**Microsoft Intune planning guide**

A successful Microsoft Intune deployment or migration starts with planning. This guide steps you through common mobile device management (MDM) and mobile application management (MAM) goals. It also provides guidance on inventorying your devices, licensing, reviewing current policies and infrastructure, creating a rollout plan, and more.

## **Task 1: Determine your objectives**

Organizations use mobile device management (MDM) and mobile application management (MAM) to control organization data securely, and with minimal disruption to users. When evaluating an MDM/MAM solution, such as Microsoft Intune, look at what the goal is, and what you want to achieve.

In this section, we discuss common objectives when using Intune.

### **Objective: Access organizational apps and email**

Users expect to work on devices using organization apps, including reading and responding to email, updating and sharing data, and more. In Intune, you can deploy different types of apps, including:

* Office 365 apps
* Win32 apps
* Line-of-business (LOB) apps
* Custom apps
* Allow (or block) access to built-in apps or store apps

**Task**: Make a list of the apps your users regularly use. These apps are the apps you want on their devices. Some considerations:

* Many organizations deploy the Office suite of apps to PCs and tablets, such as Word, Excel, OneNote, PowerPoint, and Teams. On smaller devices, such as mobile phones, individual apps might be installed, depending on the user requirements.

For example, the sales team may require Teams, Excel, and SharePoint. On mobile devices, you can deploy only these apps, instead of deploying the entire Office suite.

* Users expect to read and reply to email and join meetings on all devices, including personal devices. On organization-owned devices, you can deploy Outlook and Teams. And, manage and control all device settings and all app settings, including PIN and password requirements. On personal devices, you don't have this control. So, determine if you want to give users access to organization apps, such as email and meetings.

For more information and considerations, see [Personal devices vs Organization-owned devices](https://docs.microsoft.com/en-us/mem/intune/fundamentals/intune-planning-guide#personal-devices-vs-organization-owned-devices)

### **Objective: Secure access on all devices**

When data is stored on mobile devices, it should be protected from malicious activity.

**Task**: Determine how you want to secure your devices, and minimize the impact of malicious activity. Some considerations:

* Anti-virus (AV) and malware protection are a must. Intune integrates with [different Mobile Threat Defense (MTD) partners](https://docs.microsoft.com/en-us/mem/intune/protect/mobile-threat-defense) to help protect enrolled devices, personal devices, and apps. On Windows 10/11 devices, you can use [Microsoft Defender for Endpoint](https://docs.microsoft.com/en-us/mem/intune/protect/advanced-threat-protection) and Intune together.

[Microsoft Defender for Endpoint](https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/microsoft-defender-advanced-threat-protection) includes security features and a [portal](https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/portal-overview) to help monitor, and react to threats.

* If a device is compromised, you'll want to limit the impact using [conditional access](https://docs.microsoft.com/en-us/mem/intune/protect/conditional-access). For example:
  + If a device meets a threat level you set, you can block access to organization resources. Conditional access helps prevent the spread of malicious activity.
  + Conditional access helps protect your network and resources from devices, even devices that aren't enrolled with Intune.

For example, Intune integrates with Microsoft Defender for Endpoint. Microsoft Defender for Endpoint scans a device, and determines if it's compromised. Then, conditional access can automatically block access on this device from organization resources, including email.

* Updates to the device, the operating system, and apps also help keep your data secure. Create a plan on how and when updates are installed. There are policies in Intune that help you manage updates, including updates to store apps.
* Determine how users will authenticate with organization resources from their many devices. For example, you can:
  + Use [certificates](https://docs.microsoft.com/en-us/mem/intune/protect/certificates-configure) on devices to authenticate features and apps, such as connecting to a virtual private network (VPN), opening Outlook, and more. These certificates allow for a "password-less" user experience. Password-less is considered more secure than requiring users to enter their organization username and password.

If you're planning to use certificates, be sure you have a supported [public key infrastructure (PKI) infrastructure](https://docs.microsoft.com/en-us/mem/intune/protect/certificates-configure) ready to create and deploy certificate profiles.

* + Use multi-factor authentication (MFA) when you need an extra layer of authentication on organization-owned devices. Or, use MFA to authenticate apps on personal devices. Biometrics, such as face recognition and fingerprints, can also be used.

If you'll use biometrics for authentication, be sure your devices support biometrics. Most modern devices do.

* + Implement a Zero Trust deployment. With Zero Trust, you use the features in Azure AD and Microsoft Intune to secure all endpoints, uses password-less authentication, and more. For more information, see the [Zero Trust Deployment Center](https://docs.microsoft.com/en-us/security/zero-trust/).

### **Objective: Distribute IT**

Many organizations want to give different admins control over locations, divisions, and so on. For example, the **Charlotte IT Admins** group controls and monitors the policies in the Charlotte campus. These Charlotte IT Admins can only see and manage policies for the Charlotte location. They can't see and manage policies for the Redmond location. This approach is called distributed IT.

In Intune, distributed IT uses [scope tags](https://docs.microsoft.com/en-us/mem/intune/fundamentals/scope-tags) and [device enrollment categories](https://docs.microsoft.com/en-us/mem/intune/enrollment/device-group-mapping). Scope tags use role-based access control (RBAC). So, only users in a specific group have permission to manage policies and profiles for users and devices in their scope.

When using device categories, devices are automatically added to groups based on categories you create. When users enroll their device, they choose a category, such as Sales, IT admin, point-of-sale device, and so on. These device groups are now ready to receive the profiles and policies you create.

To make managing devices easier, you can use Intune device categories to automatically add devices to groups based on categories that you define.

**Task**: Determine how you want to distribute your rules and settings (policies and profiles). Some considerations:

* Determine your admin structure. For example, you might want to separate by location, such as **Charlotte IT Admins** or **Redmond IT Admins**. You might want to separate by role, such as **Network Admins** that control all network access, including VPN.

These categories will become your [scope tags](https://docs.microsoft.com/en-us/mem/intune/fundamentals/scope-tags).

* Many organizations separate groups by the device type, such as iOS, iPadOS, Android, or Windows devices. Some examples:
  + Distribute specific apps to specific devices. For example, deploy the Microsoft shuttle app to devices in the Redmond network.
  + Deploy policies to specific locations. For example, deploy a VPN profile to devices in the Charlotte network so they automatically connect when in range.
  + Control settings on specific devices. For example, disable the camera on Android Enterprise devices used on a manufacturing floor, create a Windows Defender antivirus profile for all Windows devices, or add Exchange e-mail settings to all iOS/iPadOS devices.

These categories will become your [device enrollment categories](https://docs.microsoft.com/en-us/mem/intune/enrollment/device-group-mapping).

### Objective: Keep organization data inside the organization

When data is stored on mobile devices, the data should be protected from accidental loss or sharing. This objective includes wiping organization data from personal and organization-owned devices.

**Task**: Create a plan to cover different scenarios that impact your organization. Some considerations:

* A device is lost or stolen, or no longer being used. A user leaves the organization.
  + In Intune, you can [remove devices by using wipe, retire, or manually unenroll them](https://docs.microsoft.com/en-us/mem/intune/remote-actions/devices-wipe). You can also automatically remove devices that haven't checked in for x number of days.
  + At the app level, you can [remove organization data from Intune-managed apps](https://docs.microsoft.com/en-us/mem/intune/apps/apps-selective-wipe). A selective wipe is great for personal devices, as it keeps personal data on the device, and only removes organization data.
* On personal devices, you may want to prevent users from copy/paste, taking screenshots, or forwarding emails. [App protection policies](https://docs.microsoft.com/en-us/mem/intune/apps/app-protection-policy) can block these features on devices you don't manage. For more information, see [prevent data leaks on non-managed devices using Intune](https://docs.microsoft.com/en-us/mem/intune/protect/data-leak-prevention).

On managed devices (devices enrolled in Intune), you can also control these features using device configuration profiles. [Device configuration profiles](https://docs.microsoft.com/en-us/mem/intune/configuration/device-profiles) control settings on the device, not the app. On devices that access highly sensitive or confidential data, device configuration profiles can prevent copy/paste, taking screenshots, and more.

* On Office apps, [prevent unauthorized access to organization data](https://docs.microsoft.com/en-us/mem/intune/protect/data-outside-protect) by using Azure Information Protection. This feature uses labels to classify your files, such as confidential data.

For more information and considerations, see [Personal devices vs Organization-owned devices](https://docs.microsoft.com/en-us/mem/intune/fundamentals/intune-planning-guide#personal-devices-vs-organization-owned-devices) (in this article).

## **Task 2: Inventory your devices**

Organizations have a range of devices, including desktop computers, laptops, tablets, and mobile phones. These devices can be owned by the organization, or owned by your users. When planning your device management solution, be sure to consider everything that will access your organization resources, including users' personal devices.

This section includes device information that you should consider.

### Supported platforms

Intune supports Android device administrator, Android Enterprise, iOS, iPadOS, macOS, and Windows devices. For the specific versions, see [supported platforms](https://docs.microsoft.com/en-us/mem/intune/fundamentals/supported-devices-browsers).

**Task**: If your devices use unsupported versions, which are primarily older operating systems, then it's time to upgrade the OS or replace the devices. These older OS' and devices might have limited support, and are a potential security risk. This task includes desktop computers running Windows 7, iPhone 7 devices running the original v10.0 OS, and so on.

### Personal devices vs Organization-owned devices

On personal devices, it's normal and expected for users to check email, join Teams meetings, update SharePoint files, and more. Many organizations allow personal devices, and many organizations only allow organization-owned devices.

As an organization and as an admin, you decide if you'll allow personal devices.

**Task**: Determine how you want to handle personal devices. If being "mobile" is important to your organization, consider the following approaches:

* On personal devices, give users the choice to enroll in Intune. Once enrolled, admins fully manage these devices, including pushing policies, controlling device features and settings, and even wiping devices. As an admin, you may want this control, or you may think you want this control.

When users enroll their personal devices, they may not realize or understand that admins can do anything on the device, including accidentally wiping or resetting the device. As an admin, you may not want this liability or potential impact on devices your organization doesn't own.

Also, many users refuse to enroll. They find other ways to access organization resources. For example, you require devices be enrolled to use the Outlook app to check organization email. To skip this requirement, users open any web browser on the device, and sign in to Outlook web access, which may not be what you want. Or, they create screenshots, and save the images on the device, which also isn't what you want.

* On personal devices, use app configuration policies and app protection policies. Users don't enroll in Intune. These devices aren't managed by you.

Use a [Terms and conditions](https://docs.microsoft.com/en-us/mem/intune/enrollment/terms-and-conditions-create) statement with a conditional access policy. If users don't agree, then they don't get access to apps. If users agree to the statement, then a device record is added to Azure AD, and the device becomes a known entity. When the device is known, you can track what's being accessed from the device.

Next, control access and security using app policies.

Look at the tasks your organization uses the most, such as email and joining meetings. Use [app configuration policies](https://docs.microsoft.com/en-us/mem/intune/apps/app-configuration-policies-overview) to configure app-specific settings. Use [app protection policies](https://docs.microsoft.com/en-us/mem/intune/apps/app-protection-policy) to control the security and access to these apps.

For example, users can use the Outlook app on their personal device to check work email. Using Intune, admins create an Outlook app protection policy that uses multi-factor authentication (MFA) every time the Outlook app opens, prevents copy and paste, and more.

* You want every device to be fully managed. In this scenario, give users all the devices they need, including mobile phones. Invest in a hardware refresh plan so users continue to be productive and effective. Enroll these organization-owned devices in Intune, and manage them using policies.

This option prevents personal devices.

As a best practice, always assume data will leave the device. Be sure your tracking and auditing methods are in place. For more information, see the [Zero Trust Deployment Center](https://docs.microsoft.com/en-us/security/zero-trust/).

### Manage desktop computers

Intune can manage desktop computers running Windows 10 and newer. The Windows client OS includes built-in modern device management features, and removes dependencies on local Active Directory (AD) group policy. You get the benefits of the cloud when creating rules and settings in Intune, and deploying these policies to all your Windows client devices, including desktop computers and PCs.

For more information, see [Guided scenario - Cloud-managed Modern Desktop](https://docs.microsoft.com/en-us/mem/intune/fundamentals/guided-scenarios-cloud-managed-pc).

If your Windows devices are currently managed using Configuration Manager, you can still enroll these devices in Intune. This approach is called "co-management". Co-management offers many benefits, including running remote actions on the device (restart, remote control, factory reset), conditional access with device compliance, and more. You can also cloud-attach your devices to Intune.

For more information, see [What is co-management](https://docs.microsoft.com/en-us/mem/configmgr/comanage/overview), [Paths to co-management](https://docs.microsoft.com/en-us/mem/configmgr/comanage/quickstart-paths), and [Endpoint Manager tenant attach](https://docs.microsoft.com/en-us/mem/configmgr/tenant-attach/device-sync-actions).

**Task**: Look at what you currently use for mobile device management, what the goals are, and determine the best path. Some considerations:

* If you currently don't use anything, then going straight to Intune may be best.
* For new devices not enrolled in Configuration Manager, or any MDM solution, then going straight to Intune may be best.
* If you currently use Configuration Manager, then your options include:
  + If you want to keep your existing infrastructure, and move some workloads to the cloud, then use co-management. You get the benefit of both services. Existing devices can receive some policies from Configuration Manager (on-premises), and other policies from Intune (cloud).
  + If you want to keep your existing infrastructure, and use Intune to help monitor your on-premises devices, then use tenant-attach. You get the benefit of using the Endpoint Manager admin center, while still using Configuration Manager to manage devices.
  + If you want a pure cloud solution to manage devices, then move to Intune. This scenario is rare. Existing Configuration Manager users often prefer to continue using Configuration Manager. The [setup deployment guide](https://docs.microsoft.com/en-us/mem/intune/fundamentals/deployment-guide-intune-setup) has some good information.

For more information, see [co-management workloads](https://docs.microsoft.com/en-us/mem/configmgr/comanage/workloads).

## **Task 3: Determine costs and licensing**

Managing devices is a relationship with different services. Intune includes the settings and features you can control on different devices. There are also other services that play a key role:

* **Azure Active Directory (AD) Premium** includes several features that are key to managing devices, including:
  + [Windows Autopilot](https://docs.microsoft.com/en-us/mem/autopilot/enrollment-autopilot): Windows client devices can automatically enroll in Intune, and automatically receive your policies.
  + [Multi-factor authentication](https://docs.microsoft.com/en-us/mem/intune/enrollment/multi-factor-authentication) (MFA): Users must enter two or more verification methods, such as a PIN, an authenticator app, a fingerprint, and more. MFA is a great option when using app protection policies for personal devices, or organization-owned devices that require extra security.
  + [Conditional access](https://docs.microsoft.com/en-us/mem/intune/protect/conditional-access): If users and devices follow your rules, such as a 6-digit passcode, then they get access to organization resources. If users or devices don't meet your rules, then they don't get access.
  + [Dynamic user groups and dynamic device groups](https://docs.microsoft.com/en-us/mem/intune/fundamentals/groups-add): Add users or devices automatically to groups when they meet criteria, such as a city, job title, OS type, OS version, and more.
* **Office 365** includes the apps that users rely on, including Outlook, Word, SharePoint, Teams, OneDrive, and more. You can deploy these apps to devices using Intune.
* **Microsoft Defender for Endpoint** helps monitor and scan your Windows client devices for malicious activity. You can also set an acceptable threat level. When combined with conditional access, you can block access to organization resources if the threat level is exceeded.
* **Azure Information Protection** classifies and protects documents and emails by applying labels. On Office apps, you can use this service to [prevent unauthorized access to organization data](https://docs.microsoft.com/en-us/mem/intune/protect/data-outside-protect), including apps on personal devices.

All of these services are included in the **Microsoft 365 E5** license. For more information, see [Microsoft 365 licensing plans](https://www.microsoft.com/microsoft-365/compare-all-microsoft-365-plans).

**Task**: Determine what services and programs your organization needs and uses to be productive and secure. Some considerations:

* If your goal is to deploy policies (rules) and profiles (settings), without any enforcement, at a minimum, you need Intune. Intune is available with different subscriptions, including as a stand-alone service. For more information, see [Microsoft Intune licensing](https://docs.microsoft.com/en-us/mem/intune/fundamentals/licenses).

You currently use Configuration Manager, and want to set up co-management for your devices. Intune is already included in your Configuration Manager license. If you want new devices or existing co-managed devices to be fully managed by Intune, then you need a separate Intune license.

* You want to enforce the compliance or password rules you create in Intune. At a minimum, you need Intune and Azure AD Premium. Intune and Azure AD Premium are available with **Enterprise Mobility + Security**.

For more information, see [Enterprise Mobility + Security pricing options](https://www.microsoft.com/microsoft-365/enterprise-mobility-security/compare-plans-and-pricing).

* You want to only manage Office 365 apps on devices. At a minimum, you need Office 365. For more information, see [MDM for Office 365 vs Microsoft Intune](https://support.office.com/article/choose-between-mdm-for-office-365-and-microsoft-intune-c93d9ab9-efb2-4349-9b93-30c30562ee22) and [FAQ about Mobile Device Management for Office 365](https://support.office.com/article/frequently-asked-questions-about-mobile-device-management-for-office-365-3871f99c-c9db-4a23-86f9-902c1b02f58d).
* You want to deploy Office 365 apps to your devices, and create policies to help secure devices that run these apps. At a minimum, you need Intune and Office 365.
* You want to create policies in Intune, deploy Office 365 apps, and enforce your rules and settings. At a minimum, you need Intune, Office 365, and Azure AD Premium. Since all these services are included in Microsoft 365, then it might be cost effective to use the Microsoft 365 license.

For more information, see [Microsoft 365 licensing plans](https://www.microsoft.com/microsoft-365/compare-all-microsoft-365-plans).

## **Task 4: Review existing policies and infrastructure**

Many organizations have existing policies and device management infrastructure that's only being "maintained". For example, you might have 20-year-old group policies, and don't know what they do. When considering a move to the cloud, instead of looking at what you've always done, determine the goal.

With these goals in mind, create a baseline of your policies. If you have multiple device management solutions, now might be the time to use a single mobile device management solution.

**Task**: Start looking at tasks that you run on-premises, and could move to the cloud. Remember, instead of looking at what you've always done, determine the goal. Some considerations:

* Review your existing policies and their structure. Some policies may apply globally, some apply at the site level, and some are specific to a device. The goal is to know and understand the intent of global policies, the intent of local policies, and so on.

AD group policies are applied in the LSDOU order - local, site, domain, and organizational unit (OU). In this hierarchy, OU policies overwrite domain policies, domain policies overwrite site policies, and so on.

In Intune, policies are applied to users and groups you create. There isn't a hierarchy. If two policies update the same setting, then the setting shows as a conflict. For more information, see [Common questions, issues, and resolutions with device policies and profiles](https://docs.microsoft.com/en-us/mem/intune/configuration/device-profile-troubleshoot#if-multiple-policies-are-assigned-to-the-same-user-or-device-how-do-i-know-which-settings-gets-applied).

When coming from AD group policy to Intune, your AD global policies will logically start to apply to groups you have, or groups you need. These groups will include users and devices you want to target at the global level, site level, and so on. This task gives you an idea of the group structure you'll need in Intune.

* Be prepared to create new policies and profiles in Intune. Intune includes several features that cover scenarios that may interest you. Some examples:
  + **Security baselines**: On Windows 10/11 devices, [Security baselines](https://docs.microsoft.com/en-us/mem/intune/protect/security-baselines) are security settings that are pre-configured to recommended values. If you're new to securing devices, or want a comprehensive baseline, then look at Security Baselines.
  + **Administrative templates**: On Windows 10/11 devices, use [ADMX templates](https://docs.microsoft.com/en-us/mem/intune/configuration/administrative-templates-windows) to configure group policy settings for Windows, Internet Explorer, Office, and Microsoft Edge version 77 and later. These ADMX templates are the same ADMX templates used in AD group policy, but are 100% cloud-based in Intune.
  + **Group policy**: Use [group policy analytics](https://docs.microsoft.com/en-us/mem/intune/configuration/group-policy-analytics) to import and analyze your GPOs. This feature helps you determine how your GPOs translate in the cloud. The output shows which settings are supported in MDM providers, including Microsoft Intune. It also shows any deprecated settings, or settings not available to MDM providers.
  + **Guided scenarios**: [Guided scenarios](https://docs.microsoft.com/en-us/mem/intune/fundamentals/guided-scenarios-overview) are a customized series of steps focused on end-to-end use cases. These scenarios automatically include policies, apps, assignments, and other management configurations.
* Create a policy baseline that includes the minimum of your goals. For example:
  + Secure e-mail: At a minimum, you might want to:
    - Enable [conditional access](https://docs.microsoft.com/en-us/mem/intune/protect/conditional-access) for Exchange Online, or connecting to an on-premises email solution.
    - Create Outlook app protection policies.
  + Device settings: At a minimum, you might want to:
    - Require a six character PIN to unlock the device.
    - Prevent backups to personal cloud services, such as iCloud or OneDrive.
  + Device profiles: At a minimum, you might want to:
    - Create a [Wi-Fi profile](https://docs.microsoft.com/en-us/mem/intune/configuration/wi-fi-settings-configure) with the preconfigured settings that connect to the Contoso Wi-Fi wireless network.
    - Create a [VPN profile](https://docs.microsoft.com/en-us/mem/intune/configuration/vpn-settings-configure) with a certificate to automatically authenticate, and connect to an organization VPN.
    - Create an [email profile](https://docs.microsoft.com/en-us/mem/intune/configuration/email-settings-configure) with the preconfigured settings that connect to Office 365 or a Gmail email solution.
  + Apps: At a minimum, you might want to:
    - Deploy Office 365 with app protection policies.
    - Deploy line of business (LOB) with app protection policies.
* Review the current structure of your groups. In Intune, you can create and assign policies to user groups, device groups, and dynamic user and device groups (requires Azure AD Premium).

When you create groups in the cloud, such as Intune or Microsoft 365, they're created in Azure AD. You don't see the Azure AD branding, but that's what you're using.

* + Creating new groups is an easy task. They can be created in the [Microsoft Endpoint Manager admin center](https://go.microsoft.com/fwlink/?linkid=2109431). For more information, see [add groups to organize users and devices](https://docs.microsoft.com/en-us/mem/intune/fundamentals/groups-add).
  + Moving existing distribution lists (DL) to Azure AD might be more challenging. Once they DLs are in Azure AD, these groups can be used by Intune and Microsoft 365. For more information, see:
    - [What is hybrid identity with Azure Active Directory?](https://docs.microsoft.com/en-us/azure/active-directory/hybrid/whatis-hybrid-identity)
    - [Azure AD Connect sync: Understand and customize synchronization](https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sync-whatis)
  + If you have existing Office 365 groups, you can move to Microsoft 365. Your existing groups remain, and you get all the features services of Microsoft 365. For more information, see:
    - [What is Microsoft 365?](https://docs.microsoft.com/en-us/learn/modules/what-is-m365/)
    - [Migration to Microsoft 365 Enterprise](https://docs.microsoft.com/en-us/microsoft-365/enterprise/migration-microsoft-365-enterprise-workload)
    - [Upgrade to Microsoft 365 Business](https://docs.microsoft.com/en-us/microsoft-365/business/migrate-to-microsoft-365-business)
* If you have multiple device management solutions, then switch to a single mobile device management solution. We recommend using Intune to help protect organization data in apps and on devices.

## **Task 5: Create a rollout plan**

The next task is to plan how and when your users and devices receive your policies. In this task, also consider:

* Define your goals and success metrics. Use these data points to create other rollout phases. Make sure goals are SMART (Specific, Measurable, Attainable, Realistic, and Timely). Plan to measure against your goals at each phase so your rollout project stays on track.
* Have clearly-defined goals and objectives. Include these objectives in all awareness and training activities so users understand why your organization chose Intune.

**Task**: Create a plan to roll out your policies, and choose how users enroll their devices in Intune. Some considerations:

* Roll out your policies in phases. For example:
  + Start with a pilot or test group. These groups should know they're the first users, and be willing to provide feedback. Use this feedback to improve configuration, documentation, notifications, and make it easier for users in a future rollout. These users shouldn't be executives or VIPs.

After initial testing, add more users to the pilot group. Or, create more pilot groups that focus on a different rollout, such as:

* + - **Departments**: Each department can be a rollout phase. You target an entire department at a time. In this rollout, users in each department might use their device in the same way, and access the same applications. Users likely have the same types of policies.
    - **Geography**: Deploy your policies to all users in a specific geography, whether it's the same continent, country/region, or same organization building. This rollout lets you focus on the specific location of users. You could provide a Windows Autopilot for pre-provisioned deployment approach, as the number of locations deploying Intune at the same time is less. There are chances of different departments or different use cases at the same location. So, you could be testing different use cases simultaneously.
    - **Platform**: This rollout deploys similar platforms at the same time. For example, deploy policies to all iOS/iPadOS devices in February, all Android devices in March, and all Windows devices in April. This approach might simplify help desk support, as they only support one platform at a time.

Using a staged approach, you can get feedback from a wide range of user types.

* + After a successful pilot, you're ready to start a full production rollout. The following example is an Intune rollout plan that includes targeted groups and timelines:

| **Rollout phase** | **July** | **August** | **September** | **October** |
| --- | --- | --- | --- | --- |
| Limited Pilot | IT (50 users) |  |  |  |
| Expanded Pilot | IT (200 users), IT Executives (10 users) |  |  |  |
| Production rollout phase 1 |  | Sales and Marketing (2000 users) |  |  |
| Production rollout phase 2 |  |  | Retail (1000 users) |  |
| Production rollout phase 3 |  |  |  | HR (50 users), Finance (40 users), Executives (30 users) |

* This template is also available to download at [Intune deployment planning, design, and implementation - Table templates](https://www.microsoft.com/download/details.aspx?id=103005).
* Choose how users will enroll their personal and organization-owned devices. There are different enrollment approaches you can use, including:
  + **User self-service**: Users enroll their own devices following steps provided by their IT organization. This approach is most common, and is more scalable than user-assisted enrollment.
  + **User-assisted enrollment**: Using this pre-provisioned deployment approach, an IT member helps users through the enrollment process, in person or using Teams. This approach is common with executive staff and other groups that might need more assistance.
  + **IT tech fair**: At this event, the IT group sets up an Intune enrollment assistance booth. Users receive information on Intune enrollment, ask questions, and get help enrolling their devices. This option is beneficial for IT and users, especially during the early phases of an Intune rollout.

The following example includes the enrollment approaches:

| **Rollout phase** | **July** | **August** | **September** | **October** |
| --- | --- | --- | --- | --- |
| Limited Pilot |  |  |  |  |
| Self-service | IT |  |  |  |
| Expanded Pilot |  |  |  |  |
| Self-service | IT |  |  |  |
| Pre-provisioned | IT Executives |  |  |  |
| Production rollout phase 1 |  | Sales, Marketing |  |  |
| Self-service |  | Sales and Marketing |  |  |
| Production rollout phase 2 |  |  | Retail |  |
| Self-service |  |  | Retail |  |
| Production rollout phase 3 |  |  |  | Executives, HR, Finance |
| Self-service |  |  |  | HR, Finance |
| Pre-provisioned |  |  |  | Executives |

## **Task 6: Communicate changes**

Change management relies on clear and helpful communications about upcoming changes. The idea is to smooth your Intune deployment, be sure users are aware of changes, and any disruption.

**Task**: Your rollout communication plan should include important information, how to notify users, and when to communicate. Some considerations:

* Determine what information to communicate. Communicate in phases to your groups and users, starting with an Intune rollout kickoff, pre-enrollment, and then post-enrollment:
  + **Kickoff phase**: Broad communication that introduces the Intune project. It should answer key questions, such as:
    - What is Intune?
    - Why the organization is using Intune, including benefits to the organization and to users
    - Provide a high-level plan of the deployment and rollout.
    - If personal devices won't be allowed unless the devices are enrolled, explain why you made the decision.
  + **Pre-enrollment phase**: Broad communication that includes information about Intune and additional services (such as Office, Outlook, and OneDrive), user resources, and specific timelines when users and groups are to receive Intune.
  + **Enrollment phase**: Communication targeting organization users and groups that are scheduled to receive Intune. It should inform users that they're ready to receive Intune, include enrollment steps, and who to contact for help and questions.
  + **Post enrollment phase**: Communication targeting organization users and groups that have enrolled in Intune. It should provide additional resources that might be helpful to users, and collect feedback about their experience during and after enrollment.

The [Intune Adoption Kit](https://aka.ms/IntuneAdoptionKit) might be helpful. Use it as-is, or change it for your organization.

* Choose how to communicate Intune rollout information to your targeted groups and users. For example:
  + Create an organization wide in-person meeting, or use Microsoft Teams.
  + Create an email for pre-enrollment, email for enrollment, and email for post-enrollment. For example:
    - **Email 1**: Explain the benefits, expectations, and schedule. Take this opportunity to showcase any other services whose access is granted on devices managed by Intune.
    - **Email 2**: Announce that services are now ready for access through Intune. Tell users to enroll now. Give users a timeline before their access is affected. Remind users of benefits and strategic reasons for migration.
  + Use an organization web site that explains the rollout phases, what users can expect, and who to contact for help.
  + Create posters, use organization social media platforms (such as Yammer), or distribute flyers to announce the pre-enrollment phase.
* Create a timeline that includes when and who. The first Intune kickoff communications can target the entire organization, or just a subset. They can take place over several weeks before the Intune rollout begins. After that, information could be communicated in phases to users and groups, aligned with their Intune rollout schedule.

The following example is a high-level Intune rollout communications plan:

| **Communication plan** | **July** | **August** | **September** | **October** |
| --- | --- | --- | --- | --- |
| Phase 1 | All |  |  |  |
| Kickoff meeting | First week |  |  |  |
| Phase 2 | IT | Sales and Marketing | Retail | HR, Finance, and Executives |
| Pre-rollout Email 1 | First week | First week | First week | First week |
| Phase 3 | IT | Sales and Marketing | Retail | HR, Finance, and Executives |
| Pre-rollout Email 2 | Second week | Second week | Second week | Second week |
| Phase 4 | IT | Sales and Marketing | Retail | HR, Finance, and Executives |
| Enrollment email | Third week | Third week | Third week | Third week |
| Phase 5 | IT | Sales and Marketing | Retail | HR, Finance, and Executives |
| Post-enrollment email | Fourth week | Fourth week | Fourth week | Fourth week |

## **Task 7: Support help desk and end users**

Include your IT support and helpdesk in the early stages of Intune deployment planning and pilot efforts. Early involvement exposes your support staff to Intune, and they gain knowledge and experience in identifying and resolving issues more effectively. It also prepares them for supporting the organization's full production rollout. Knowledgeable help desk and support teams also help users adopt these changes.

**Task**: Incorporate support training. Validate the end-user experience with success metrics in your deployment plan. Some considerations:

* Determine who will support end users. Organizations may have different tiers or levels (1-3). For example, tier 1 and 2 may be part of the support team. Tier 3 includes members of the MDM team responsible for the Intune deployment.

Tier 1 is typically the first level of support and the first tier to contact. If tier 1 can't resolve the issue, then they escalate to tier 2. Tier 2 escalates it to tier 3. [Microsoft support](https://docs.microsoft.com/en-us/mem/get-support) may be considered as tier 4.

* + In the initial rollout phases, be sure all tiers in your support team document issues and resolutions. Look for patterns, and adjust your communications for the next rollout phase. For example:
    - If different users or groups are hesitant about enrolling their personal devices, consider a Teams calls to answer common questions.
    - If users are having the same issues enrolling organization-owned devices, then host an in-person event to help users enroll the devices.
* Create a help desk workflow, and constantly communicate support issues, trends, and other important information to all tiers in your support team. For example, hold daily or weekly Teams meetings so all tiers are aware of trends, patterns, and can get help.

The following example shows how Contoso implements their IT support or helpdesk workflows:

* + End-user contacts IT support or helpdesk tier 1 with an enrollment issue.
  + IT support or helpdesk tier 1 can't determine the root cause and escalates to tier 2.
  + IT support or helpdesk tier 2 investigates. Tier 2 can't resolve the issue and escalates to tier 3, and provides additional information to help with the issue.
  + IT support or helpdesk tier 3 investigates, determines the root cause, and communicates the resolution to tier 2 and 1.
  + IT support/helpdesk tier 1 then contacts the users, and resolves the issue.

This approach, especially in early stages of the Intune rollout, adds many benefits, including:

* + Assist in technology learning.
  + Quickly identify issues and resolution.
  + Improve the overall user experience.
* Train your help desk and support teams. Have them enroll devices running the different platforms used in your organization (Android, iOS/iPadOS, macOS, Windows) so they're familiar with the process. Consider using help desk and support teams as a pilot group for your scenarios.

There are training resources available, including  Microsoft tutorials on [enrollment](https://docs.microsoft.com/en-us/mem/intune/enrollment/tutorial-use-autopilot-enroll-devices), [compliance](https://docs.microsoft.com/en-us/mem/intune/protect/tutorial-protect-email-on-enrolled-devices), [configuration](https://docs.microsoft.com/en-us/mem/intune/configuration/tutorial-walkthrough-administrative-templates), and courses through training partners.

The following example is an Intune support training agenda:

* + Intune support plan review
  + Intune overview
  + Troubleshooting common issues
  + Tools and resources
  + Q & A

The [educate your end users documentation](https://docs.microsoft.com/en-us/mem/intune/fundamentals/end-user-educate), community-based [Intune forum](https://social.technet.microsoft.com/Forums/home), and [end-user documentation](https://docs.microsoft.com/en-us/intune-user-help/use-managed-devices-to-get-work-done) are also great resources.