Experiences with Multi Admin Approval

Multi Admin Approval is a feature in Intune, that require a second administrative account to approve a change before the change is applied.

With Multi Admin Approval (MAA), you configure access policies that protect specific configurations, like Apps or Scripts for devices. Access policies specify what is protected and which group of accounts are permitted to approve changes to those resources.

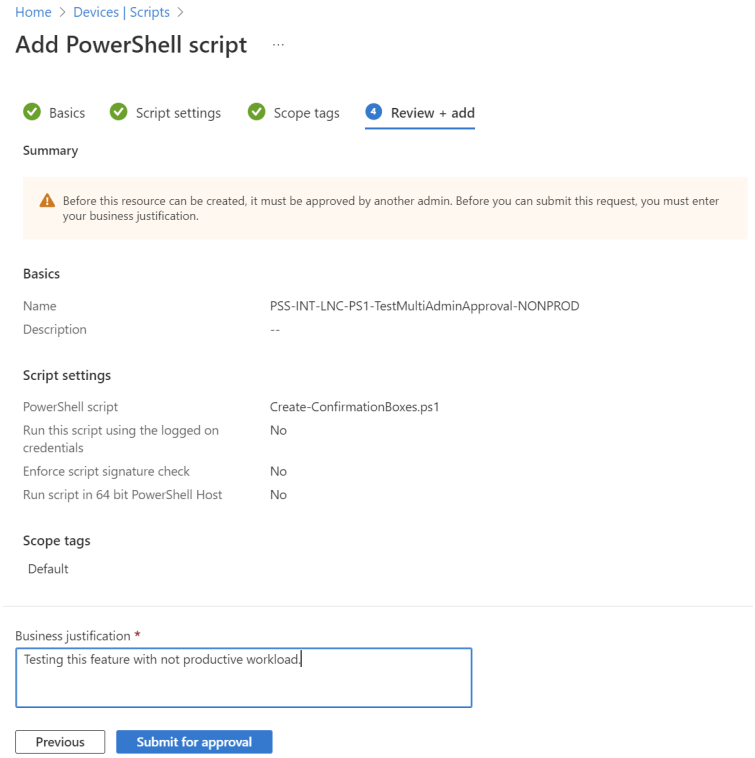
When any account in the Tenant is used to make a change to a resource that’s protected by an access policy, Intune won't apply the change until a different account explicitly approves it. Only administrators who are members of an approval group that’s assigned a protected resource in an access protection policy can approve changes. Approvers can also reject change requests.

Field report

- This feature is currently only applicable for Intune apps and Windows / MacOs scripts.
- To create or approve an approval request the account needs the role Intune Administrator even when in the account is in the approver group.
- The appropriately protected Intune resources (apps, scripts) cannot be restricted individually but are tenant wide protected for everyone via Multi Admin Approval.
- At the time of writing every request with scripts is only valid for one hour and then the status changes to expired. This does not apply to the Intune applications.
- Following entity actions need a separate approval request, whenever one of the actions is performed:.
  - Edit
  - Create
  - Modify
  - Delete
  - Assign

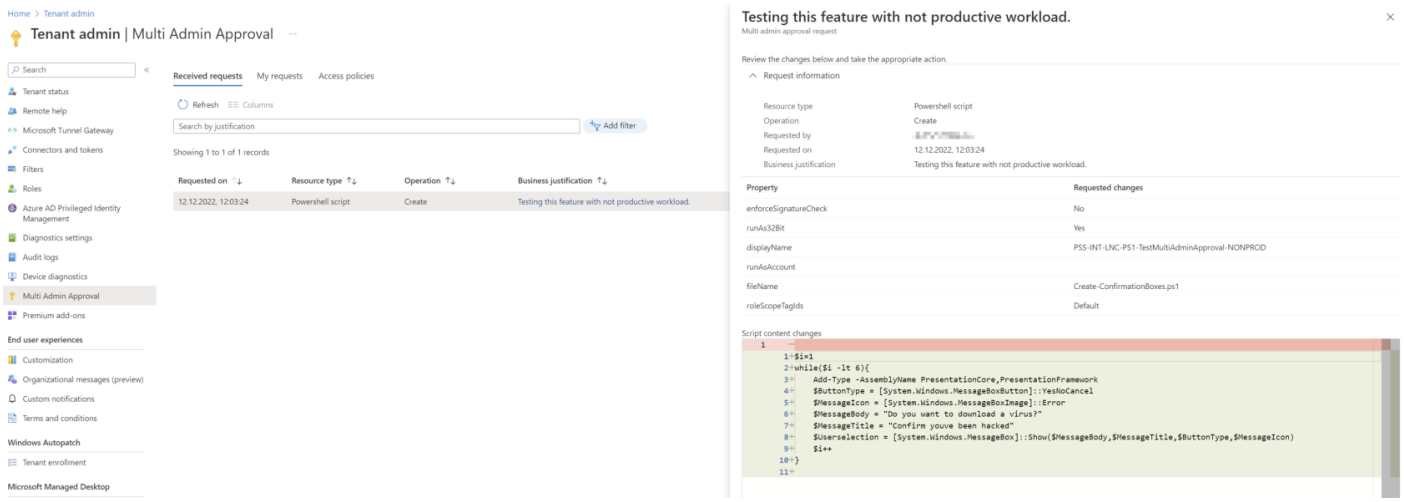
Steps of approval requests

After doing a described action (create, modify, delete, etc.) on an Intune resource which is protected by an access policy, will create an approval request in the Intune Admin Center. To submit the change you can use the normal Intune Admin Center.



Needs approval

After that submission a new approval request is created in the Intune Admin Center which needs to be approved or rejected from an other administrator account.



This approval is then moved to approved or rejected status according to the selection made.

Rejected

Rejected means that no further actions have to be made. The entity is archived and the status is set to rejected.

Approved

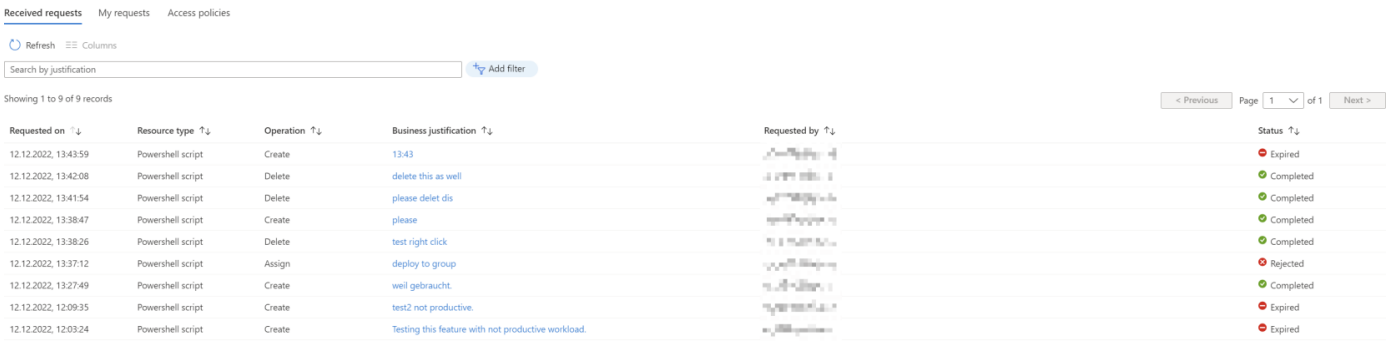
When approved by a different administrator your entity is then forwarded back to you so you can deploy the change at a time when it suits the creating person. The apps are implemented directly, without this following steps. This was tested with the scripts.

When "Complete request" is pressed by the owner of the approval request, the deployment of the change starts and gets implemented accordingly. The request then changes to the state of "Completed".

Completed

Completed are all requests which where approved by a different administrator and deployed by the owner. These changes were effectively made to the environment.

The Multi Administrator Approval is also very practical to trace changes.

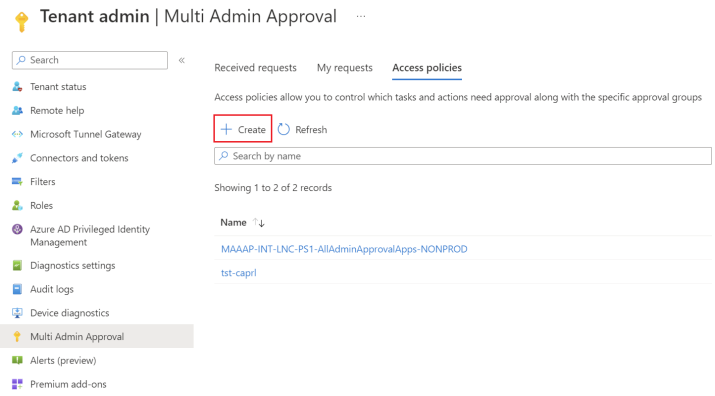


Expired

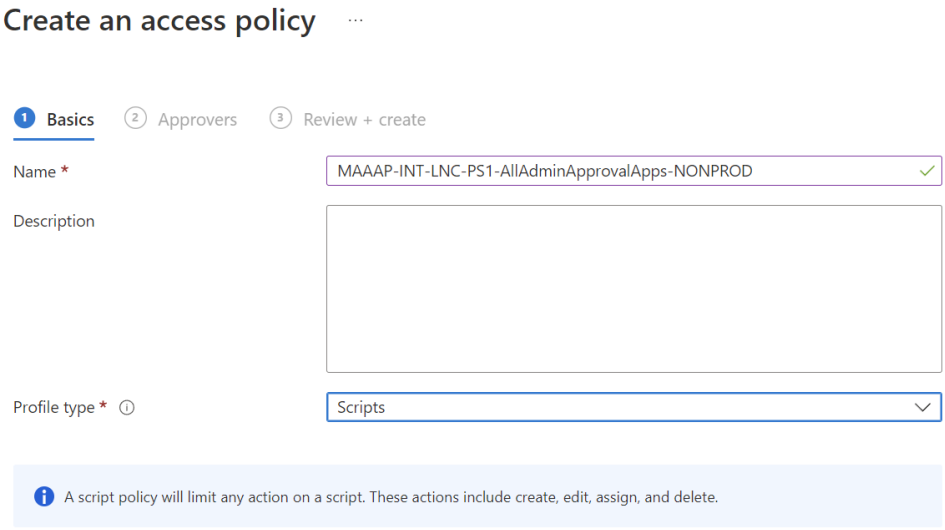
All requests which are not applied in one hour will get the status "Expired".

Create access policy

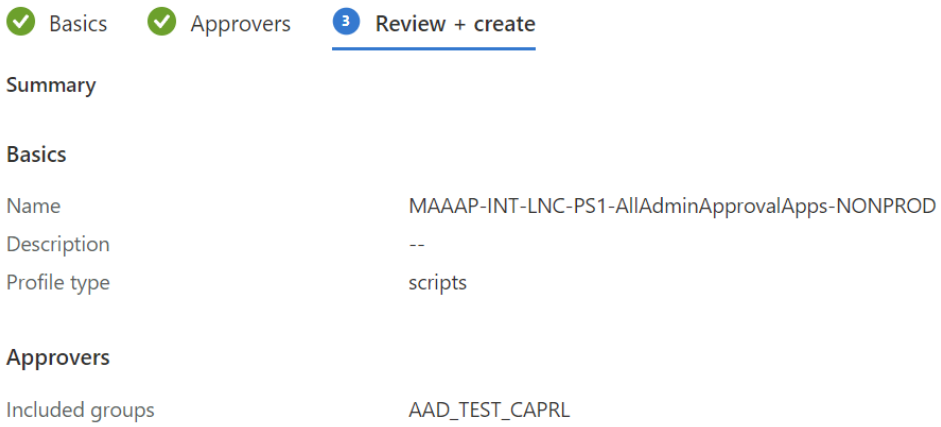
To create an access policy, you can change to "Multi Admin Approval" under "Tenant administration". There under "Access policies" you can create a new policy.



First you have to name the policy and choose the Profile type. Currently there are only two options; Scripts and Apps to select.



In addition, the approver group must be selected there. This group must contain the accounts which are authorized to approve or reject approval requests. These accounts must have to activate the "Intune Administrator" role.



Revision #8
Created 9 December 2022 14:58:10 by Luca Noah Caprez
Updated 13 December 2022 09:50:32 by Luca Noah Caprez