Microsoft

# Store and share files inside and outside your organization to work securely across organizational boundaries

Cumbersome restrictions and limitations on mobile devices, apps, and remote access can be taxing from an IT perspective and frustrating for your employees. Users need to be able to create, access, and share files from anywhere, but you also need to ensure that these actions are safe and secure. Microsoft 365 offers security solutions that can help secure your collaboration and productivity apps, including third-party apps, so that your employees can connect and communicate wherever they are, using the tools they are familiar with, as securely as if they were right at their desks.

## How can I securely share documents outside my organization?

### Microsoft Azure Information Protection

Azure Information Protection provides classification, labeling, and protection so you can track and control how information is used. Data can be classified as public or confidential according to standards you define for content, context, and source. These classifications can be applied automatically or manually, or you can suggest classifications so that your employees can decide what to apply.

Azure Information Protection is integrated with other Microsoft cloud services, such as Microsoft Office 365 and Azure AD. It can be used with your in-house line-of-business applications and information protection solutions from software vendors, whether these applications and solutions are on-premises or in the cloud.

To classify documents using Azure Information Protection, you must first configure your company's classification policy. Configure the policy by signing in to the Azure portal as an administrator, selecting Azure Information Protection in the apps list. All Azure Information Protection users start with a default policy that you can configure to suit your needs. Once you have created the policy that works best, publish your changes to deploy the policy to all managed apps and devices.

## Microsoft Outlook

Microsoft Outlook allows your employees to take files from any business or personal device, attach the file to emails, and access a dedicated library where all group files are stored. Navigate to your Microsoft OneDrive for Business and SharePoint locations to add permissions for your recipients in real time. When users send a document via Outlook and they select a OneDrive or SharePoint file to share, the Outlook attachment feature shows senders what permissions they're granting to the recipients. Users have the ability to change these permissions or attach a copy instead without having to go to where the file is stored.

## OneDrive for Business

You can share files with external partners through OneDrive for Business and apply security features such as password protection and multi-factor authentication to ensure that the document is viewed only by the right person.

## Office 365 Message Encryption and Office 365 Message Encryption viewer

If your employees need to send a sensitive message to external users, they can increase security by encrypting the message using Office 365 Message Encryption and the message recipient will decrypt the message using the Office 365 Message Encryption viewer.

## Microsoft Teams

Microsoft Teams is a collaborative, chat-enabled, mobile-friendly online work hub where your employees can store files, discuss projects, edit collaboratively, and converse wisely without needing to send intra-office email. Azure AD Conditional Access policies can be configured in Microsoft Teams to secure the data there. You can deploy Microsoft Teams through Microsoft System Center Configuration Manager (ConfigMgr) or through Microsoft Intune.

## Yammer

Yammer lets your employees know what's happening with each other day to day, from big company announcements to small, spontaneous ideas. Yammer offers security features to keep sensitive organizational data safe. It supports single sign-on authentication, allows admins to set password policies, provides admins with session management tools that let you see the devices that users are signed in to (and sign them out if needed), and offers a logical firewall that can restrict access to a specified IP range so that your network is accessible only in designated physical locations or through your organization's virtual private network (VPN). You can manage access and permissions in Yammer by setting up the Yammer network to comply with your organization's standards.

## Microsoft Cloud App Security

Microsoft Cloud App Security allows you to share documents securely via third-party applications. Use the tools in Microsoft Cloud App Security to discover and assess risks by identifying cloud apps on your network and gaining visibility into shadow IT. Then you can help protect your information using built-in or custom policies for data sharing and data loss prevention.

# How can I work on documents across devices and offline securely?

## Microsoft Intune

Manage mobile devices with Microsoft Intune through mobile device management (MDM). Then apply Intune App Protection Policy to help prevent data loss and better protect company data accessed, even when devices are used that you aren't managing. By implementing app-level policies, you can restrict access to company resources and keep data within the purview of your IT department.

## Office 365 and OneDrive for Business

You can use Office 365 apps offline, and OneDrive for Business files can also be saved to your hard drive through OneDrive sync so you can access them offline. The next time you connect to the internet, any documents you edited while you're offline will automatically upload to OneDrive for Business. With OneDrive for Business, your employees can sync files for offline use on any company-managed device. OneDrive for Business also syncs from SharePoint sites so your employees can keep files in File Explorer and access them offline.

# Deployment tips from our experts

## Enable security features in Office 365 apps

Office 365 apps like Outlook, OneDrive, Microsoft Teams, and Yammer all come with built-in features that enable users to more securely share files and be productive. A few simple things you can do include:

- Add permissions to file recipients in OneDrive for Business or SharePoint before sending in Outlook.
- Use password protection to ensure documents are viewed only by the right people.
- Send a sensitive message to external users securely by encrypting the message using Office 365 Message Encryption.
- Set password policies and manage security settings in Yammer.
- Configure Azure AD Conditional Access policies to secure the data in Microsoft Teams.

## Classify and share documents securely

Classify documents in Azure Information Protection to track and control how information is used. Then share documents securely via third-party applications using Microsoft Cloud App Security to protect your information.

## Prevent data loss on mobile devices

Manage mobile devices with Microsoft Intune and through MDM. Then implement app-level policies in Intune App Protection Policy to help prevent data loss.

## Plan for success with Microsoft FastTrack

FastTrack comes with your subscription at no additional charge. Whether you're planning your initial rollout, needing to onboard your product, or driving end-user adoption, FastTrack is your benefit service that is ready to assist you.

Get started at FastTrack for Microsoft 365.

Microsoft