Microsoft

Collaborate and share documents securely in real time

Introduction

Empower your employees to create, edit, and share a single document securely with multiple stakeholders. With Microsoft 365 security solutions, users can identify, classify, track, and protect documents to prevent leaks or access by unauthorized readers; these security solutions allow stakeholders to easily download a version for themselves with security that travels with the documents.

How can I make it easier for groups of people to work securely on the same document?

Microsoft Azure Active Directory (Azure AD)

To enable your employees to work more collaboratively without sacrificing security, you must first import employee identities into Azure AD and then integrate your on-premises directories with Azure AD using Azure AD Connect. This capability allows you to provide a common, secure identity for your users for Microsoft Office 365, Azure, and thousands of other software as a service (SaaS) applications that are integrated with Azure AD.

With a common, secure identity, you can enable single sign-on (SSO) and multi-factor authentication (MFA) for employees to sign in to Office 365. Office 365 includes collaborative productivity apps like SharePoint Online and OneDrive for Business, both of which allow for real-time editing, cloud syncing, and secure sharing and collaboration.

Azure AD business-to-business (B2B) collaboration

Azure AD B2B collaboration capabilities enable organizations using Azure AD to work securely with users from other organizations regardless of size. Organizations using Azure AD can provide access to documents, resources, and applications to their partners while maintaining complete control over their own corporate data (see Figure 1). Developers can use the Azure AD B2B application programming interfaces (APIs) to write applications that bring organizations together more securely. Partners can use their own credentials with no requirement to use Azure AD. B2B collaboration users (guest) can be added to your organization in the Azure portal.

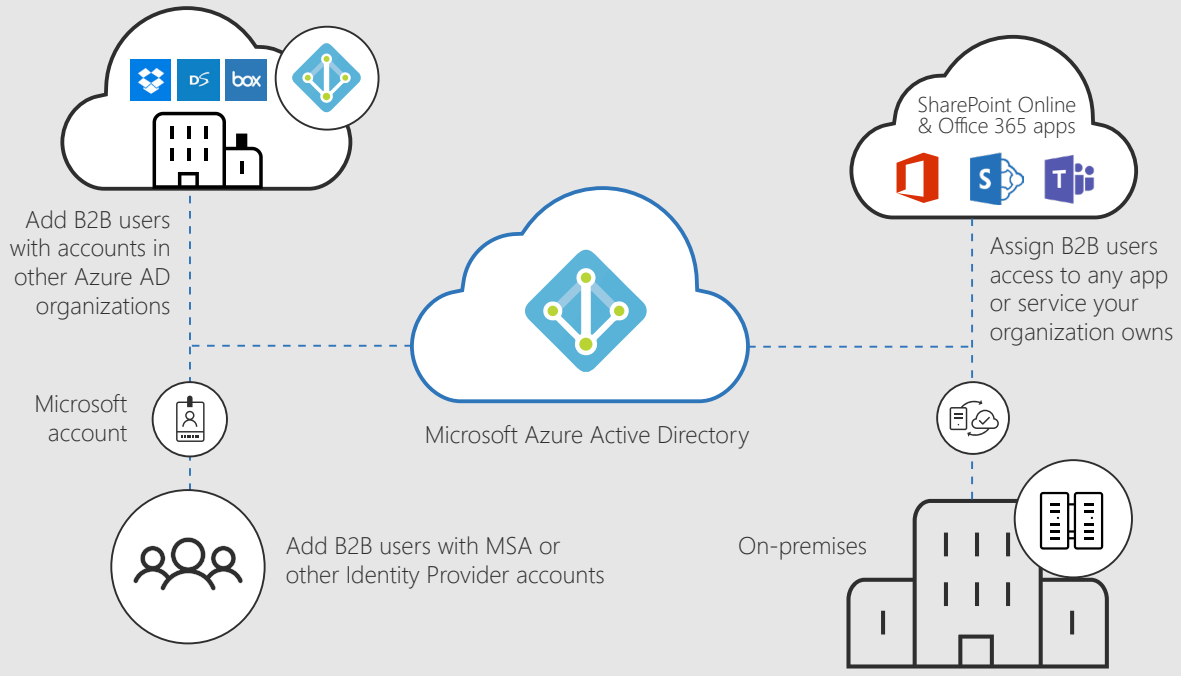

Figure 1. Azure AD B2B collaboration enables organizations using Azure AD to work securely with users from other organizations while maintaining control over their own corporate data.

Azure AD business-to-consumer (B2C) collaboration

Azure AD B2C is a cloud identity service allowing you to connect to any customer that puts your brand first. Governments and enterprises worldwide use Azure AD B2C to serve their applications to their citizens and customer's with fully customizable experiences while protecting their identities. You can build identities in Windows, Android, and iOS devices, or the web, and allow your customer's users to sign in with their existing social accounts or personal emails, including Microsoft accounts, Facebook, Google+, and LinkedIn. Learn how to set up identity management for the customers that use your application.

How can I protect organizational data while ensuring my users can view, edit, and share documents?

Azure Information Protection

Azure Information Protection is a cloud-based solution that helps you and your employees classify, label, and protect your documents and emails. It allows you to restrict who can view, edit, and share documents. Azure Information Protection offers several ways to classify data that will determine who can see, edit, or share a document. These classifications can be flexible: if an employee needs to override these classifications, you can require a justification for the override.

You can choose from several default sensitivity labels to use, such as "confidential" or "Internal only," or create custom labels according to your organization's needs. Sensitive documents are protected after they have been labeled and classified. You can track who opened a document and where, and then determine what that person can do with the document after it's opened. You can revoke access to the document at any time.

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 and select Azure Information Protection in the apps list. All Azure Information Protection users start with a default policy that you can then configure to suit your needs. Once you have created the policy that works best, publish your changes to deploy that policy to all managed apps and devices.

Microsoft Office 365 Message Encryption

Office 365 Message Encryption, an online service that is built in to Azure Information Protection, allows your organization to send and receive encrypted email messages between people inside and outside the organization. Email message encryption helps ensure that only intended recipients can view message content. Office 365 Message Encryption works with Outlook.com, Yahoo!, Gmail, and other email services.

Office 365 administrators can define message flow rules to determine the conditions for encryption. For example, a rule can require the encryption of all messages addressed to a specific recipient.

Microsoft Data Loss Prevention (DLP) in Microsoft Exchange

Microsoft DLP helps identify, monitor, protect, and prevent accidental sharing of sensitive information in Office 365 products. Microsoft DLP allows you to identify sensitive information across Exchange Online, SharePoint Online, and OneDrive for Business. For example, you can identify any document containing a credit card number that's stored in any OneDrive for Business site, or you can monitor just the OneDrive sites of specific people. Microsoft DLP lets you prevent the accidental sharing of sensitive information. For example, you can identify any document or email containing a health record that's shared with people outside your organization and automatically block access to that document or block the email from being sent. You can also monitor and protect sensitive information on desktop and online versions of Microsoft Excel, PowerPoint, Word, SharePoint, and OneDrive for Business.

You can define your own custom policies and email flow rules, or use the Microsoft DLP policy templates to help you choose the conditions, rules, and actions to define a DLP policy that will help you inspect messages. To create and manage DLP policies on the data loss prevention page, go to the Office 365 Security and Compliance Center.

Azure Information Protection scanner

For organizations with an on-premises directory, you can deploy the Azure Information Protection scanner to classify existing documents. The scanner helps you to discover, classify, label, and protect documents so that those protections travel wherever the documents do.

OneDrive for Business

OneDrive for Business offers options for protecting and controlling the flow of organizational information. For example, you can block file syncing on unmanaged devices, audit actions on OneDrive for Business files, and use mobile device management policies to manage any device that connects to your organization's OneDrive for Business account. You can control as much or as little of your employee permissions as you need to.

OneDrive for Business prevents sensitive information from leaking by allowing you to restrict who can share or receive a document. You can manage sharing settings for OneDrive for Business and SharePoint Online together. If you don't allow your employees to share externally through SharePoint, they can't share externally through OneDrive for Business. If you change your external sharing settings at any time, links shared beyond your organization will stop working.

Furthermore, you can block or limit access to SharePoint and OneDrive for Business content from unmanaged devices (those not joined to a domain or aren't compliant in Microsoft Intune). You can block or limit access for employees or groups of employees in addition to sites within your organization or other site collections.

You can also allow your employees to control permissions on their documents. Employees can designate documents as read-only, and limit who can access documents by restricting sharing to direct-link only.

Deployment tips from our experts

Start by provisioning employee identities in Azure AD

Identity is the foundation for secure collaboration. Your first step is to import employee identities into Azure AD and then integrate your on-premises directories with Azure AD using Azure AD Connect.

Collaborate securely with other organizations

With Azure AD B2B and B2C capabilities, you can work securely with customers and partners.

Protect documents and emails

Help protect information through access control, classification, and labeling that extend to shared documents and external stakeholders with Azure Information Protection. Then define message flow rules in Office 365 Message Encryption to determine the conditions for email encryption.

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