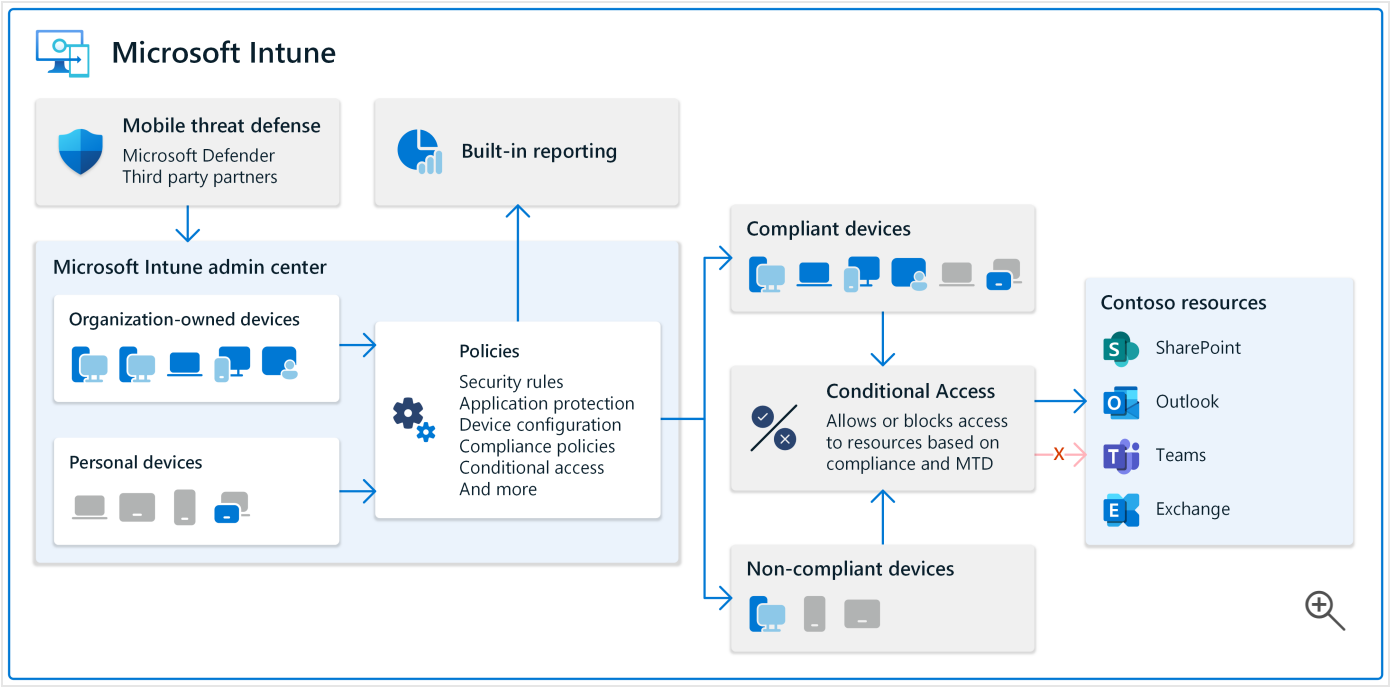
Learn about managing and securing your devices in Microsoft Intune

Summarize this article for me

Managing devices is a significant part of any endpoint management strategy and solution. Organizations have to manage desktops, laptops, tablets, mobile phones, wearables, and more. It can be a large task, especially if you're not sure where to start.

Microsoft Intune can help. Intune is a cloud-based service that can control devices through policy, including security policies.

The goal of any organization that's managing devices is to secure devices and the data they access.



Device management involves:

- Configuring features built into the device, like enabling Bluetooth and preventing automatic connections to Wi-Fi hotspots
- Securing the devices and preventing unauthorized access to organization resources from the devices, like using mobile threat defense and encrypting hard disks
- Creating compliance rules that maintain device integrity, like setting a minimum OS version and preventing simple passwords

- Being responsible for organization owned devices and personally owned devices that access your organization resources

From a service perspective, Intune uses Microsoft Entra ID for device storage and permissions. Using the Microsoft Intune admin center, you can manage device tasks and policies in a central location designed for endpoint management.

This article discusses concepts and features you should consider when managing your devices.

Manage organization owned and personal devices

Many organizations allow personally owned devices to access organization resources, including email and meetings. There are different options available and these options depend on how strict your organization is.

You can require personal devices be enrolled in your organization's device management services. On these personal devices, your admins can deploy policies, set rules, and configure device features. Or, you can use app protection policies that focus on protecting app data, such as Outlook, Teams, and Sharepoint. You can also use a combination of device enrollment and app protection policies.

Devices owned by your organization should be enrolled in your MDM service, like Intune. When enrolled, your admins create policies and set rules that protect data. Don't rely on end users to manage these devices.

For more information and guidance, go to:

- Microsoft Intune planning guide
- Deployment guide: Setup or move to Microsoft Intune

Use your existing devices and use new devices

You can manage new devices and existing devices. Intune supports Android, iOS/iPadOS, Linux, macOS, and Windows devices.

There are some things you should know. For example, if another MDM provider manages your existing devices, then these devices might need to be factory reset. If the devices are using an older OS version, they might not be supported.

If your organization is investing in new devices, then we recommend you start with a cloud approach using Intune.

For more information and guidance, go to:

- Microsoft Intune planning guide
- Deployment guide: Setup or move to Microsoft Intune

For more specific information by platform, go to:

- Android platform deployment guide
- iOS/iPadOS platform deployment guide
- Linux enrollment deployment guide
- macOS platform deployment guide
- Windows enrollment deployment guide

Check the compliance health of your devices

Device compliance is a significant part of managing devices. Your organization should set password/PIN rules and check for security features on these devices. You want to know which devices don't meet your rules. This task is where compliance comes in.

You can create compliance policies that block simple passwords, require a firewall, set the minimum OS version, and more. You can use these policies and built-in reporting to see noncompliant devices and see the noncompliant settings on these devices. This information gives you an idea of the overall health of the devices accessing your organization resources.

Conditional Access is a feature of Microsoft Entra ID. With Conditional Access, you can enforce compliance. For example, if a device doesn't meet your compliance rules, then you

can block access to organization resources, including Outlook, SharePoint, and Teams. Conditional Access helps your organization secure your data and protect your devices.

For more information, go to:

- Use compliance policies to set rules for devices you manage
- Monitor results of your device compliance policies
- Learn about Conditional Access and Intune

Control device features and assign policies to device groups

All devices have features that you can control and manage using policies. For example, you can block the built-in camera, allow Bluetooth pairing, and manage the power button.

For many organizations, it's common to create device groups. Device groups are Microsoft Entra groups that only include devices. They don't include user identities.

When you have device groups, you create policies that focus on the device experience or task, like running a single app or scanning bar codes. You can also create policies that include settings that you want to always be on the device, regardless of who's using the device.

You can group devices by OS platform, by function, by location, and other features you prefer.

Device groups can also include devices that are shared with many users or aren't associated with a specific user. These dedicated or kiosk devices are typically used by frontline workers (FLW) and can also be managed by Intune.

When the groups are ready, you can assign your policies to these device groups.

For more information, go to:

- FLW device management in Intune
- Get started with Microsoft 365 for frontline workers
- Windows device settings to run as a dedicated kiosk using Intune
- Control access, accounts, and power features on shared PC or multi-user devices using

Intune

Secure your devices

To help secure your devices, you can install antivirus, scan & react to malicious activity, and enable security features.

In Intune, some common security tasks include:

- **Integrate with Mobile Threat Defense** (MTD) partners to help protect organization owned devices and personally owned devices. These MTD services scan the devices and can help remediate vulnerabilities.

  The MTD partners support different platforms, including Android, iOS/iPadOS, macOS, and Windows.

  For more specific information, go to Mobile Threat Defense integration with Intune

- **Use security baselines** on your Windows devices. Security baselines are preconfigured settings that you can deploy to your devices. These baseline settings focus on security at a granular level and can also be changed to meet any organization specific requirements.

  If you're not sure where to start, then look at security baseline and the built-in guided scenarios.

  For more specific information, go to:
  - Use security baselines to configure Windows devices in Intune
  - Guided scenarios overview

- **Manage software updates, encrypt hard disks, configure built-in firewalls**, and more using built-in policy settings. You can also use Windows Autopatch for automatic patching of Windows, including Windows quality updates and Windows feature updates.

  For more information, go to:
  - Manage endpoint security in Microsoft Intune
  - Manage device security with endpoint security policies in Microsoft Intune
  - Windows Autopatch overview

- **Manage devices remotely** using the Intune admin center. You can remotely lock, restart, locate a lost device, and restore a device to its factory settings. These tasks are helpful if a device is lost or stolen, or if you're remotely troubleshooting a device.

  For more information, go to Remote actions in Intune.

Related articles

- Learn about managing identities in Intune
- Learn about managing apps in Intune

Last updated on 03/04/2025