Manage users excluded from Conditional Access policies - Microsoft Entra ID Governance

By OWinfreyATL

Archived: 2026-04-05 20:44:21 UTC

In an ideal world, all users follow the access policies to secure access to your organization's resources. However, sometimes there are business cases that require you to make exceptions. This article goes over some examples of situations where exclusions could be necessary. You, as the IT administrator, can manage this task, avoid oversight of policy exceptions, and provide auditors with proof that these exceptions are reviewed regularly using Microsoft Entra access reviews.

Note

A valid Microsoft Entra ID P2 or Microsoft Entra ID Governance, Enterprise Mobility + Security E5 paid, or trial license is required to use Microsoft Entra access reviews. For more information, see Microsoft Entra editions.

Let's say that as the administrator, you decide to use Microsoft Entra Conditional Access to require multifactor authentication (MFA) and limit authentication requests to specific networks or devices. During deployment planning, you realize that not all users can meet these requirements. For example, you could have users who work from remote offices, not part of your internal network. You could also have to accommodate users connecting using unsupported devices while waiting for those devices to be replaced. In short, the business needs these users to sign in and do their job so you exclude them from Conditional Access policies.

As another example, you might be using named locations in Conditional Access to specify a set of countries and regions from which you don't want to allow users to access their tenant.

Unfortunately, some users might still have a valid reason to sign in from these blocked countries/regions. For example, users could be traveling for work and need to access corporate resources. In this case, the Conditional Access policy to block these countries/regions could use a cloud security group for the excluded users from the policy. Users who need access while traveling, can add themselves to the group using Microsoft Entra self-service Group management.

Another example might be that you have a Conditional Access policy blocking legacy authentication for most of your users. However, if you have some users that need to use legacy authentication methods to access specific resources, then you can exclude these users from the policy that blocks legacy authentication methods.

Note

Microsoft strongly recommends that you block the use of legacy protocols in your tenant to improve your security posture.

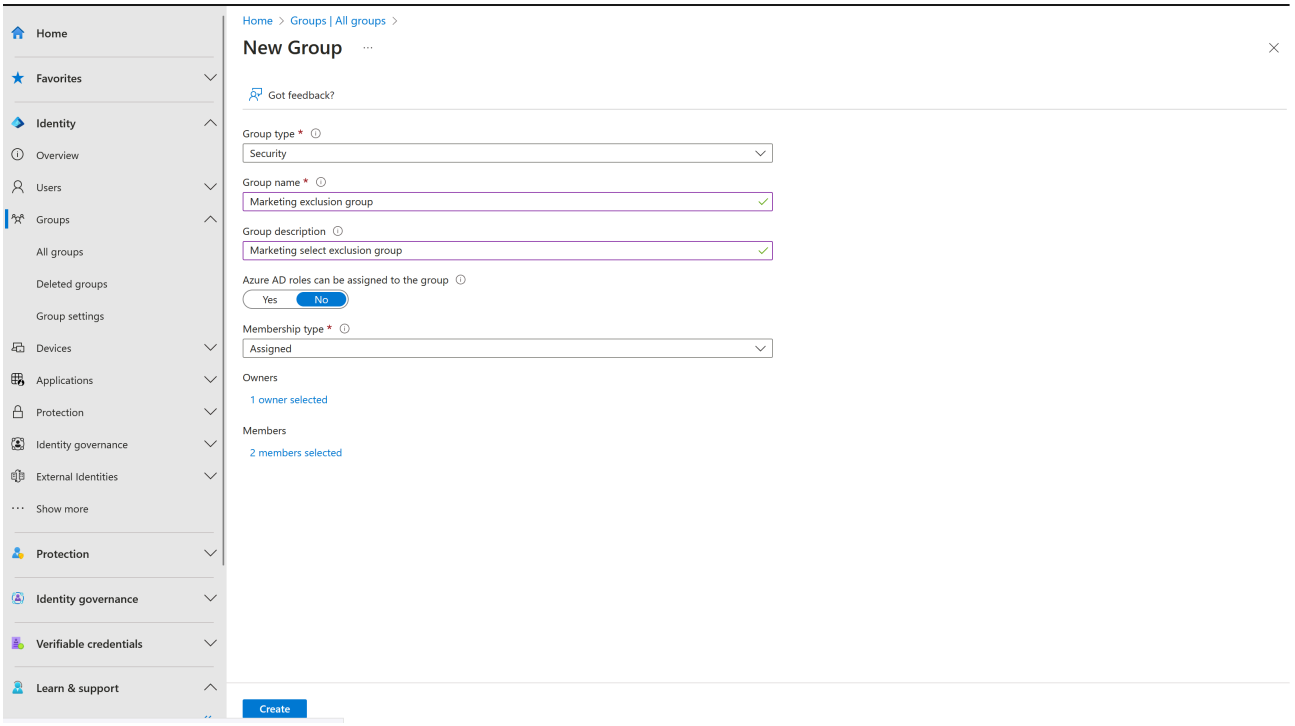
In Microsoft Entra ID, you can scope a Conditional Access policy to a set of users. You can also configure exclusions by selecting Microsoft Entra roles, individual users, or guests. You should keep in mind that when exclusions are configured, the policy intent can't be enforced on excluded users. If exclusions are configured using a list of users or using legacy on-premises security groups, you have limited visibility into the exclusions. As a result:

- Users might not know that they're excluded.
- Users can join the security group to bypass the policy.
- Excluded users could have qualified for the exclusion before but no longer qualify for it.

Frequently, when you first configure an exclusion, there's a shortlist of users who bypass the policy. Over time, more users get added to the exclusion, and the list grows. At some point, you need to review the list and confirm that each of these users is still eligible for exclusion. Managing the exclusion list, from a technical point of view, can be relatively easy, but who makes the business decisions, and how do you make sure it's all auditable? However, if you configure the exclusion using a Microsoft Entra group, you can use access reviews as a compensating control, to drive visibility, and reduce the number of excluded users.

Follow these steps to create a new Microsoft Entra group and a Conditional Access policy that doesn't apply to that group.

1. Sign in to the Microsoft Entra admin center as at least a User Administrator.
2. Browse to **Entra ID** > **Groups** > **All groups**.
3. Select **New group**.
4. In the **Group type** list, select **Security**. Specify a name and description.
5. Make sure to set the **Membership** type to **Assigned**.
6. Select the users that should be part of this exclusion group and then select **Create**.

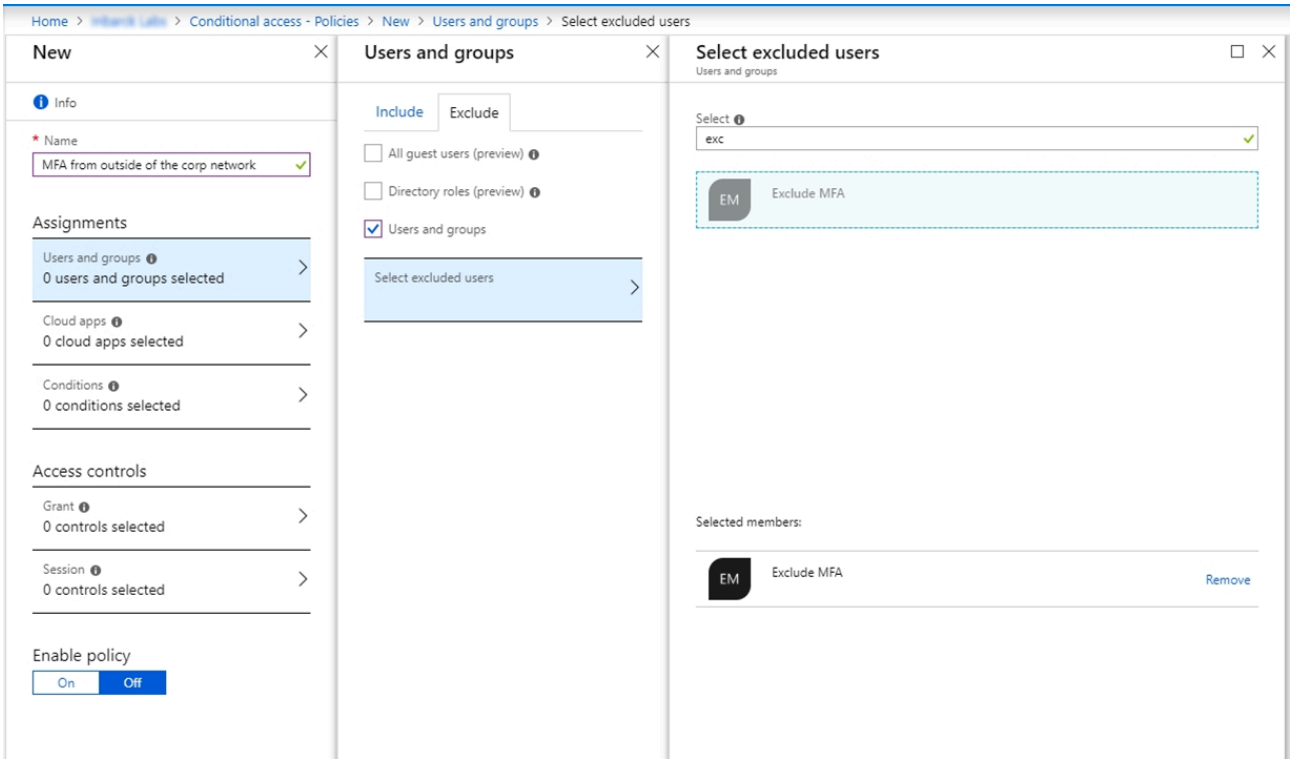


Now you can create a Conditional Access policy that uses this exclusion group.

1. Sign in to the Microsoft Entra admin center as at least a Conditional Access Administrator.
2. Browse to **Entra ID** > **Conditional Access**.
3. Select **Create new policy**.
4. Give your policy a name. We recommend that organizations create a meaningful standard for the names of their policies.
5. Under Assignments select **Users and groups**.
6. On the **Include** tab, select **All Users**.
7. Under **Exclude**, select **Users and groups** and choose the exclusion group you created.

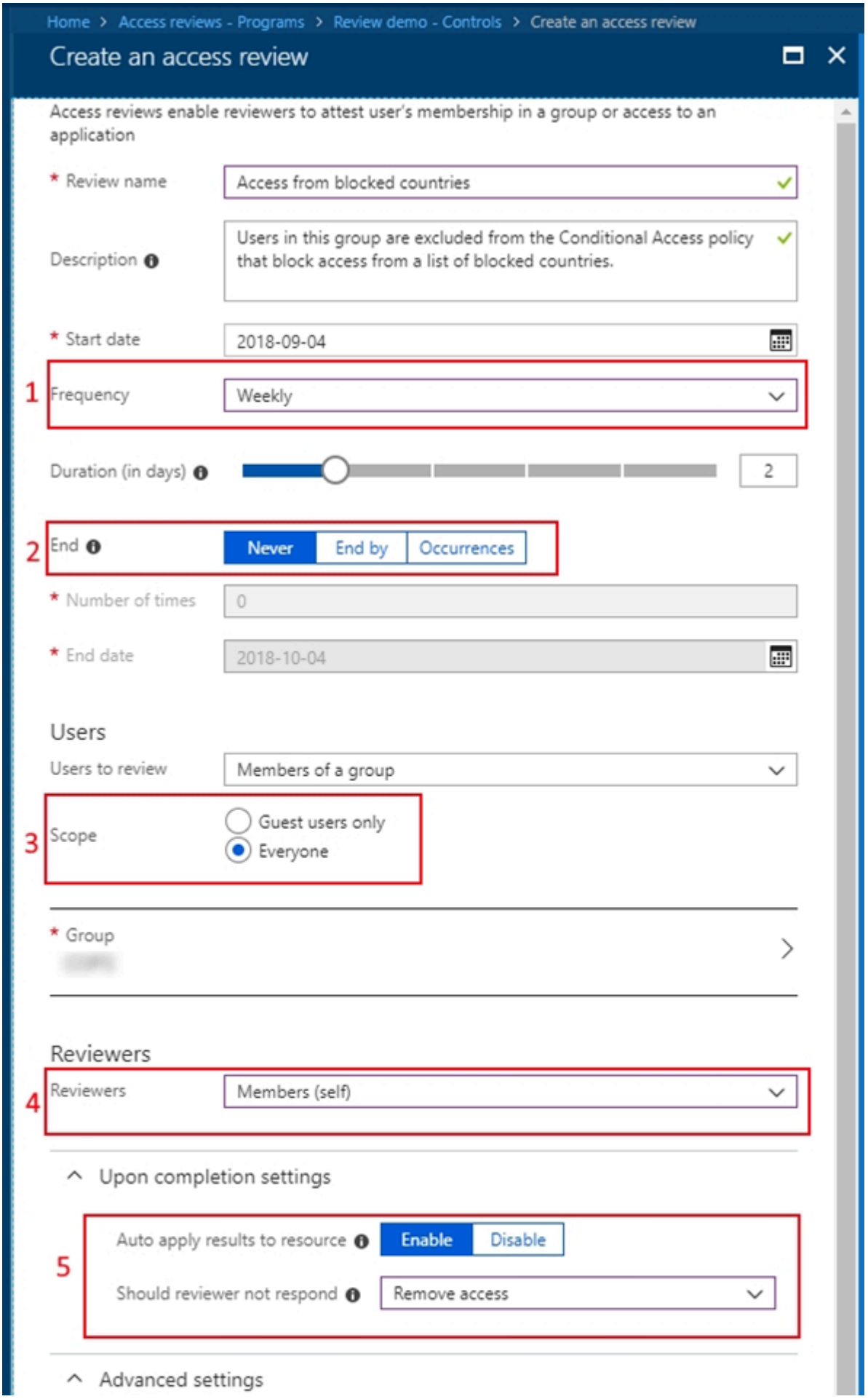
   Note

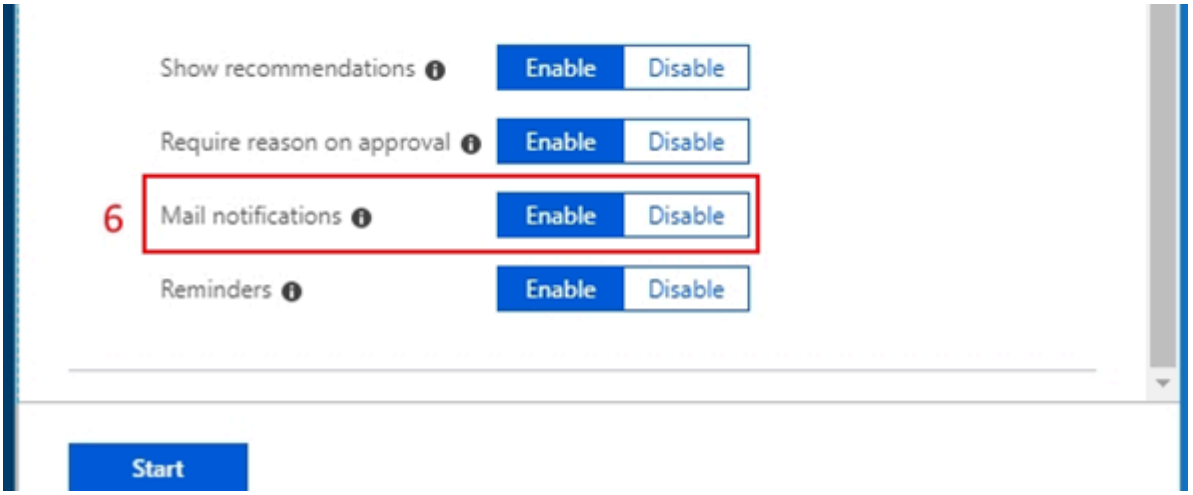
   As a best practice, it is recommended to exclude at least one administrator account from the policy when testing to make sure you are not locked out of your tenant.
8. Continue with setting up the Conditional Access policy based on your organizational requirements.



Let's cover two examples where you can use access reviews to manage exclusions in Conditional Access policies.

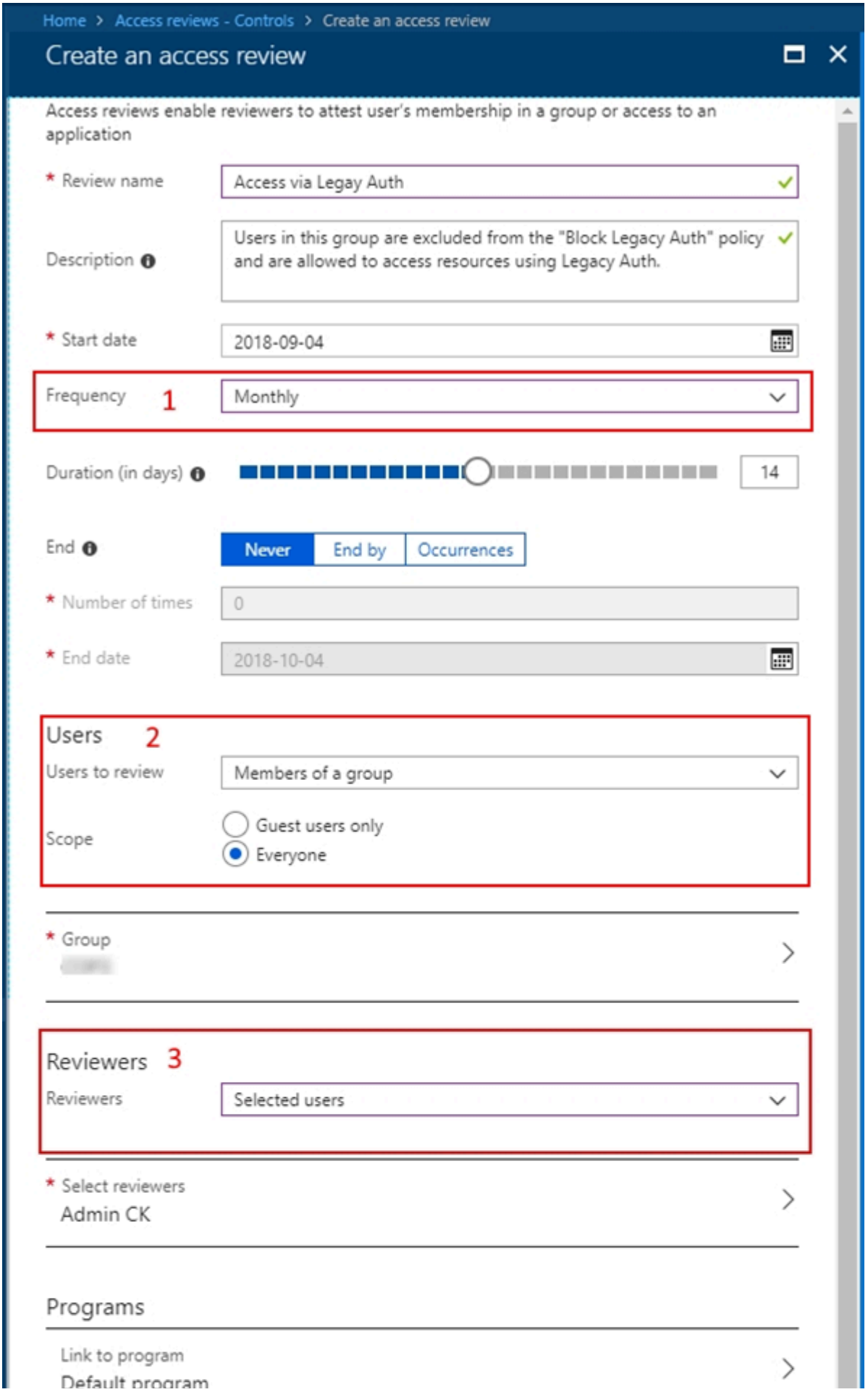
Let's say you have a Conditional Access policy that blocks access from certain countries/regions. It includes a group that is excluded from the policy. Here's a recommended access review where members of the group are reviewed.

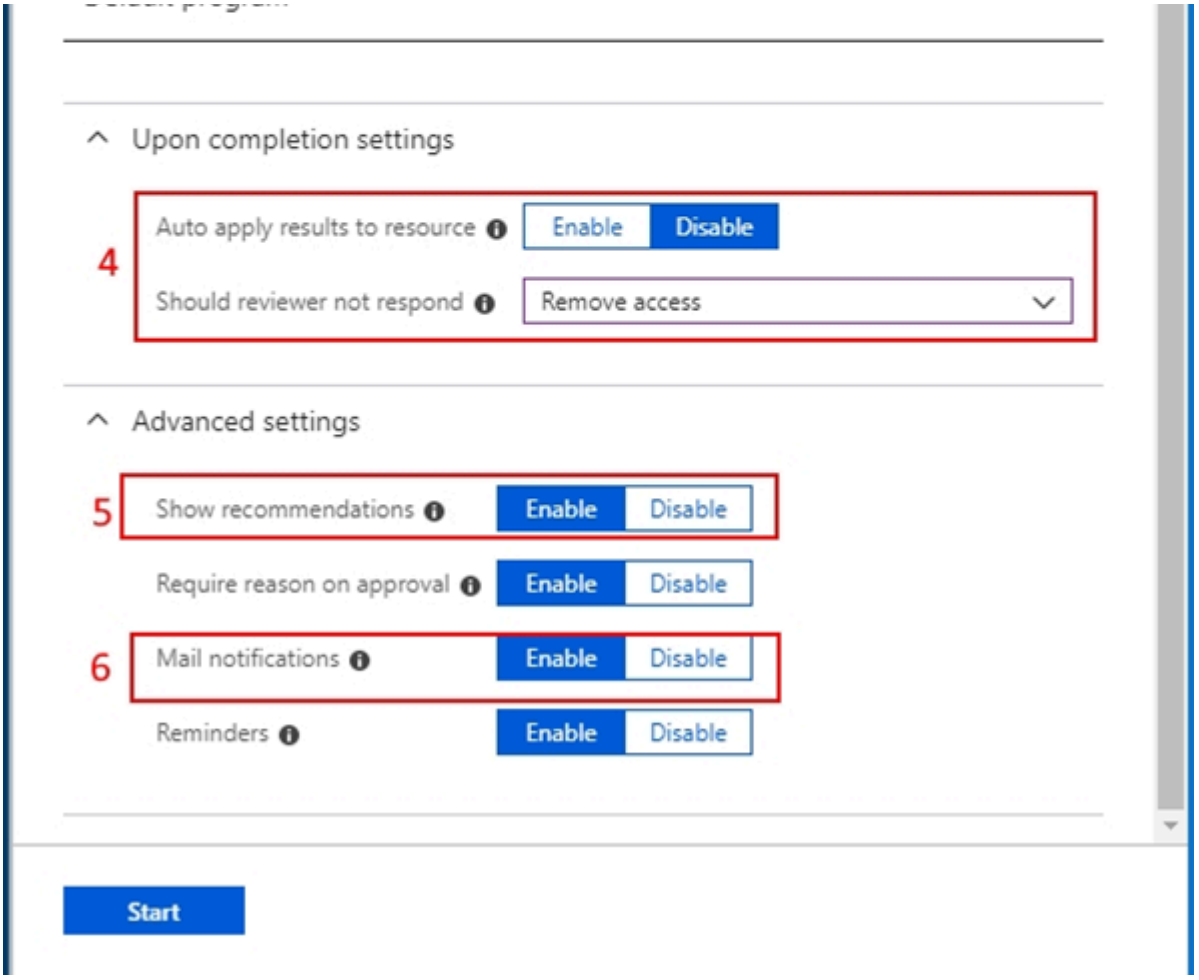

Home > Access reviews - Programs > Review demo - Controls > Create an access review
Create an access review
Access reviews enable reviewers to attest user's membership in a group or access to an application
* Review name
Access from blocked countries
Description
Users in this group are excluded from the Conditional Access policy that block access from a list of blocked countries.
* Start date
2018-09-04
1
Frequency
Weekly
Duration (in days)
2
2
End
Never
End by
Occurrences
* Number of times
0
* End date
2018-10-04
Users
Users to review
Members of a group
3
Scope
Guest users only
Everyone
* Group
Reviewers
4
Reviewers
Members (self)
Upon completion settings
5
Auto apply results to resource
Enable
Disable
Should reviewer not respond
Remove access
Advanced settings



1. The review happens every week.
2. The review never ends in order to make sure you're keeping this exclusion group most up to date.
3. All members of this group are in scope for the review.
4. Each user needs to self-attest that they still need access from these blocked countries/regions, therefore they still need to be a member of the group.
5. If the user doesn't respond to the review request, they're automatically removed from the group, and no longer has access to the tenant while traveling to these countries/regions.
6. Enable email notifications to let users know about the start and completion of the access review.

Let's say you have a Conditional Access policy that blocks access for users using legacy authentication and older client versions and it includes a group that is excluded from the policy. Here's a recommended access review where members of the group are reviewed.

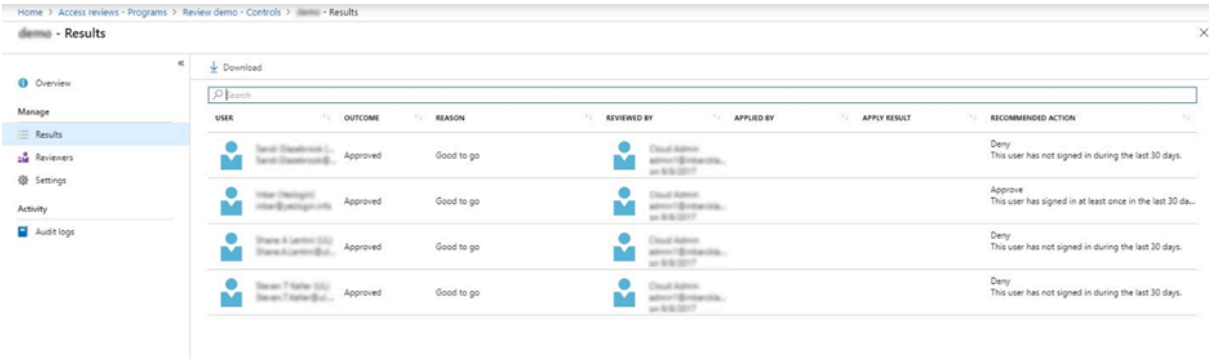

Home > Access reviews - Controls > Create an access review
Create an access review
Access reviews enable reviewers to attest user's membership in a group or access to an application
* Review name
Access via Legay Auth
Description
Users in this group are excluded from the "Block Legacy Auth" policy and are allowed to access resources using Legacy Auth.
* Start date
2018-09-04
Frequency
1
Monthly
Duration (in days)
14
End
Never
End by
Occurrences
* Number of times
0
* End date
2018-10-04
Users
2
Users to review
Members of a group
Scope
Guest users only
Everyone
* Group
Reviewers
3
Reviewers
Selected users
* Select reviewers
Admin CK
Programs
Link to program
Default program



1. This review would need to be a recurring review.
2. Everyone in the group would need to be reviewed.
3. It could be configured to list the business unit owners as the selected reviewers.
4. Auto-apply the results and remove users that aren't approved to continue using legacy authentication methods.
5. It might be beneficial to enable recommendations so reviewers of large groups can easily make their decisions.
6. Enable mail notifications so users are notified about the start and completion of the access review.

Now that you have everything in place, group, Conditional Access policy, and access reviews, it's time to monitor and track the results of these reviews.

1. Sign in to the Microsoft Entra admin center as at least an Identity Governance Administrator.
2. Browse to **ID Governance** > **Access reviews**.
3. Select the Access review you're using with the group you created an exclusion policy for.
4. Select **Results** to see who was approved to stay on the list and who was removed.



5. Select **Audit logs** to see the actions that were taken during this review.

As an IT administrator, you know that managing exclusion groups to your policies is sometimes inevitable. However, maintaining these groups, reviewing them regularly by the business owner or the users themselves, and auditing these changes can be made easier with access reviews.

- Create an access review of groups or applications
- What is Conditional Access in Microsoft Entra ID?

Source: https://docs.microsoft.com/en-us/azure/active-directory/governance/conditional-access-exclusion