Approve or deny requests for Microsoft Entra roles in PIM - Microsoft Entra ID Governance

By kenwith

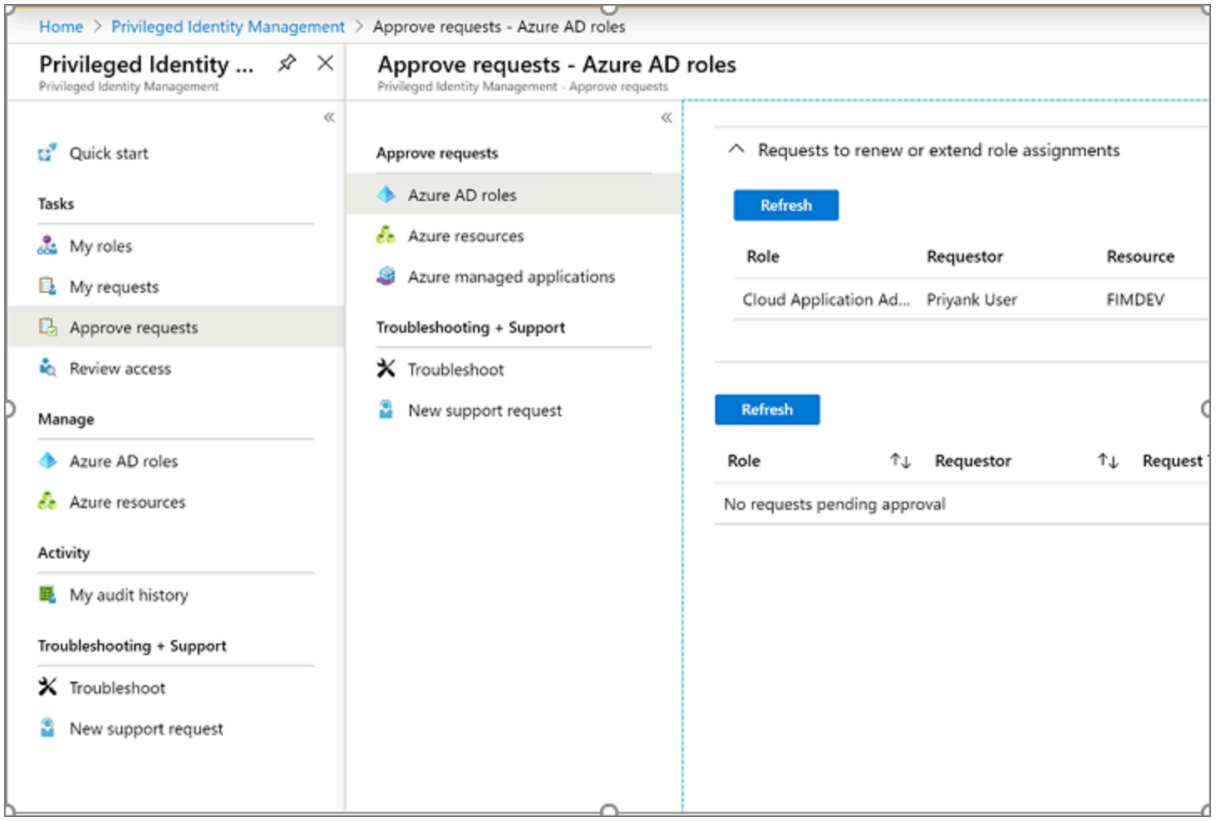
Archived: 2026-04-06 00:16:45 UTC

Approve or deny requests for Microsoft Entra roles in Privileged Identity Management

Privileged Identity Management (PIM) in Microsoft Entra ID allows you to configure roles to require approval for activation, and choose one or multiple users or groups as delegated approvers. Delegated approvers have 24 hours to approve requests. If a request isn't approved within 24 hours, then the eligible user must re-submit a new request. The 24-hour approval time window isn't configurable.

As a delegated approver, you receive an email notification when a Microsoft Entra role request is pending your approval. You can view these pending requests in Privileged Identity Management.

1. Sign in to the Microsoft Entra admin center.
2. Browse to **ID Governance** > **Privileged Identity Management** > **Approve requests**.



In the **Requests for role activations** section, you can see a list of requests pending your approval.

```
GET https://graph.microsoft.com/v1.0/roleManagement/directory/roleAssignmentScheduleRequests/filterByCurrentUs
```


```
{
   "@odata.context": "https://graph.microsoft.com/v1.0/$metadata#Collection(unifiedRoleAssignmentScheduleReques
   "value": [
       {
           "@odata.type": "#microsoft.graph.unifiedRoleAssignmentScheduleRequest",
           "id": "00aa00aa-bb11-cc22-dd33-44ee44ee44ee",
           "status": "PendingApproval",
           "createdDateTime": "2021-07-15T19:57:17.76Z",
           "completedDateTime": "2021-07-15T19:57:17.537Z",
           "approvalId": "00aa00aa-bb11-cc22-dd33-44ee44ee44ee",
           "customData": null,
           "action": "SelfActivate",
           "principalId": "aaaaaaaa-bbbb-cccc-1111-222222222222",
           "roleDefinitionId": "88d8e3e3-8f55-4a1e-953a-9b9898b8876b",
           "directoryScopeId": "/",
           "appScopeId": null,
           "isValidationOnly": false,
           "targetScheduleId": "00aa00aa-bb11-cc22-dd33-44ee44ee44ee",
           "justification": "test",
           "createdBy": {
               "application": null,
               "device": null,
               "user": {
                   "displayName": null,
                   "id": "d96ea738-3b95-4ae7-9e19-78a083066d5b"
               }
           },
           "scheduleInfo": {
               "startDateTime": null,
               "recurrence": null,
               "expiration": {
                   "type": "afterDuration",
                   "endDateTime": null,
                   "duration": "PT5H30M"
               }
           },
           "ticketInfo": {
               "ticketNumber": null,
               "ticketSystem": null
           }
       }
   ]
}
```

Note

Approvers aren't able to approve their own role activation requests. Additionally, service principals aren't allowed to approve requests.

1. Find and select the request that you want to approve. An approve or deny page appears.
2. In the **Justification** box, enter the business justification.
3. Select **Submit**. At this point, the system sends an Azure notification of your approval.

Note

Approval for **extend and renew** requests is currently not supported by the Microsoft Graph API.

For a specific activation request, this command gets all the approval steps that need approval. Multi-step approvals aren't currently supported.

```
GET https://graph.microsoft.com/beta/roleManagement/directory/roleAssignmentApprovals/<request-ID-GUID>
```

```
{
   "@odata.context": "https://graph.microsoft.com/beta/$metadata#roleManagement/directory/roleAssignmentApprova
   "id": "<request-ID-GUID>",
   "steps@odata.context": "https://graph.microsoft.com/beta/$metadata#roleManagement/directory/roleAssignmentAp
   "steps": [
       {
           "id": "<approval-step-ID-GUID>",
           "displayName": null,
           "reviewedDateTime": null,
           "reviewResult": "NotReviewed",
           "status": "InProgress",
           "assignedToMe": true,
           "justification": "",
           "reviewedBy": null
       }
   ]
}
```

```
 PATCH
https://graph.microsoft.com/beta/roleManagement/directory/roleAssignmentApprovals/<request-ID-GUID>/steps/<appro
{
    "reviewResult": "Approve", // or "Deny"
    "justification": "Trusted User"
}
```

Successful PATCH calls generate an empty response.

1. Find and select the request that you want to deny. An approve or deny page appears.
2. In the **Justification** box, enter the business justification.
3. Select **Deny**. A notification appears with your denial.

Here's some information about workflow notifications:

- Approvers are notified by email when a request for a role is pending their review. Email notifications include a direct link to the request, where the approver can approve or deny.
- Requests are resolved by the first approver who approves or denies.
- All approvers are notified when an approver responds to an approval request.
- Global Administrators and Privileged Role Administrators are notified when an approved user becomes active in their role.

Note

A Global Administrator or Privileged Role Admin who believes that an approved user shouldn't be active can remove the active role assignment in Privileged Identity Management. Although administrators aren't notified of pending requests unless they're an approver, they can view and cancel any pending requests for all users by viewing pending requests in Privileged Identity Management.

- Email notifications in Privileged Identity Management
- Approve or deny requests for Azure resource roles in Privileged Identity Management

---