**Running an Azure AD Access Review for Every Guest in Every Group**

When I wrote about [Azure AD Access Reviews for Office 365 Groups](https://petri.com/azuread-access-reviews-group-membership) (now Microsoft 365 Groups) in November 2017, I concluded that “*any tenant that wants to use access reviews to control external access to Office 365 Groups or Microsoft Teams faces the challenge of having to create individual access reviews for each group that has guest members*.” It’s taken Microsoft a while, but now they’ve launched [the public preview for access reviews covering guest users in all Teams and Groups](https://techcommunity.microsoft.com/t5/azure-active-directory-identity/access-reviews-for-guests-in-all-teams-and-microsoft-365-groups/ba-p/1994697) in a tenant.

It’s not as if a major technical challenge exists to know what groups have guest members. Perhaps the impulse comes from the [ongoing success of Teams](https://office365itpros.com/2020/10/28/teams-115-million-users/) and the fact that every team is underpinned by a Microsoft 365 group. Many companies exploit Azure B2B collaboration in Teams to share information and work with people in other organizations (I am a guest member in seven other tenants). The upshot is that you end up with lots of guest accounts. With over 500,000 users, Accenture is [the world’s largest Teams deployment](https://www.accenture.com/_acnmedia/pdf-19/accenture-microsoft-collaboration-capabilities.pdf), and the number of teams with guests it must manage is probably mindboggling.

**Creating an All-Guests Access Review**

If you’ve created access reviews before, you’ll find it simple to set up the preview. Go to the Identity Governance section of the Azure AD admin center, select Access reviews, and create a new review. Figure 1 shows that we’ve selected the scope is all groups (including groups with [guests used for Yammer communities](https://petri.com/yammer-previews-support-for-azure-b2b-collaboration)) and that the review covers only guests instead of all members.

Image 1 Expand

Graphical user interface, application

Description automatically generatedFigure 1: Creating a new Azure AD access review (image credit: Tony Redmond)

The next step is to nominate the people who will do the review and the review period. Usually, the best people to decide whether a guest should retain their access is the group/team owner. You can choose other people to review membership with the caveat that these people should know why the guest was added to a group membership.

The settings in Figure 2 show that we’ve opted for an annual review and that the review cycle will continue indefinitely (no end date is set). The duration is 182 days, meaning that reviewers have this time to perform the review and decide to keep or deny membership to guests.

Image 2 Expand

Graphical user interface, application

Description automatically generatedFigure 2: Nominating the reviewers and review period for the access review (image credit: Tony Redmond)

The review settings (Figure 3) dictate what happens when reviewers assess guest members. We can see that if they don’t do anything, membership is left unchanged. If they do decide, Azure AD can auto-apply their choice (enable auto-apply results) or leave the membership to be manually adjusted (disable auto-apply results). In most cases, it’s best to auto-apply results, especially if no change happens when a review isn’t done.

Image 2 Expand

Graphical user interface, application

Description automatically generatedFigure 3: Settings for the access review (image credit: Tony Redmond)

The ability to be notified about guest sign-in history is an interesting “decision helper.” If the guest hasn’t signed in within the last 30 days, their account is flagged on the basis that an unused membership could be removed (you can use the [same sign-in data for reporting guest access](https://petri.com/use-powershell-fetch-account-signin-data-from-graph) for up to 180 days).

**Email Reminders**

The settings chosen for the review opted for email notifications. Once the review begins, Azure AD sends email to the owners of each group with guests to prompt them to review their guest members (Figure 4 – the logo used in the message is an example of [custom branding for Azure AD](https://office365itpros.com/2020/03/04/azure-active-directory-backgrounds/)).

Image 4 Expand

Graphical user interface, text, application, email

Description automatically generatedFigure 4: Email reminder that an access review is requested (image credit: Tony Redmond)

Some up-front communication is needed to let group owners know that reviews are about to start and what they need to do. If this doesn’t happen, group owners might be underimpressed to receive a blizzard of messages in a short period (I received 26).

**Progressing Access Reviews**

Clicking the *Start review* link in the message brings the group owner to the My Access page where they can access the membership data for the groups to review via the Access reviews link. After selecting a group, the decision can be made to approve, deny, or “can’t make up my mind” for each guest (Figure 5). Or if they want to depend on Azure AD, they can take the *Accept recommendations* option and have Azure AD do the work.

Image 5 Expand

Graphical user interface, text, application, email, website

Description automatically generatedFigure 5: Performing an access review for guest members (image credit: Tony Redmond)

The problem about letting Azure AD decide is that some sparse criteria are used. As far as I can see, Azure AD denies access to any guest who hasn’t signed in within the last 30 days. This might be what you want, but a 30-day period is too short to use as a basic rule. People do take vacations and guests don’t sign into other tenants unless they need to, such as to access a document or take part in a Teams conversation. Fortunately, it’s easy to reverse an automatic decision and do the right thing by selecting and editing the guest entry (Figure 6).

Image 6 Expand

Graphical user interface, application

Description automatically generatedFigure 6: Correcting an automatic decision (image credit: Tony Redmond)

In fairness, Microsoft recognizes that the 30-day cutoff is a blunt instrument to decide to deny or approve recommendations. Expect to see the ability to customize the period in the future. However, even if Microsoft allows tenants to go back 180 days, sign-in data is sometimes no indicator of guest activity. For instance, guests in Outlook groups use email for communication and might never sign into the host tenant.

One thing I noticed is that if new guests are added to a group after a review commences, they don’t show up for the review. The logic here is that someone (group owner or admin) has decided that the guest should be in the group, so there’s no need to review that call. Also, it prevents the “shifting sands” problem where reviewers don’t know when a review cycle is complete.

**Completing the Review**

Eventually, the review period completes, and Azure AD then applies the decisions made by group owners. Unlike other access reviews, Microsoft hasn’t added the ability for an administrator to stop a review early to apply the access decisions.

Azure AD administrators can review details of how access reviews are progressing through the admin center (Figure 7). However, I can’t imagine this being done in large tenants where this policy might cover thousands of groups. This seems like an opportunity for ISVs to build better dashboards and tools to help large tenants cope with guest access reviews.

Image 7 Expand

Graphical user interface, application

Description automatically generatedFigure 7: The Azure AD administrator view of an access review (image credit: Tony Redmond)

Microsoft hasn’t included cmdlets to interact with access reviews in the AzureAD PowerShell module, but you can use the Graph to fetch details of reviews by issuing calls with the *Invoke-RestMethod* cmdlet or the Graph module for PowerShell. The [documentation for the API](https://docs.microsoft.com/en-us/graph/api/resources/accessreviewsv2-root?view=graph-rest-beta) is available online.

**Licensing**

Azure AD Premium P2 licenses are required for those involved (creating or administering) in access reviews. Microsoft describes the requirement and gives some examples of how to calculate how many licenses an organization might need [on this page](https://docs.microsoft.com/en-us/azure/active-directory/governance/access-reviews-overview).

**Good Feature for Large Organizations**

Having the ability to create an access review that takes in all groups with guests in a tenant is a nice feature that is likely to be popular with large organizations, especially those who have Azure AD Premium P2 licenses already. Smaller tenants can approach the problem in different ways using tools like PowerShell to [track guest membership of groups](https://office365itpros.com/2019/10/15/report-old-guest-accounts-office365-groups/) or to [find out if guests are active](https://petri.com/guest-account-obsolete-activity).

One gap which remains is for tenant administrators to [know what users do as guests in other tenants](https://petri.com/problem-guest-users-outside-tenant). Perhaps Microsoft will deliver an access review with that scope next?