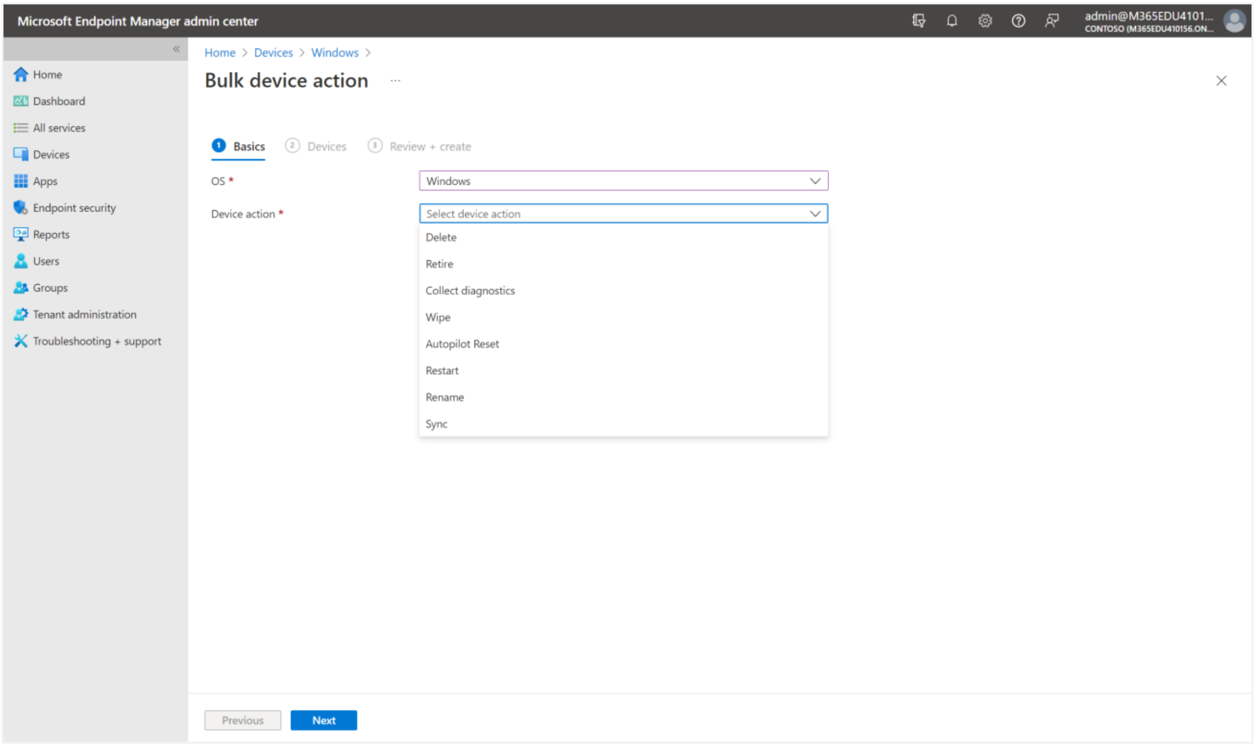
	Name	Enabled	OS	Version	Join Type	Owner	MDM	Compliant
☑	DESKTOP-55VR9...	✓ Yes	Windows	10.0.22000.376	Azure AD joined	Ashley Kozak	Microsoft Intune	✓ Yes

Other device actions

The following list includes some everyday actions you can perform on school devices. To see a complete list of what can be done on which device, simply select **All devices** and choose a specific device.

- Autopilot Reset
- BitLocker Key Rotation
- Collect Diagnostics

- Delete
- Fresh Start
- Full Scan
- Quick Scan
- Rename Device
- Restart
- Update Windows Defender Security Intelligence
- Lost Mode
- Wipe
- Synchronize Device



Bulk device action

OS * Windows

Device action * Select device action

Autopilot motherboard replacement

Repairing Autopilot-enrolled devices can be complex, as OEM requirements must be balanced with Autopilot requirements. If a motherboard replacement is needed on an Autopilot device, we recommend the following process:

1. Deregister the device from Autopilot.
2. Replace the motherboard.
3. Capture a new device ID (4K HH).

4. Reregister the device with Autopilot. **NOTE:** For DFCI management, the device must be reregistered by a partner or OEM. Self-registration of devices is not supported with DFCI management.
5. Reset the device.
6. Return the device.

For more information, see Autopilot motherboard replacement scenario guidance.

UP NEXT: By this point in the cookbook, you have reviewed the basic steps for full device lifecycle management. In the next section, we'll look at some advanced Intune capabilities that can help support your device management needs today and into the future.

Advanced capabilities

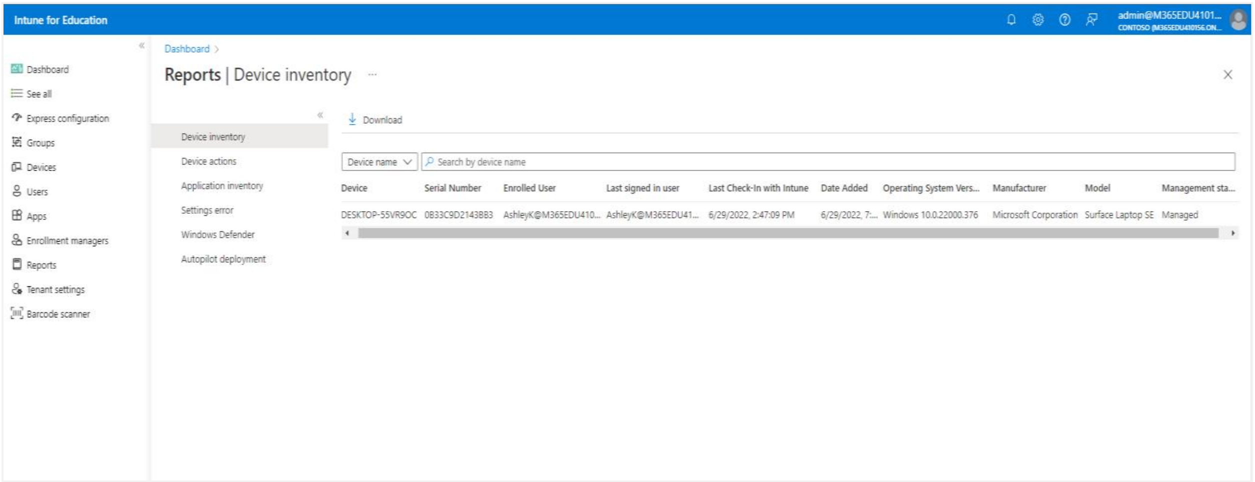
This section of the cookbook provides information about the advanced capabilities in Intune for Education for device management, reporting, security, and support.

Device management and reporting

As an IT administrator, you can view current devices, applications, settings, and overall health in Microsoft Endpoint Manager. You can also download reports to review or share offline.

To access, view, and download reports:

1. Go Microsoft Endpoint Manager, and then select **Reports**.



Device	Serial Number	Enrolled User	Last signed in user	Last Check-In with Intune	Date Added	Operating System Vers...	Manufacturer	Model	Management sta...
DESKTOP-55VR9OC	0B33C9D2143BB3	AshleyK@M365EDU410...	AshleyK@M365EDU41...	6/29/2022, 2:47:09 PM	6/29/2022, 7:...	Windows 10.0.22000.376	Microsoft Corporation	Surface Laptop SE	Managed

2. Review the desired reports. For more information about common reports, see:

   Device inventory

   Device actions

   Application inventory

   Settings errors

   Windows Defender

   Autopilot deployment

3. If needed, use the search box to find specific devices, applications, and settings.
4. To download a report, select **Download**. The report will download as a comma-separated value (CSV) file, which you can view and modify in a spreadsheet app like Microsoft Excel.

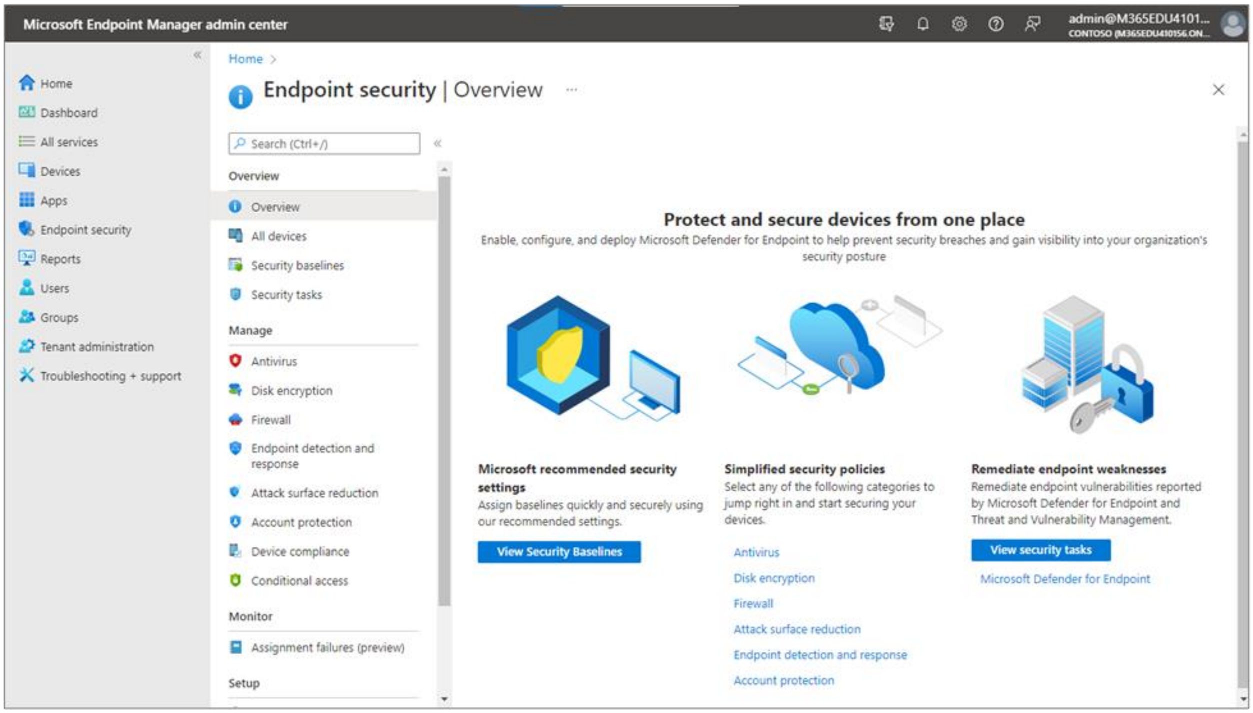
Endpoint security

Intune for Education helps protect devices and school data with tools like security baselines and Windows Update policies. Through the Endpoint security node, you can configure device security and manage security tasks for devices at risk. The node configures and deploys Microsoft Defender for Endpoint to help prevent security breaches and gain visibility into your school's security posture.

Create security policies

To create security policies in Intune for Education:

1. In the Microsoft Endpoint Manager admin center, select the **Endpoint security** node.
2. Under **Manage**, choose the policies you want to set from the included list. For more information, see Antivirus, Disk encryption, Firewall, Endpoint detection and response, Attack surface reduction, and Account protection.
3. Select **Create policy**. For more information, see Creating an endpoint security policy.



Protect and secure devices from one place

Enable, configure, and deploy Microsoft Defender for Endpoint to help prevent security breaches and gain visibility into your organization's security posture

Microsoft recommended security settings
Assign baselines quickly and securely using our recommended settings.

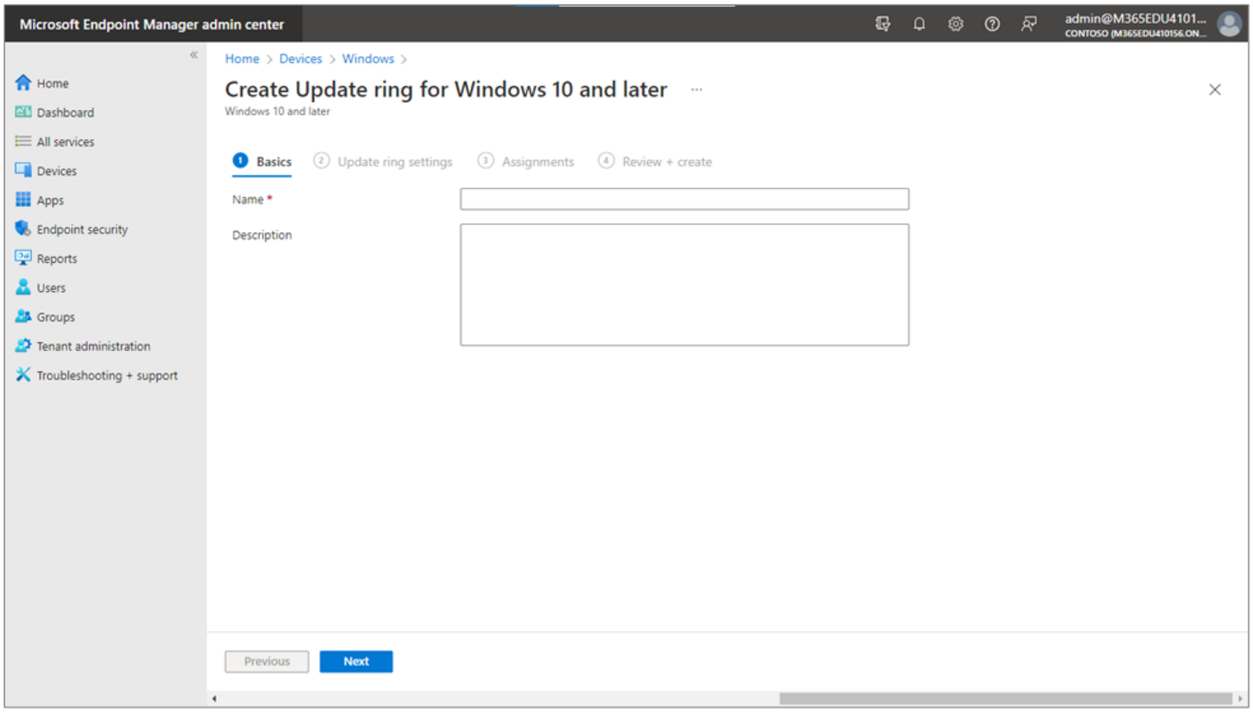
Simplified security policies
Select any of the following categories to jump right in and start securing your devices.

Remediate endpoint weaknesses
Remediate endpoint vulnerabilities reported by Microsoft Defender for Endpoint and Threat and Vulnerability Management.

Create Windows Update policies

Create update rings that specify how and when feature and quality updates are applied to your Windows 10 and later devices. With Windows 11 SE, new features and quality updates include the content of all previous updates. If you have installed the latest update, you know your Windows devices are up to date.

1. In the Microsoft Endpoint Manager admin center, select **Devices → Windows → Update rings for Windows 10 and later → Create Profile**.



2. Under **Basics**, specify a name and description (optional).
3. Under **Update ring settings**, configure settings for your school needs. For more information, see Windows Update settings and Creating and assigning update rings.

NOTE: You can also create expedited quality updates for Windows 10 and later. This policy lets you expedite the installation of the most recent Windows security updates on Intune-managed devices. For more information, see Create and assign an expedited quality update.

Managing DFCI profiles in Surface Laptop SE

Managing devices from the cloud has dramatically simplified IT deployment and provisioning. Surface devices are designed to use a unique Unified Extensible Firmware Interface (UEFI) setting that provides the ability to enable or disable built-in devices and components, protect UEFI settings from being changed, and adjust device boot settings. With Device Firmware Configuration Interface profiles built into Intune, Surface UEFI management extends the modern management stack down to the UEFI hardware level. DFCI enables Windows to pass management commands from Intune to UEFI for Autopilot-deployed devices. DFCI also supports zero-touch provisioning, eliminates BIOS passwords, and provides control of security settings for boot options, cameras and microphones, built-in peripherals, and more. For more information, see Manage DFCI with Windows Autopilot and Manage DFCI on Surface devices. Then, return to this document to continue with the steps below.

Prerequisites

The following prerequisites are required to manage DFCI with Intune:

- The device must be managed with Intune, as DFCI management is not supported with Set Up School PCs (provisioning package) enrollments. For more information, see DFCI Management.
- The device should be registered through Windows Autopilot in Intune. The device must be registered for Windows Autopilot by a Microsoft CSP partner or registered directly by the OEM. **NOTE:** Devices manually registered for Autopilot (such as by importing a CSV file) are not allowed to use DFCI. By design, DFCI management requires external attestation of the device's commercial acquisition through an OEM or a Microsoft CSP partner registration to Windows Autopilot.
- The device manufacturer must have DFCI added to their UEFI firmware in the manufacturing process or as a firmware update that you install. Work with your device vendors to determine the manufacturers that support DFCI.

Manage DFCI profiles with Autopilot

There are four basic parts to managing a DFCI profile with Windows Autopilot:

- Create a DFCI profile.
- Create an Autopilot profile.
- Create an enrollment status profile.
- Configure DFCI settings on Surface devices.

The DFCI environment requires creating a DFCI profile that contains settings and an Autopilot profile to apply those settings to registered devices. An enrollment status profile is also recommended to ensure settings are pushed down during OOBE setup when users start the device.

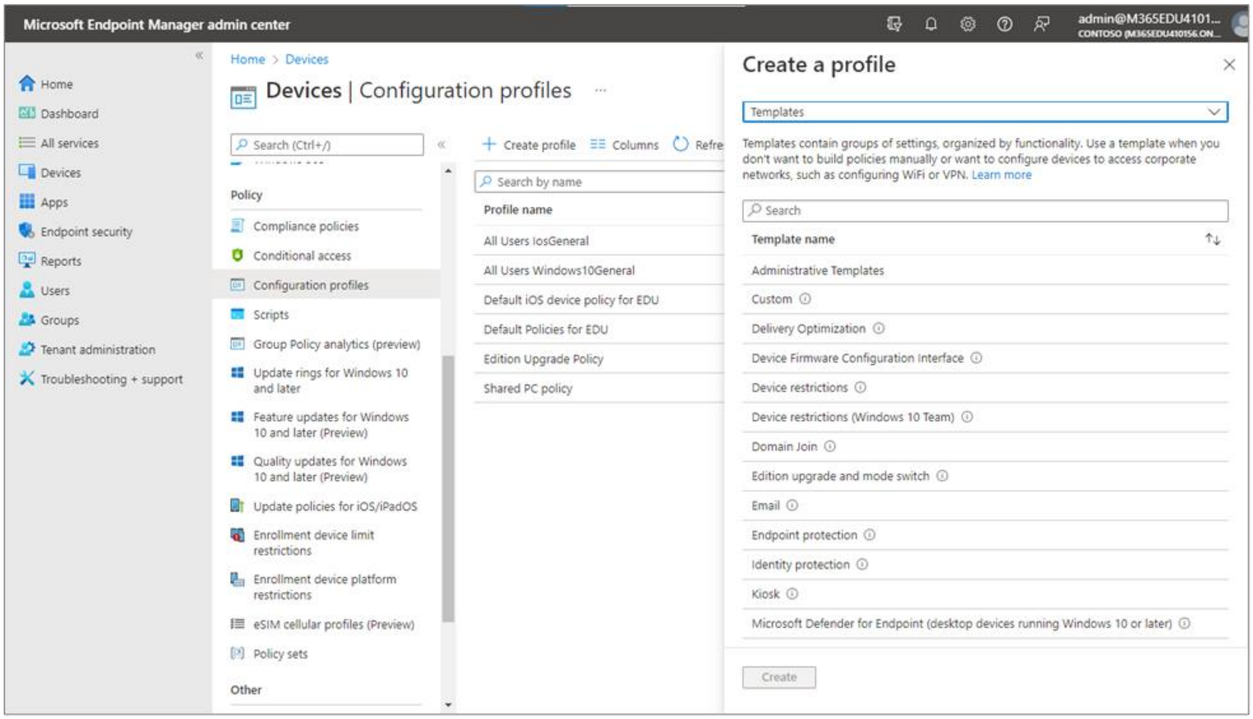
Create a DFCI profile

Create a DFCI profile, and then assign it to the Azure AD security group that contains your targeted Surface devices:

1. In Microsoft Endpoint Manager, select **Devices** → **Configuration profiles** → **Create profile**.
2. In the **Create a profile** pane:

    - For the platform, select **Windows 10 and later**.

- For the profile type, select **Templates**, and then select **Device Firmware Configuration Interface**.
- Enter a name and description for the profile.


Microsoft Endpoint Manager admin center
admin@M365EDU4101...
CONTOSO (M365EDU410156.ON...
Home
Dashboard
All services
Devices
Apps
Endpoint security
Reports
Users
Groups
Tenant administration
Troubleshooting + support
Home > Devices
Devices | Configuration profiles
Search (Ctrl+/)
Policy
Compliance policies
Conditional access
Configuration profiles
Scripts
Group Policy analytics (preview)
Update rings for Windows 10 and later
Feature updates for Windows 10 and later (Preview)
Quality updates for Windows 10 and later (Preview)
Update policies for iOS/iPadOS
Enrollment device limit restrictions
Enrollment device platform restrictions
eSIM cellular profiles (Preview)
Policy sets
Other
Create profile
Columns
Refre
Search by name
Create a profile
Templates
Search
Create

Profile name
All Users IosGeneral
All Users Windows10General
Default iOS device policy for EDU
Default Policies for EDU
Edition Upgrade Policy
Shared PC policy

Templates contain groups of settings, organized by functionality. Use a template when you don't want to build policies manually or want to configure devices to access corporate networks, such as configuring WiFi or VPN. Learn more

Template name
Administrative Templates
Custom
Delivery Optimization
Device Firmware Configuration Interface
Device restrictions
Device restrictions (Windows 10 Team)
Domain Join
Edition upgrade and mode switch
Email
Endpoint protection
Identity protection
Kiosk
Microsoft Defender for Endpoint (desktop devices running Windows 10 or later)

3. In **Configuration settings**, review the available settings in the UEFI configuration.
4. Select **Assignments**.
5. Under **Select groups to include**, select the Azure AD security group that contains your target devices.
6. Select **Next** to continue through applicability rules.
7. Review the group settings, and then select **Create**.

Create an Autopilot profile

To create an Autopilot profile:

1. In Microsoft Endpoint Manager, choose **Select devices** → **Windows enrollment**.
2. Scroll to **Deployment profiles**, and then follow the on-screen prompts.

For more information, see How to create Autopilot Profile. Then, return to this document to continue with the steps below.

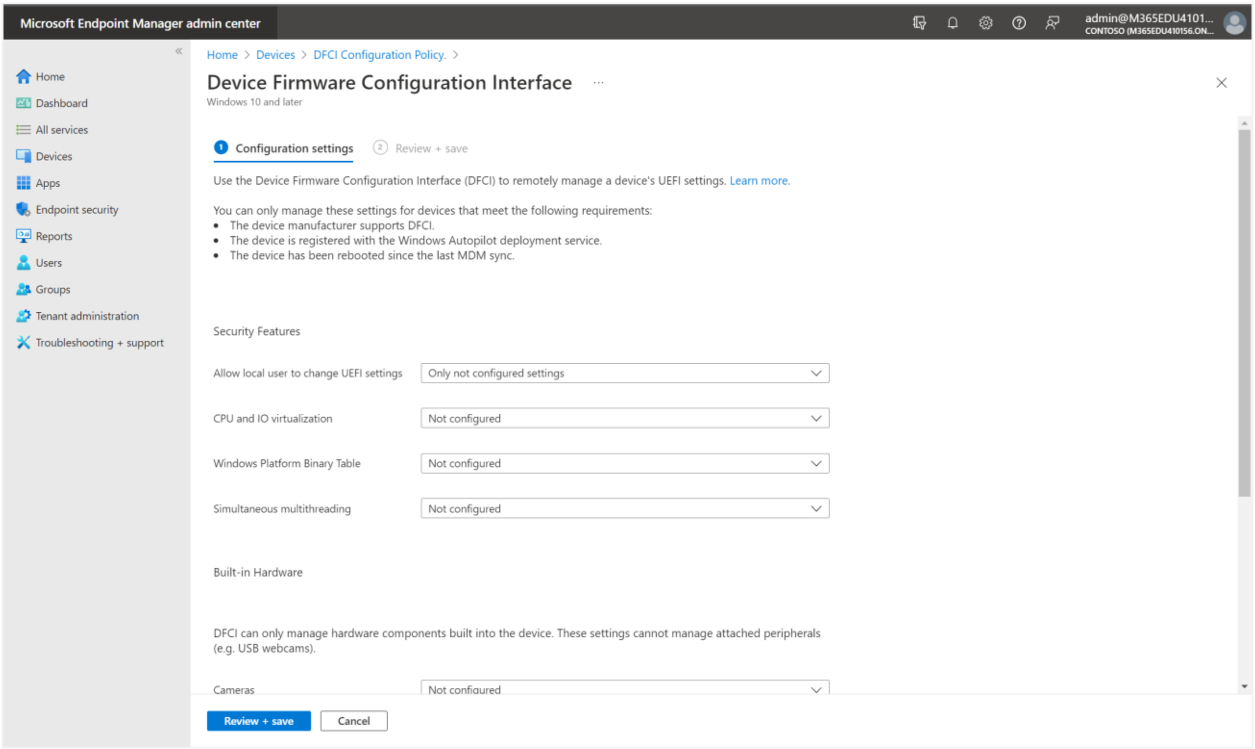
Create an enrollment status profile

To ensure devices apply the DFCI configuration during OOBE before users sign in, you must configure enrollment status. For more information, see Set up an enrollment status page, and then return to this document to continue with the steps below.

Configure DFCI settings on Surface devices

You can configure DFCI policy settings by editing the DFCI profile from Microsoft Endpoint Manager:

1. In the Microsoft Endpoint Manager admin center, select **Devices** → **Windows** → **Configuration profiles**.
2. Select the **DFCI profile name** → **Properties** → **Settings**.



Device Firmware Configuration Interface

Windows 10 and later

Use the Device Firmware Configuration Interface (DFCI) to remotely manage a device's UEFI settings. Learn more.

You can only manage these settings for devices that meet the following requirements:

- The device manufacturer supports DFCI.
- The device is registered with the Windows Autopilot deployment service.
- The device has been rebooted since the last MDM sync.

Security Features

Allow local user to change UEFI settings: Only not configured settings

CPU and IO virtualization: Not configured

Windows Platform Binary Table: Not configured

Simultaneous multithreading: Not configured

Built-in Hardware

DFCI can only manage hardware components built into the device. These settings cannot manage attached peripherals (e.g. USB webcams).

Cameras: Not configured

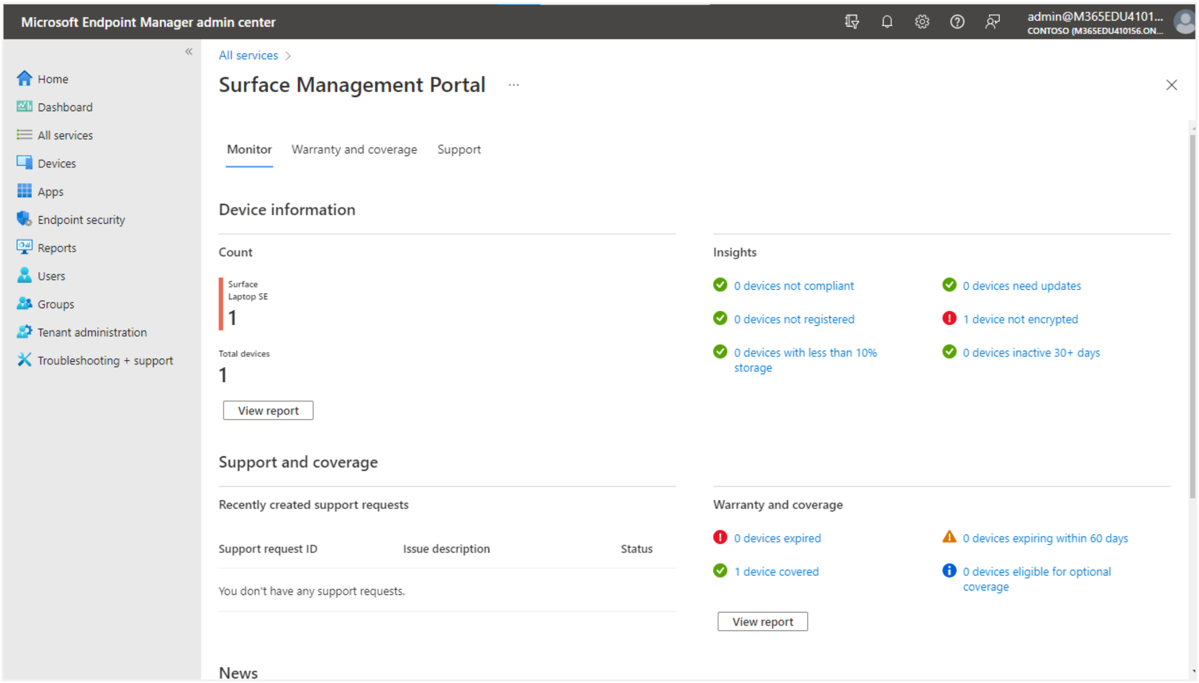
For more information, see Configuring the DFCI environment and managing UEFI configuration settings for targeted Surface devices.

Microsoft Surface Management Portal

Located in the Microsoft Endpoint Manager admin center, the Microsoft Surface Management Portal enables you to self-serve, manage, and monitor your school's Intune-managed Surface devices at scale. Get insights into device compliance, support activity, warranty coverage, and more. When Surface Laptop SE devices are enrolled in cloud management and users sign in for the first time, information automatically flows into the Surface Management Portal, giving you a single pane of glass for Surface-specific administration activities.

To access and use the Surface Management Portal:

1. In the Microsoft Endpoint Manager admin center, select **All services** → **Surface Management Portal**.



Device information

Count

Surface Laptop SE
1

Total devices
1

Insights

0 devices not compliant
0 devices need updates
0 devices not registered
1 device not encrypted
0 devices with less than 10% storage
0 devices inactive 30+ days

Support and coverage

Recently created support requests

Support request ID	Issue description	Status
You don't have any support requests.		

Warranty and coverage

0 devices expired
0 devices expiring within 60 days
1 device covered
0 devices eligible for optional coverage

News

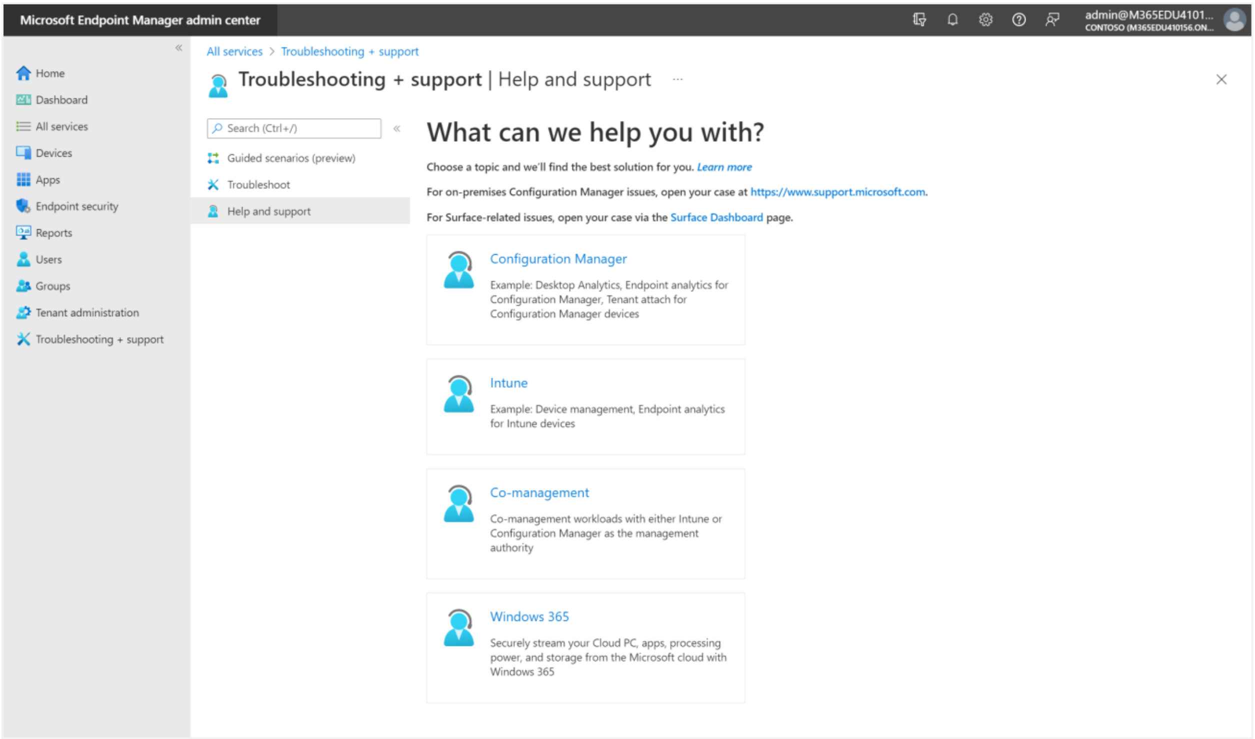
2. To display insights for all your Surface devices, select **Monitor**. This shows devices that are out of compliance or not registered, have critically low storage, require updates, or are currently inactive.
3. To see details on each insights category, select **View report**. This displays diagnostic information that you can customize and export.
4. To see the device's warranty information, select **Device warranty and coverage**.
5. To see support requests and their status, select **Support requests**.

Microsoft Endpoint Manager support

Microsoft provides global technical, presales, billing, and subscription support for cloud-based device management services, including Intune, Configuration Manager, Windows 365, and Microsoft Managed Desktop. For more information, see Microsoft Endpoint Manager support page.

To access troubleshooting support:

1. In the Microsoft Endpoint Manager admin center, select **Troubleshooting + support → Help and support**.


Microsoft Endpoint Manager admin center
admin@M365EDU4101...
CONTOSO (M365EDU410156.ON...
Home
Dashboard
All services
Devices
Apps
Endpoint security
Reports
Users
Groups
Tenant administration
Troubleshooting + support
All services > Troubleshooting + support
Search (Ctrl+/)
Guided scenarios (preview)
Troubleshoot
Help and support

Troubleshooting + support | Help and support

What can we help you with?

Choose a topic and we'll find the best solution for you. *Learn more*

For on-premises Configuration Manager issues, open your case at https://www.support.microsoft.com.

For Surface-related issues, open your case via the Surface Dashboard page.

Configuration Manager

Example: Desktop Analytics, Endpoint analytics for Configuration Manager, Tenant attach for Configuration Manager devices

Intune

Example: Device management, Endpoint analytics for Intune devices

Co-management

Co-management workloads with either Intune or Configuration Manager as the management authority

Windows 365

Securely stream your Cloud PC, apps, processing power, and storage from the Microsoft cloud with Windows 365

2. In the **Help and support** pane, select a tile for your desired support scenario: Configuration Manager, Intune, Co-management, or Windows 365.
3. On the page that is presented, review your selected support scenario.
4. Above **How can we help?**, select one of three icons to open different panes: Find solutions, Contact support, or Service requests.
5. In the **Find solutions** pane, use the text box to specify a few details about the issue. The console may offer suggestions based on what you have entered. Depending on the presence of specific keywords, the console provides help like:

   - **Run diagnostics.** Start automated tests and investigations of your tenant from the console to reveal known issues. When you run a diagnostic, you may receive mitigation steps to help with resolution.
   - **View insights.** Find links to documentation that provides context and background specific to the product area or actions you have described.

- **Recommended articles.** Browse suggested troubleshooting topics and other content related to the issue you have described.

6. If needed, use the **Contact support** pane to file an online support ticket. When opening a case, be sure to include as much detail as possible in the **Description** field. Important information includes timestamp and date, device ID, device model, serial number of the OS version, and any other details relevant to the issue.
7. To review your case history, select the **Service requests** pane. Active cases are at the top of the list, with closed issues also available for review.

For more information

Combining a unique suite of technologies—including Intune for Education and Windows 11 SE—with leading devices like Surface Laptop SE, Microsoft continues to demonstrate its commitment to making education more engaging, manageable, and secure. In this cookbook, we explored how to deploy and manage your school's Windows 11 SE and Surface Laptop SE devices at scale using Intune for Education.

The following resources provide additional information about topics covered in this cookbook:

- Microsoft 365 Education documentation
- Microsoft Education interactive demos
- Intune for Education
- Surface Laptop SE for Education
- Windows 11 SE for Education
- Manage devices running Windows 11 SE
- Set up Intune for Education devices with Windows Autopilot

Appendix: Device Management – Level 2

Microsoft Intune delivers streamlined remote management throughout the school year, giving IT the ability to manage apps, control security and privacy remotely, and generate compliance reports.

Remote device management

With Intune for Education, you can manage groups, applications, resources, and individual needs of multiple students. There are several ways to manage students' devices, including organizing what groups they belong to; determining what apps they have access to; and configuring device settings, customizations, and restrictions. You can also monitor when users sign in and troubleshoot devices remotely.

Managing groups

By organizing students, classrooms, or learning curricula into groups, you can provide students with the resources they need, as well as manage several student devices all at once.

NOTE: Before you begin creating groups, it is a good idea to plan them out to determine what students may need from their devices. For example:

- For all devices, block apps from using location services.
- For AP Computer Science, assign students apps to edit code.
- For 12th grade History, enable web browsing to access academic articles.
- For all Photography students, enable the device's camera.

Out of the box, Intune for Education comes with default groups that enable you to manage *All devices* and *All users*. There are also two additional groups if you use Microsoft SDS: *All teachers* and *All students*. SDS also creates individual groups for students and teachers of specific schools, which fold under the *All teachers* and *All students* groups. Beyond the defaults, groups can be customized to suit various needs. For example, if you have both Windows and iOS devices in your school, you can create groups, such as *All iPads* and *All Windows 10 PCs.*

Finally, two group types can be created: assigned groups and dynamic groups. Assigned groups are used when you want to manually add users or devices to a group. Dynamic groups reference rules that you create to assign students or devices to groups and then automate the assignment of devices to those groups.

For more information, see:

- Create groups in Intune for Education
- Edit a group name
- Move a group up or down within your existing group list
- Delete a group to remove apps and settings from devices
- Assign and delegate group admins
- Manually add or remove users and devices to an existing assigned group
- Edit dynamic group rules to accommodate for new devices, locations, or school years

Managing apps and settings

With Intune for Education, school IT administrators have access to diverse apps to help students unlock their learning potential. This section discusses tools and resources for adding apps to Intune for Education, assigning apps to groups, and managing device policies.

Add apps to Intune for Education

Multiple apps can be added to Intune for Education. Devices running Windows 11 SE are preinstalled with Office apps. During Express Configuration, all Office desktop apps are available in a single app called Microsoft 365.

Popular school apps

With Intune for Education, you can add popular school apps from the web. Keep in mind that only approved apps can be installed from the list found here. For more information, see Add popular apps to Intune for Education.

Desktop apps

Intune for Education makes it easy to add desktop apps to your deployment. You can upload and add desktop apps to your Intune for Education inventory and then assign them to groups and install them on Windows. Note that only approved apps can be installed from the list found here. For more information, see Add desktop apps in Intune for Education.

Web apps

Using Intune for Education, you can also add websites to your app inventory. Again, keep in mind that only approved apps can be installed from the list found here. For more information, see Add web apps to Intune for Education.

Assign apps to groups

With Intune for Education, you can make certain apps only available to select groups. For more information, see Assign apps to install them on school devices.

NOTE: If you assign an app to a device running Windows 11 SE and receive the **0x87D300D9** error code with a **Failed** state:

- Be sure the app is on the available apps list, or add your own app.
- If you submitted a request to add your own app and it was approved, check that the app meets package requirements.
- If the app is not approved, it will not run on Windows 11 SE. Add your own app or use an app that runs in a web browser, such as a web app or PWA.

Manage device policies

You can manage the settings of several devices from a single touchpoint. For more information, see:

- Add Wi-Fi profiles
- Add Take a Test profile
- View all Windows device settings

Remote assistance

With devices managed by Intune for Education, you can remotely assist students and teachers with device issues. For more information, see Remote assistance for managed devices - Intune for Education.

Device inventory and reporting

Windows and cloud security

Security extends from hardened firmware to the operating system through cloud management. You can manage devices with just a few clicks; control mics, USB ports, and Bluetooth; disable webcams; lock the operating system when the laptop is closed; and control physical access using the integrated Kensington Nano Security Slot.

Windows Update for Business

Windows Update for Business enables you to keep the Windows client devices in your school always up to date with the latest security defenses and Windows features. To do this, you directly connect these systems to the Windows Update service. For more information, see Windows Update for Business.

Microsoft Defender for Endpoint

Microsoft Defender for Endpoint is an enterprise endpoint security platform designed to help networks prevent, detect, investigate, and respond to advanced threats. You can use Defender for Endpoint to help secure your entire school network. For more information, see Onboard devices and configure Microsoft Defender for Endpoint capabilities.

Microsoft Intelligent Security Graph

Microsoft Intelligent Security Graph (ISG) offers application control with a tool that provides an option to automatically enable apps that ISG recognizes as having a known good reputation. Using ISG can help reduce the amount of time spent on complex application control processes. For more information, see Microsoft ISG.

Microsoft Endpoint Manager and DFCI support

With DFCI profiles built into Intune for Education, Surface UEFI management extends the modern management stack to the UEFI hardware level. With DFCI profiles, you can dramatically simplify IT deployment and provisioning across the device's lifecycle—all from the cloud. DFCI management requires the device to be enrolled with Windows Autopilot and be registered by a partner or OEM. For more information, see Manage DFCI on Surface devices.

Microsoft Defender SmartScreen

Microsoft Defender SmartScreen helps to protect students from phishing or malware websites and apps, and from downloading potentially malicious files. Microsoft Defender SmartScreen comes preinstalled on all Surface Laptop SE devices and adds another layer of protection against malicious activity. For more information, see Microsoft Defender SmartScreen.