Microsoft

Managing Microsoft Teams

Exam Ref MS-700

Ed Fisher

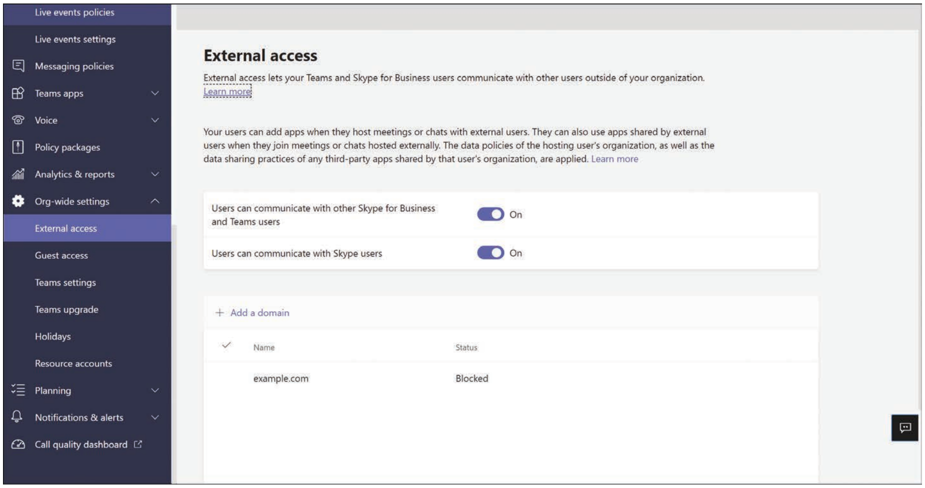
Microsoft

Exam Ref MS-700 Managing Microsoft Teams

Ed Fisher

controlled in Org-wide settings, and can be turned off or on, and it can be configured explicitly to either allow or block specific SIP domains. You also have the option to allow or block communication with users of the Skype consumer service. To configure messaging and calling options for guests, follow these steps:

1. Log on to the TAC at *https://admin.teams.microsoft.com*.
2. In the left menu, scroll down to **Org-wide settings**, and select **External access**.
3. To permit external access, turn on both settings as shown in Figure 1-27.



External access

External access lets your Teams and Skype for Business users communicate with other users outside of your organization. Learn more

Your users can add apps when they host meetings or chats with external users. They can also use apps shared by external users when they join meetings or chats hosted externally. The data policies of the hosting user's organization, as well as the data sharing practices of any third-party apps shared by that user's organization, are applied. Learn more

Users can communicate with other Skype for Business and Teams users: On

Users can communicate with Skype users: On

+ Add a domain

✓	Name	Status
	example.com	Blocked

FIGURE 1-27 Settings for External access

4. If you want to block a specific domain or domains, you can do so by selecting **+Add a domain** and adding the specific DNS suffixes you wish to block. Or if desired, you can add only those domains you wish to permit.
5. Select **Save** to save any changes.

REAL WORLD THERE ARE TWO SIDES, AND DNS REQUIREMENTS TOO

Before your users can have VoIP calls and chat with external users, both SIP domains must have policies that permit the external access. If your organization settings allow all, but the other organization only allows specific domains and yours is not on the list, your users will not be able to communicate with users in the other organization. External access also requires that both domains have the appropriate SRV records in place for Open Federation. See *https://docs.microsoft.com/en-us/microsoft-365/enterprise/external-domain-name-system-records?view=o365-worldwide#external-dns-records-required-for-skype-for-business-online* for more information.

Remove guests

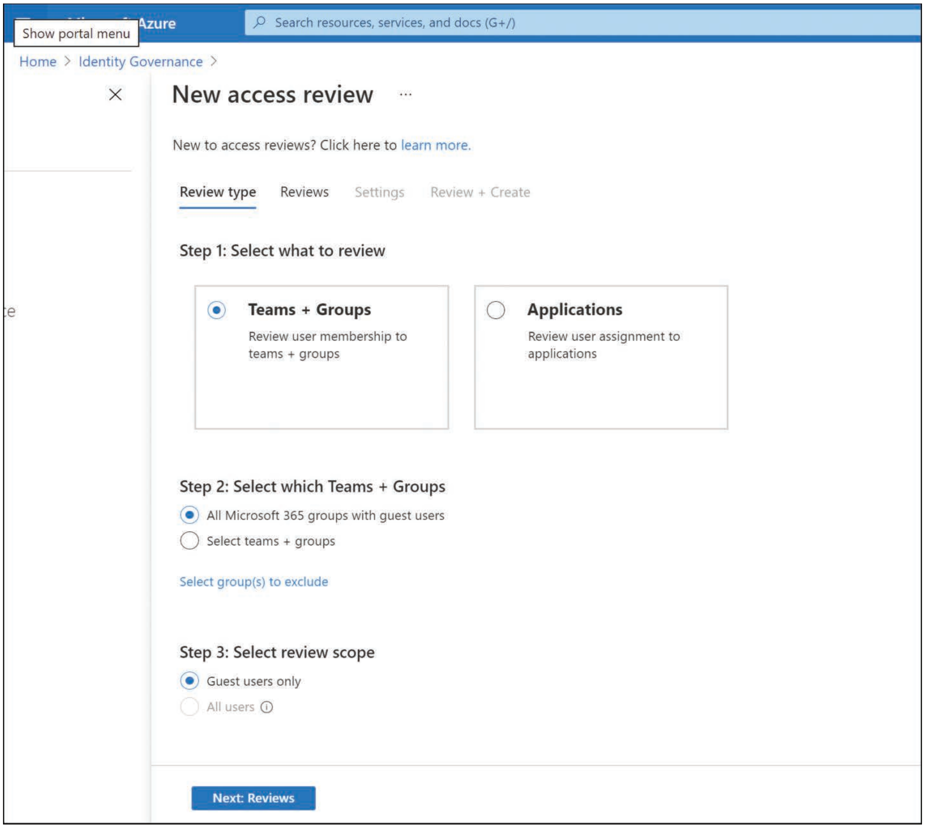
Teams owners can remove guests from their specific teams. When an admin needs to remove a guest user from the organization, they can do so using the Azure Active Directory portal. To do this, follow these steps:

1. Log on to the Azure AD portal at *https://portal.azure.com*.
2. In the Search box, type **users** and then select **Users** under **Services**.
3. You can search or sort or filter for guest users. To filter, select **Add filters** and then select **User type** and select **Apply**.
4. Select **Guest** and select **Apply**.
5. Select the user or users you wish to remove, and select **Delete user**.

Manage Azure AD access review for guests

Access reviews are a powerful tool for reviewing access to Microsoft Teams and other corporate resources. These can be scheduled automatically to force a review of who has access to what, both to ensure that access is still valid and that the people with access still have a need. Access reviews are an Azure AD Premium Plan 2 feature and require either a Global Administrator or a User Administrator to initiate an access review in the Azure AD portal. They can assign any team owner to review the access to their team. To create an access review for all guest users in all teams, do the following:

1. Log on to the Azure AD portal at *https://portal.azure.com*.
2. In the Search box, enter **Identity Governance** and press Enter.
3. In the left menu, select **Access reviews**.
4. Select **+ New access review** to begin.
5. On the first screen, select **Teams + Groups**, and then select the radio button next to **All Microsoft 365 groups with guest users**. Leave the scope set to the default **Guest users only**. Then select **Next: Reviews**. This is shown in Figure 1-28.



Show portal menu
Azure
Search resources, services, and docs (G+/)
Home > Identity Governance >

New access review ···

New to access reviews? Click here to learn more.

Review type
Reviews
Settings
Review + Create

Step 1: Select what to review

● **Teams + Groups**
Review user membership to teams + groups

○ **Applications**
Review user assignment to applications

Step 2: Select which Teams + Groups

● All Microsoft 365 groups with guest users
○ Select teams + groups

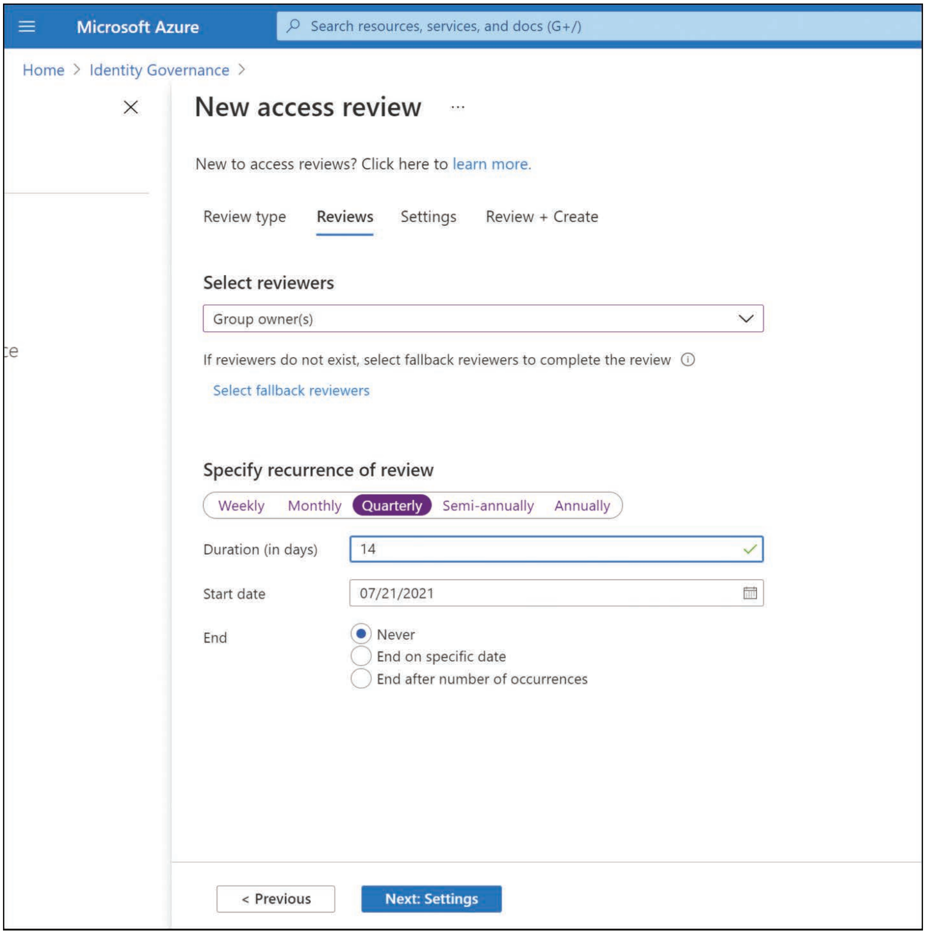
Select group(s) to exclude

Step 3: Select review scope

● Guest users only
○ All users ⓘ

FIGURE 1-28 Settings for guest access review

6. On this screen, you can select who is to perform the review, and how often they should do this. If all Microsoft 365 Groups have owners, you can select **Group owner(s)** to assign the reviews automatically. You can also select a fallback reviewer if any group no longer has an owner.
7. Then select the frequency, the duration (how long the reviewer has to complete the review), and if you wish ,the cycle of review to end at a specific date or after a specific number of iterations. When finished, select **Next: Settings**. Example review options are shown in Figure 1-29.


Microsoft Azure
Search resources, services, and docs (G+/)
Home > Identity Governance >

New access review

New to access reviews? Click here to learn more.

Review type
Reviews
Settings
Review + Create

Select reviewers

Group owner(s)

If reviewers do not exist, select fallback reviewers to complete the review

Select fallback reviewers

Specify recurrence of review

Weekly Monthly [✓ Quarterly] Semi-annually Annually

Duration (in days): 14

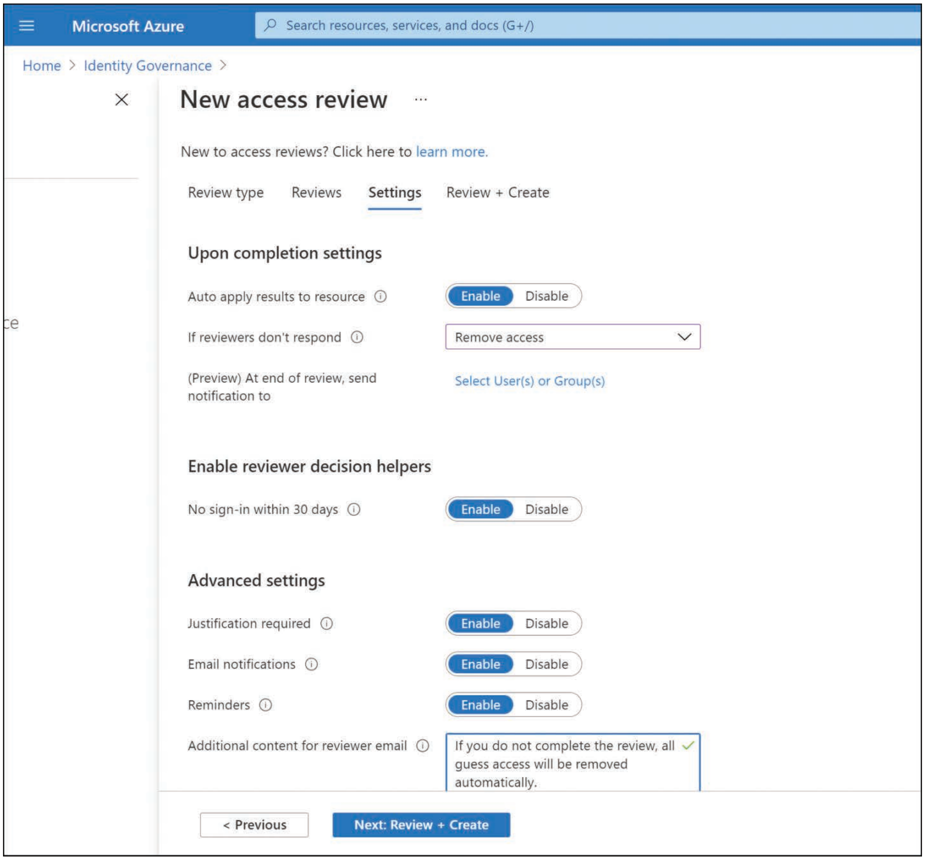
Start date: 07/21/2021

End:
● Never
○ End on specific date
○ End after number of occurrences

< Previous
Next: Settings

FIGURE 1-29 Additional settings for guest access review

8. On the next screen, you can set actions and responses based on results or lack of response by the group owner, as well as provide additional information to the reviewer, such as the last time a guest actually accessed the content. This can help a reviewer determine if the guest's access is still being used. Examples are shown in Figure 1-30. When you are satisfied with the settings, select **Next: Review + Create**.



New access review ···

New to access reviews? Click here to learn more.

Upon completion settings

Auto apply results to resource: Enable

If reviewers don't respond: Remove access

(Preview) At end of review, send notification to: Select User(s) or Group(s)

Enable reviewer decision helpers

No sign-in within 30 days: Enable

Advanced settings

Justification required: Enable

Email notifications: Enable

Reminders: Enable

Additional content for reviewer email: If you do not complete the review, all guess access will be removed automatically.

FIGURE 1-30 Additional settings for guest access review

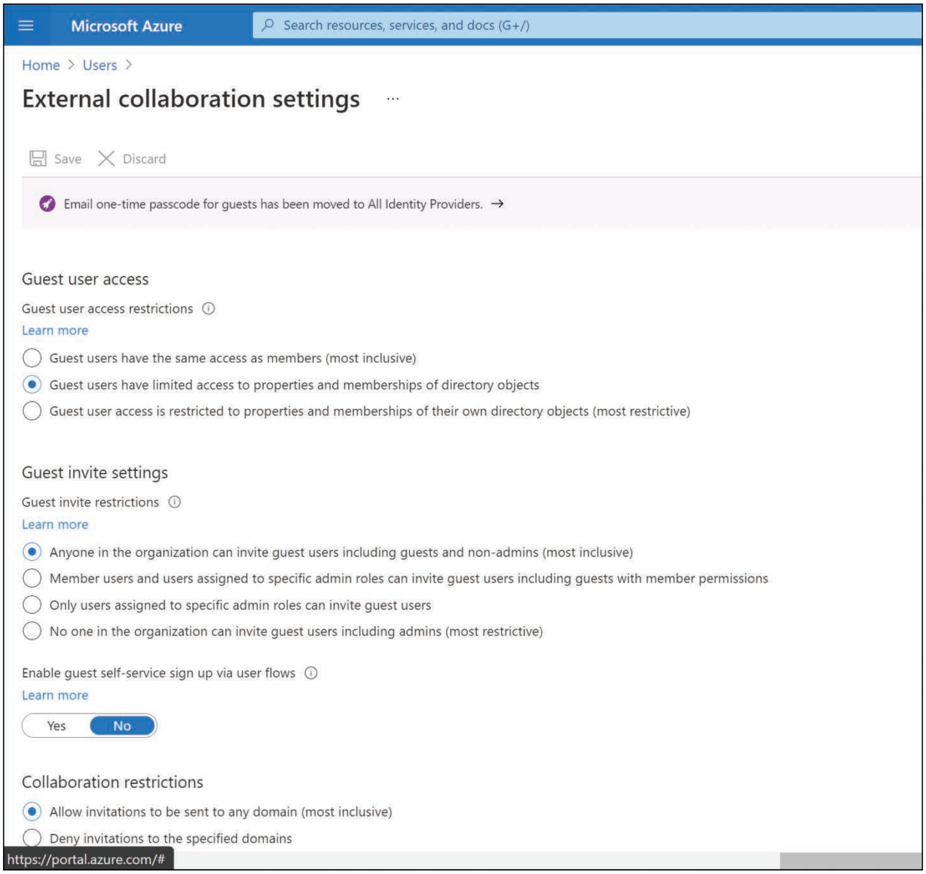
9. You can review or make changes on the final screen, and then select **Create** when done. It may take a few moments before the access review you created will show up in the main Access review console.

You can create multiple access reviews if necessary, and adjust them through the Azure portal if assigned reviewers need to change or if you have to revise the frequency or actions. By completing periodic access reviews, you help reduce the chance that someone has access to data they no longer need. This, in turn, helps with the overall security posture of your environment and makes permitting guests access to Teams more palatable to others in your organization who might otherwise be resistant to it.

Configure guest access from Azure AD portal

The last component of guest access in Teams is configuring guest access settings in the Azure AD portal. External collaboration settings are accessible under the Users blade and are specific to overall access, invitations, and allowed/denied domains. To adjust external collaboration settings, do the following:

1. Log on to the Azure portal at *https://portal.azure.com*.
2. Enter **Users** in the search box and press Enter, or select **Users** from the recent shortcuts below the search bar.
3. In the left menu, select **User settings**, and under **External users**, select **Manage external collaboration settings**.
4. Note the options include limiting access to directory data, who can invite guests, and the option to permit or deny specific domains. These are shown in Figure 1-31.



External collaboration settings

Email one-time passcode for guests has been moved to All Identity Providers. →

Guest user access

Guest user access restrictions ⓘ

Learn more

○ Guest users have the same access as members (most inclusive)
● Guest users have limited access to properties and memberships of directory objects
○ Guest user access is restricted to properties and memberships of their own directory objects (most restrictive)

Guest invite settings

Guest invite restrictions ⓘ

Learn more

● Anyone in the organization can invite guest users including guests and non-admins (most inclusive)
○ Member users and users assigned to specific admin roles can invite guest users including guests with member permissions
○ Only users assigned to specific admin roles can invite guest users
○ No one in the organization can invite guest users including admins (most restrictive)

Enable guest self-service sign up via user flows ⓘ

Learn more

Yes [✓ No]

Collaboration restrictions

● Allow invitations to be sent to any domain (most inclusive)
○ Deny invitations to the specified domains

https://portal.azure.com/#

FIGURE 1-31 External collaboration settings in the Azure portal