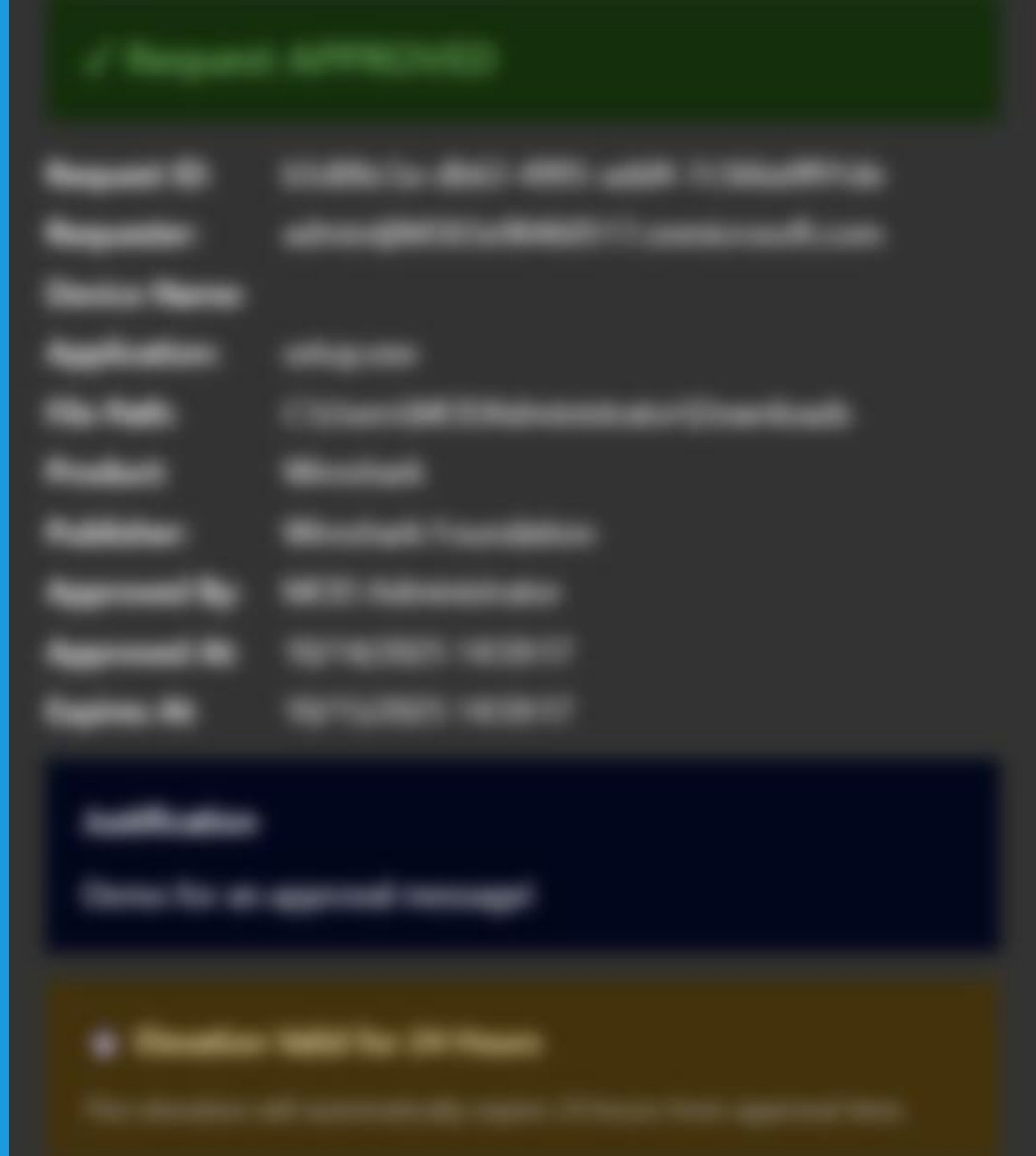
EPM Approval Workflow

Logic App with Teams Integration



Agenda

- Concept
- Components
- Why this approval flow?
- Features
- Deployment
- Demo
- Q&A

Concept

Logic App (Recurrence Trigger - every 5 minutes)

```
|
|---->  GET Microsoft Graph API
|       /deviceManagement/elevationRequests
|
|---> Filter requests with status = "supportApproved"
|
|---> For each approved request:
|   |---> Post Adaptive Card to Teams channel
|                       |---> Approve button
|                       |---> Deny button
|
|---> When button clicked:
    |---> PATCH elevation request via Graph API
```

Architecture

Logic App (Recurrence Trigger - every 5 minutes)

|

|—–> GET **Microsoft Graph API**

| /deviceManagement/elevationRequests **(EPM)**

|

|—> Filter requests with status = "supportApproved"

|

|—> For each approved request:

| |—> Post **Adaptive Card** to **Teams channel**

| |—> Approve button

| |—> Deny button

|

|—> When button clicked:

|—> PATCH elevation request via Graph API

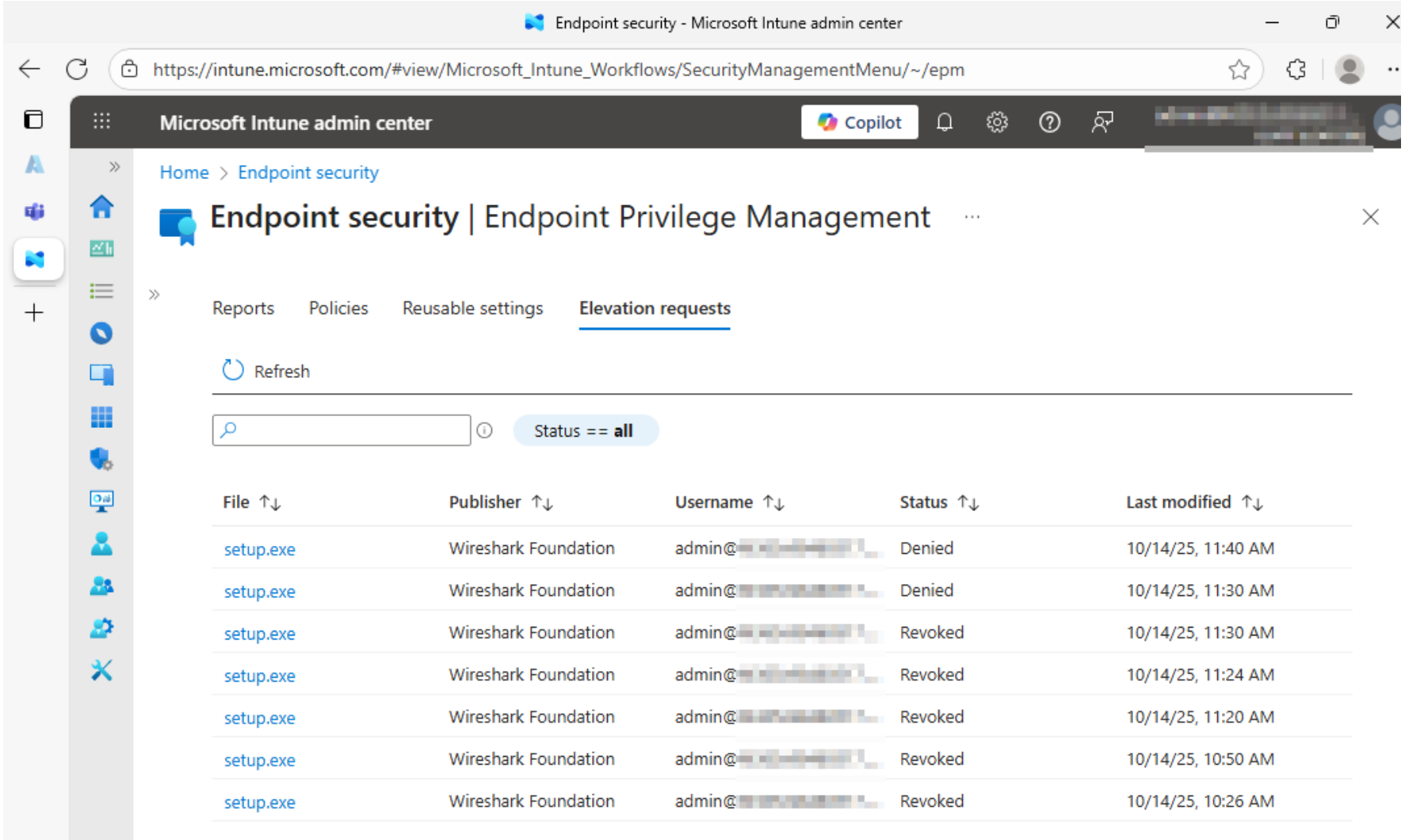
Components

- Logic App
- Microsoft Graph API
- Endpoint Privilege Management
- Adaptive Card
- Microsoft Teams

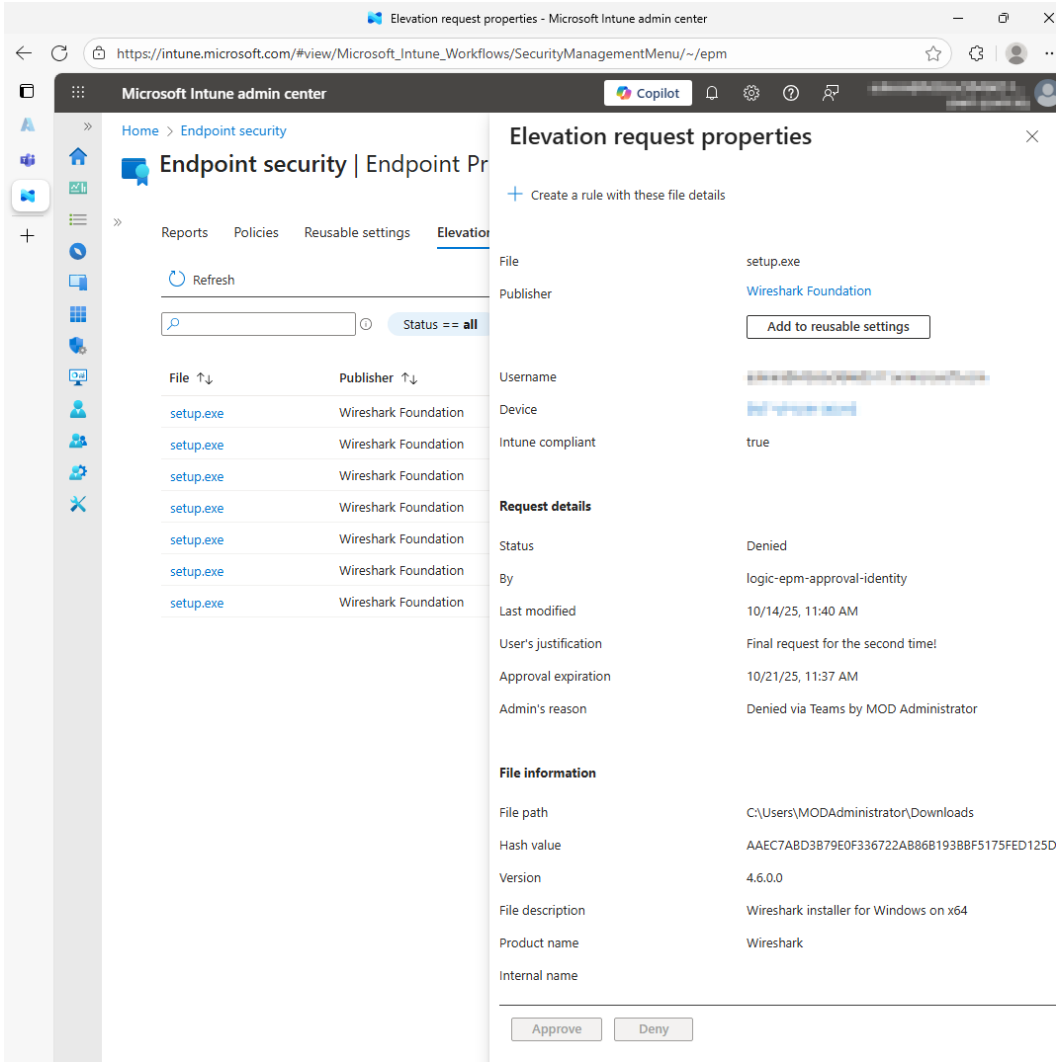
Hidden components

- Managed Identity
- Teams API Connection
- Log Analytics (Optional)

Why this approval workflow?



Why this approval workflow?



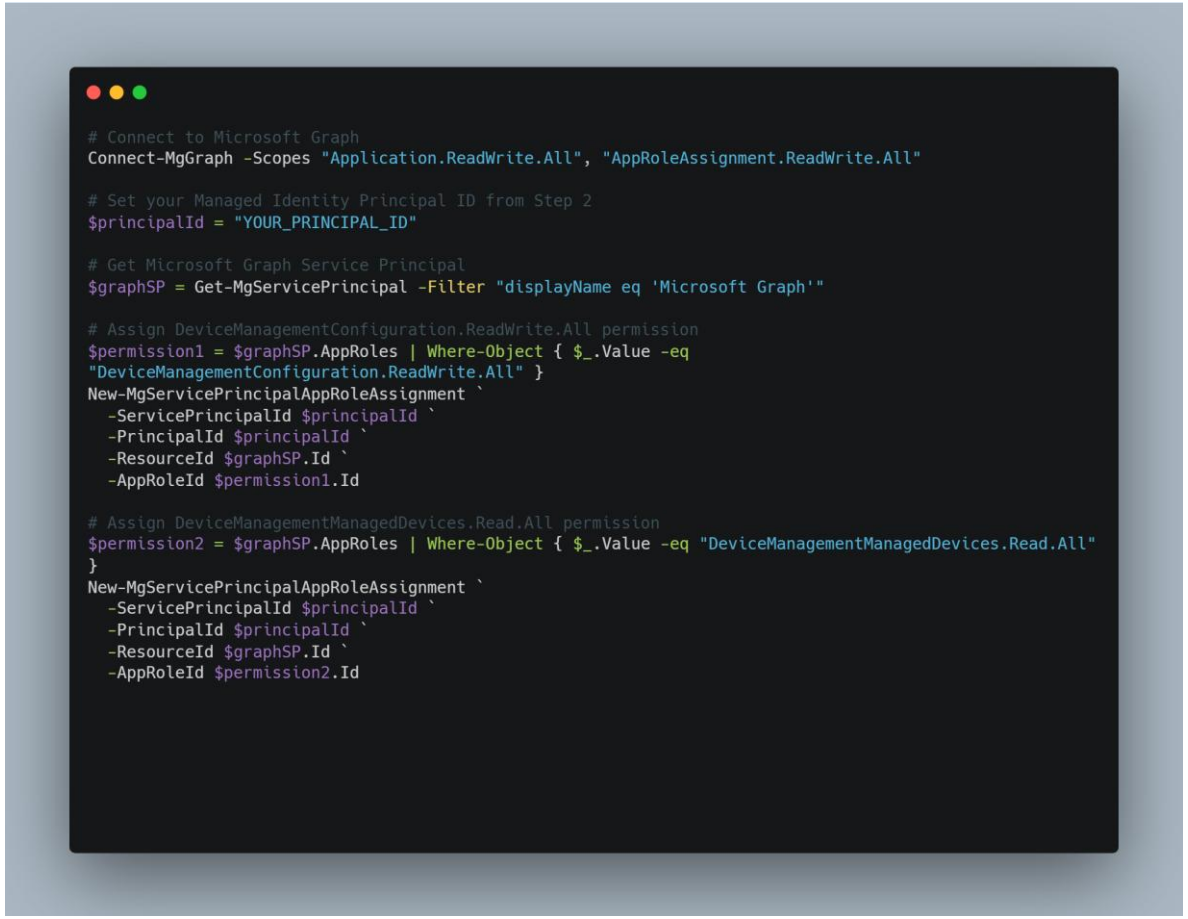
Features

- **(Automated) Polling**: Checks for new EPM elevation requests every 5 minutes
- **Teams Integration**: Posts Adaptive Cards with rich request details
- **One-Click Approval**: Approve or deny requests directly from Teams
- **Managed Identity**: Secure authentication to Microsoft Graph API
- **Least Privilege**: Uses minimal required Graph API permissions
- **Monitoring**: Integrated diagnostics with Log Analytics (Optional)
- **Secure by Design**: No secrets stored, outputs secured

Deployment

- Create a User-Assigned Managed Identity
- Assign Microsoft Graph API Permissions to the Managed Identity
- Create the Logic App
  - Assign the Managed Identity
  - Create a Teams API Connection
- [Optional] Configure Diagnostics

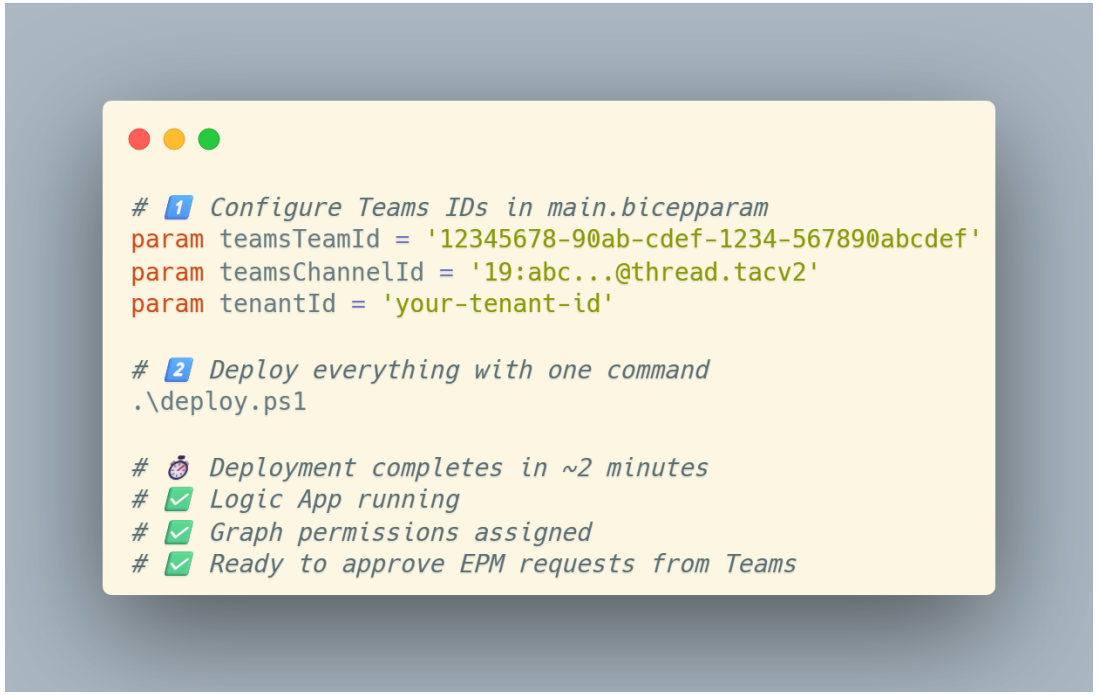
Assign Microsoft Graph API Permissions to the Managed Identity



```powershell
# Connect to Microsoft Graph
Connect-MgGraph -Scopes "Application.ReadWrite.All", "AppRoleAssignment.ReadWrite.All"

# Set your Managed Identity Principal ID from Step 2
$principalId = "YOUR_PRINCIPAL_ID"

# Get Microsoft Graph Service Principal
$graphSP = Get-MgServicePrincipal -Filter "displayName eq 'Microsoft Graph'"

# Assign DeviceManagementConfiguration.ReadWrite.All permission
$permission1 = $graphSP.AppRoles | Where-Object { $_.Value -eq
"DeviceManagementConfiguration.ReadWrite.All" }
New-MgServicePrincipalAppRoleAssignment `
  -ServicePrincipalId $principalId `
  -PrincipalId $principalId `
  -ResourceId $graphSP.Id `
  -AppRoleId $permission1.Id

# Assign DeviceManagementManagedDevices.Read.All permission
$permission2 = $graphSP.AppRoles | Where-Object { $_.Value -eq "DeviceManagementManagedDevices.Read.All"
}
New-MgServicePrincipalAppRoleAssignment `
  -ServicePrincipalId $principalId `
  -PrincipalId $principalId `
  -ResourceId $graphSP.Id `
  -AppRoleId $permission2.Id
```

Automating the deployment – Bicep!

Task	Manual	Bicep
Steps Required	10+ manual steps	1 command
Time to Deploy	20-30 minutes	2 minutes
Error Prone	High (copy/paste IDs)	Low (validated)
Repeatable	No	Yes



Demo

- Create an EPM elevation request in Intune that requires approval
  - Wait up to 5 minutes for the Logic App to run
  - Check your Teams channel for the Adaptive Card
    - Click **Approve** or **Deny** to test the workflow
    - Verify the request status updates in Intune

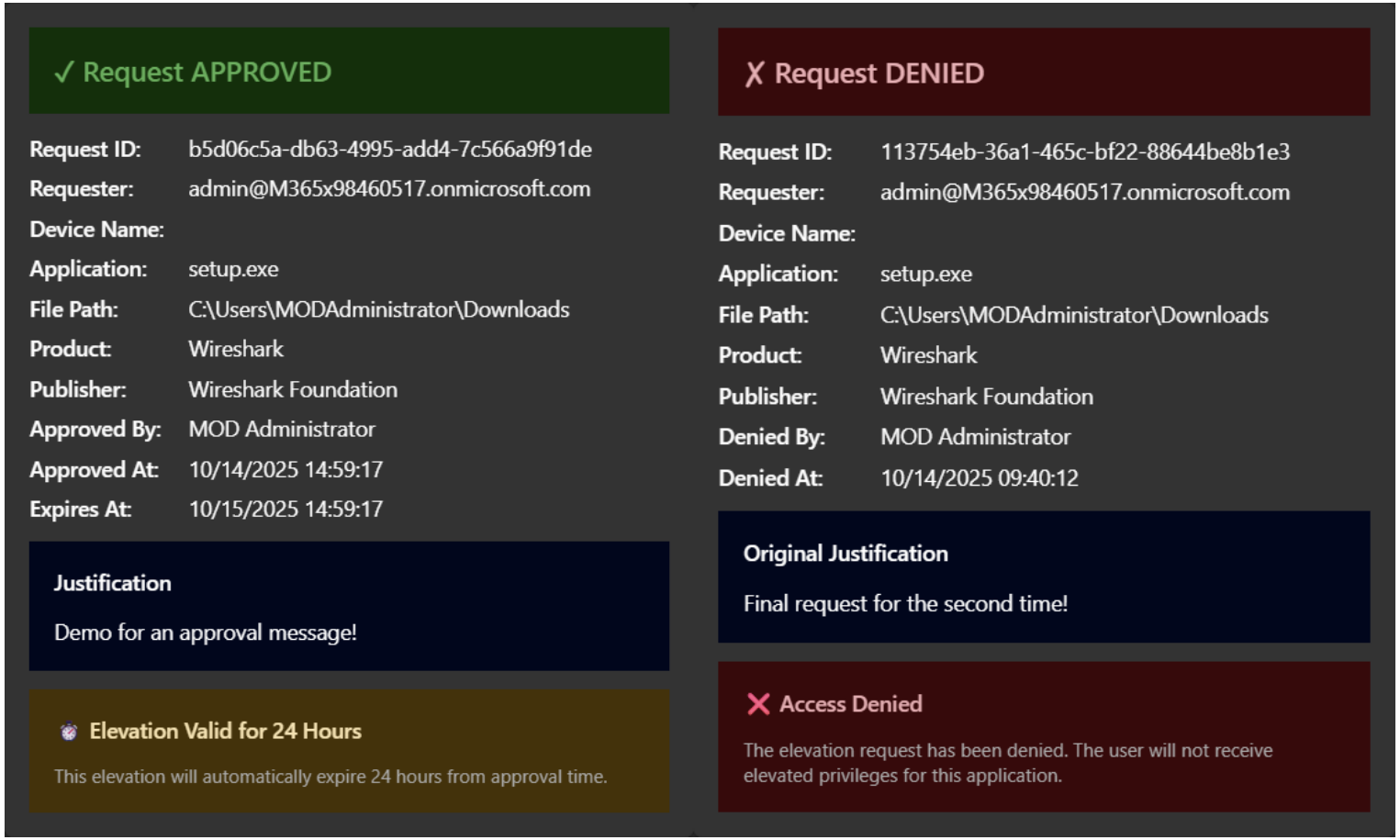
Cost Estimate

Resource	Pricing Tier	Usage Pattern	Monthly Cost
Logic App	Consumption (Pay-per-execution)	Runs every 5 minutes = ~8,640 executions/ month	**~$0.50**
Managed Identity	User-Assigned	Always included	**$0** (Free)
Teams API Connection	Standard	Included with M365	**$0** (Free)
Log Analytics (Optional)	Pay-per-GB ingestion	~500 MB/month logs	**~$2-5**

- Without Diagnostics: ~$0.50/month
- With Diagnostics: ~$2.50-$5.50/month

What's next?

- Send the notifications to a pre-defined group
  - Kinda like Alerts no?
- Convince PG to have me implement this awesome feature!
- Always open for Feature Requests!



Q&A

We would love to hear your feedback!

Session feedback available in home feed of the app after the session

Thank You!