All Things M365

Empower to Achieve

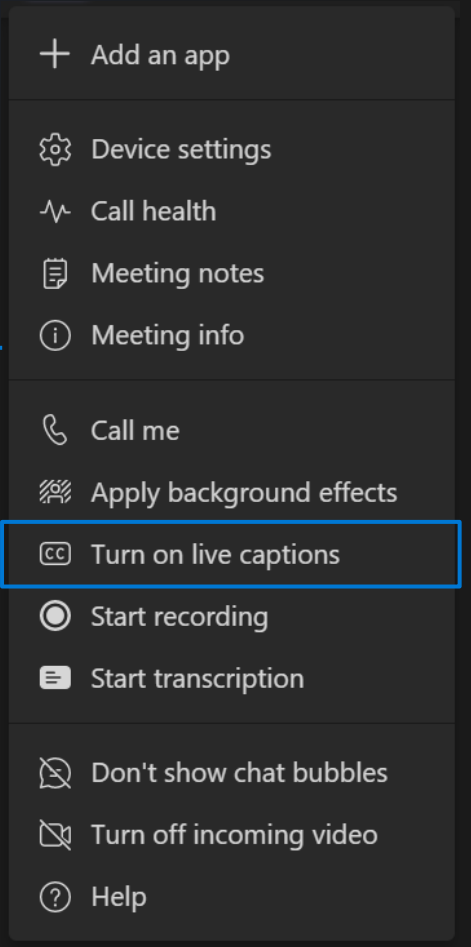
Understanding Permissions in SharePoint, OneDrive and Microsoft Teams

Microsoft Teams meetings

Need help? Use the Chat for questions or support.

MEETING CONTROLS

More actions
Including turn on live captions



Send chat messages

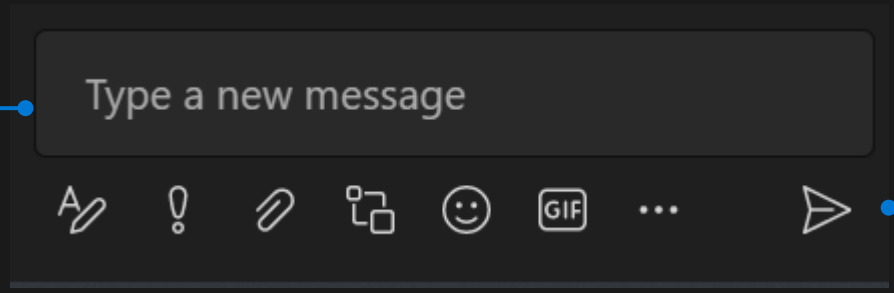
Raise your hand

Unmute or mute your microphone
Only with permission

Share your screen
Only with permission

CHAT OPTIONS

Type a message



Send your message

Introduction

About Me

Working with every version of SharePoint, OneDrive, M365, and Teams since the start of SharePoint in the late 90's when Microsoft purchased Vermeer Technologies Inc, and later what was then Office 365 in 2010. Joined the State and DIT 8 years ago. Currently working as the Sr. Enterprise M365 Admin for Enterprise Collaboration Services

About This Session

Permissions in M365 can be very simple or very complex. But usually it's pretty complex. I remember the first white paper I started reading from Microsoft on Permissions in 365 and it was close to 100 pages long. Needless to say I did not read every single page, but I feel like I experienced every single problem, including poor planning and a lack of understanding about permissions over the 27 years I've been doing this. Let's just say that Permissions are one of the very top issues you will have in SharePoint, OneDrive and Teams. And one of the hardest issues to fix, even by us admins. However, you can avoid those issues by planning permissions, and keeping your permission structures simple and clean.

Best Overall Practices for Permissions in M365

- Be aware of what permissions your content needs, and what that content is. Don’t be responsible for a data breach.
- Practice good document management
- Plan out your permissions and content structure in advance, so it makes sense, and is simple.
- Do not try to create 100’s of unique, granular permissions in one document library.
- Do not make a habit of breaking “inheritance”
- Practice “least privilege” – don’t grant a higher permission level than your users must have to work with content.
- Do not allow your users to invite others to your sites and content. Leave this permission to “owners only”.

Don’t Over Complicate.

Or: “The further you get down into the weeds, the more difficult it is to support.”

Permissions in OneDrive for Business

- OneDrive is your own, personal location for content you're working on. You fully own all content and nobody else can see it, access it, or find it in a search UNLESS you personally grant permission or share it with others.
- The nice thing about your OneDrive files is that the default view clearly tells you if a file or folder is "shared" with others.
- Again, don't make so many "granular" or "unique" permissions that you cannot keep up with it.
- Always know who has access to your content, and remove them later on if you need to.

Let's Take A Look

Permissions in SharePoint

- SharePoint Access is primarily accomplished through the use of three default “SharePoint Groups”
  - Visitors, Members, Owners. NEVER delete, or rename any of the default SharePoint groups!
- Do not break permission inheritance. You can break inheritance, requiring further permissions for individual content, lists, and libraries. While this can be an excellent way protect data, it can cause problems and administrative nightmares when overused.
- Plan your permission strategy
  - Understand the “point” of your site. Who's the target audience? What should users be able to do? What should the site be able to do? Who is the site owner? These are important questions to ask yourself. If you know the details, the entire planning process becomes easier.
  - SharePoint includes a set of permission levels for a reason. These levels are well documented and balanced to what users need to do. If you mostly keep or build off of these, you rarely have security issues. Sometimes it is necessary to edit or create permission levels. However, the permission levels included with SharePoint out-of-the-box will satisfy the majority of security requirements. If you find yourself creating a lot of new permission levels, something may be wrong. Custom levels are useful, but you should only use them as needed.
  - Don’t overcomplicate security when it comes to content access. Only secure content when there is a real security risk. Over securing content can make it a nightmare for users who need to access content and for the site managers who have to process access requests. Additionally, user adoption will suffer when users cannot access what they need when they need it. Simplifying permissions can help avoid frustration for both the users and site managers.

Let’s Take A Look

Permissions in Microsoft Teams

- Teams has two layers, and two different types of permissions making it extremely important to think about and plan out permissions.
  - The primary Teams permissions are AD groups/O365 Groups.
  - SharePoint is the “container” under Teams and has it’s own permission type which is based on SharePoint Groups.
- ALWAYS add users to your Team using Microsoft Teams! Do not grant access in the SharePoint site underneath.
- If you have a Microsoft Team, use it! Do not have your users “mix” and jump between SharePoint and Teams all the time. There’s very little you can’t do in the Teams interface these days.
- Only the “mechanic” [Team Owners] should go in and work in the SharePoint side of Teams to avoid confusion.
- NCDIT Teams do not have private channels. Once a member of a Team, you can collaborate on just about everything in the Team.
- There are no “visitors” in Teams.
- While you can create/add unique, granular permissions in the SharePoint site under Teams, it is not advised to do it on a regular basis. If you do, you need a SharePoint site, not a Team.

Let’s Take A Look