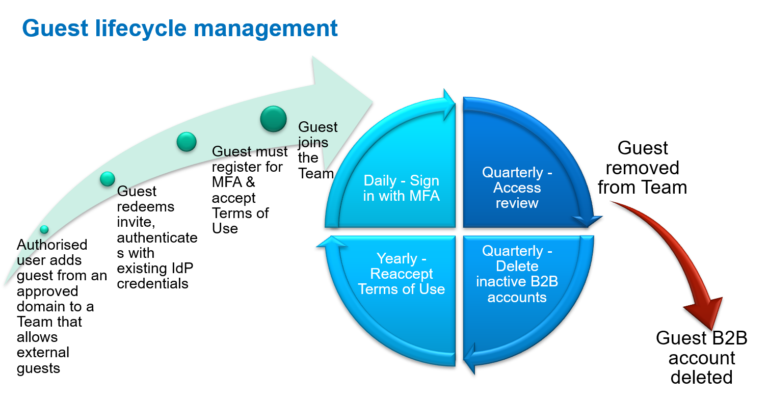
**Collaborate securely with guests in Microsoft Teams**



It is important that you allow employees to collaborate with external guests in Microsoft Teams. This way you remain in control of your data and you control the access to the data. However it is important to put the appropriate controls in place to enable your organisation to collaborate **securely**with guests in Microsoft Teams and in addition effectively manage the guests lifecycle.

Here are the top 10 tips to enable your organisation to collaborate securely with guests in Microsoft Teams.

**Benefits of enabling secure guest collaboration in Teams**

If you have not enabled guest access in Teams. Then why not? Most organisations need to collaboration with external people such as suppliers, customers or partners as part of their business activities. If you block your employees collaborating securely with guests in Teams then where are they collaborating? Are they sending you important data via email attachments? In this case you have lost control of your data the minute the send button is pressed.

Employees are smart, they will find alternative ways to collaborate and support their productivity. Its likely that these ‘alternative’ IT solutions that are being used without the approval of, and often even without the knowledge of, corporate IT organisations. You increase your security risks as you are no longer in control of your data.

By enabling guest collaboration in Teams you can minimise security risks to your data

1. Remain in full control of your data
2. You data does not leave your organisation
3. Define who has access to what information
4. Apply appropriate access controls to the guests accounts
5. Guest access is audited

**Top 10 tips to collaborate securely with guests in Microsoft Teams.**

Here are my top 10 tips on how to collaborate securely with guests in Microsoft Teams.

**1. Which domains guests can invited from**

When you enable guest access in Azure AD you can invite guests from any domain. Some organisations only what to collaborate externally in Teams with some specific organisations. In this scenario create an **Allow**list in Azure AD for your domains and add in the domain names of the organisations you want to collaborate with. Alternatively you may want to stop collaboration with users from specific domains, such as stopping guests from a personal email address. In this scenario you can create a **Blocked**list in Azure AD and add in the domains you want to block.

**2. Define who can invite guests**

By default anyone can invite guests into the tenant. This includes allowing existing guest users to invite other guests users. This maybe too open so you can change the setting to make it more restrictive. You can stop guests from inviting other guests and you can restrict it to an admin only role.

**3. Create a guest specific Acceptable Use Policy**

Guests are not internal staff so have no access to your internal Acceptable User Policy (AUP). This is not a problem as you can create a guest specific (AUP) using the Azure AD Conditional Access Terms of Use. Upload your AUP in PDF format as The Terms of Use. You have the option to set a start date to enforce the policy and a review period. Finally assign the conditional access policy to all guest users accessing Office 365 application.

**4. Enforce MFA for guests using your Azure MFA**

MFA is best practice for all accounts and not just your internal users. You can enforce MFA for all guests and limit their session time by using Conditional Access Policies.

If you do not use Azure MFA for your internal users then you need to configure the Azure MFA permissions first. Use the mobile app rather than text message, as it is more secure and in addition the text messages will incur text charges. Once configured then update the Conditional Access Policy for your guests to enforce MFA.

**5. Control a guest’s sign in frequency**

As you are not in control of guests devices or the protection they have on the device it is important to limit how long they have access before needing to sign-in again. Use a Conditional Access Policy to control the sign-in frequency for guest users. This can be set in number of hours or days. e.g. every 4 hours.

**6. Review your existing Conditional Access Policies to make sure you are not inadvertently blocking guests**

Review your existing Conditional Access Policies to make sure you do not inadvertently block guest from signing in. If you are controlling access to Office 365 from named locations (such as an office) only or needing to use a hybrid joined device or device marked as compliant then you will block guest access. This is because guests are unlikely to be accessing from one of your office or from a one of your managed devices. In addition the user risk and sign in risk can also cause issues for guests.

To overcome this add an exclusion in the relevant Conditional Access policies to exclude guest users from the policy. If the policy scope is broad such as all cloud apps then you may want to make the policies more granular and create a separate policy for Office 365 apps where guests can be added.

**7. Configure guest functionality in the Teams admin center**

In the Teams Admin centre can control features guest users can use via the Guests Access Settings for example block private calls, control, screen sharing or stopping guests editing or deleting messages.

**8. Control guest access on a per Team basis by using sensitivity labels**

When you enable guest access in Teams, all Team owners can add guests into their Teams. To control guest access on a Team by Team basis set up sensitivity labels for groups & sites. These labels will control external guest access and your SharePoint site sharing permissions. Once configured when a user creates a Team they select a sensitivity label which either allows or blocks guest access to the new Team.

**9. Regularly review guest access to see if they still need access**

Your guests are not part of your internal joiners, movers or leavers process so managing the lifecycle of a guests is often overlooked.

Therefore it is important to put in place a regular review of your guests to still see if they need access. Setting up an Azure AD Access Review will allow you to set up a review of all guests on a regular basis, such as every 6 months. Once set up either the Team owner, nominated user(s) or the guests themselves can undertake the review. At the end of the review any guests that are marked as denied can be automatically removed from the resources. and therefore lose access to the Team(s).

**10. Regularly delete the B2B accounts of inactive guests**

It is important to note that when a guest account is removed from a Team that their Azure AD account is not deleted. This is because a guest could be still active in multiple teams or other resources. Therefore over time the number of Azure AD B2B accounts will increase and so will the number of inactive B2B accounts. It is important to either extend the scope of the Access review to block and delete all denied guests. Alternatively run ran inactive guests report on a regular basis to identify your inactive guests. The output can be used to bulk delete the guest accounts in Azure AD Admin centre.