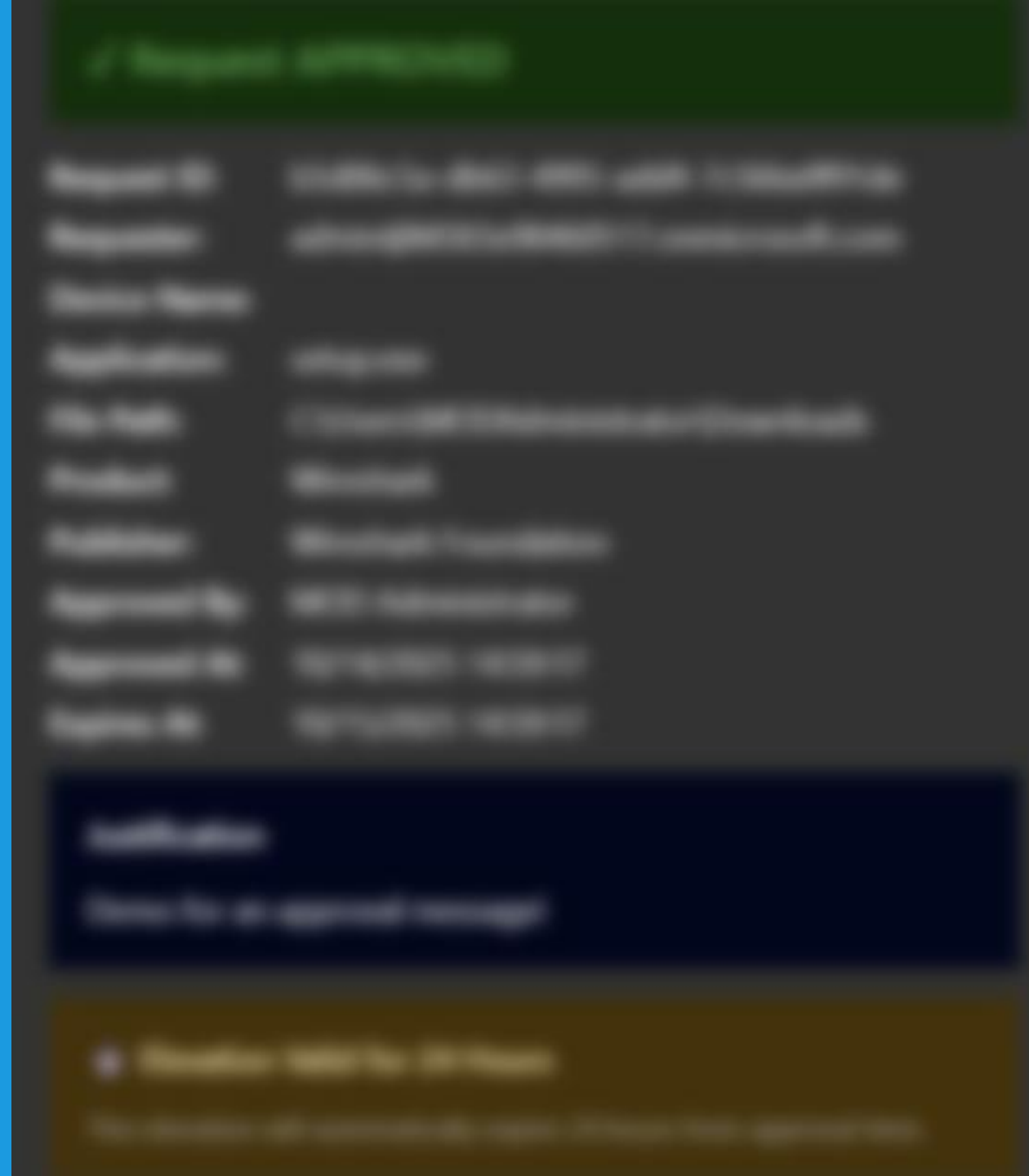




# EPM Approval Workflow

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?

The screenshot shows the Microsoft Intune admin center interface. The breadcrumb navigation is 'Home > Endpoint security'. The main heading is 'Endpoint security | Endpoint Privilege Management'. The 'Elevation requests' tab is selected, showing a list of requests. A search bar and a filter button 'Status == all' are visible. The table below lists the requests.

File ↑↓	Publisher ↑↓	Username ↑↓	Status ↑↓	Last modified ↑↓
<a href="#">setup.exe</a>	Wireshark Foundation	admin@...	Denied	10/14/25, 11:40 AM
<a href="#">setup.exe</a>	Wireshark Foundation	admin@...	Denied	10/14/25, 11:30 AM
<a href="#">setup.exe</a>	Wireshark Foundation	admin@...	Revoked	10/14/25, 11:30 AM
<a href="#">setup.exe</a>	Wireshark Foundation	admin@...	Revoked	10/14/25, 11:24 AM
<a href="#">setup.exe</a>	Wireshark Foundation	admin@...	Revoked	10/14/25, 11:20 AM
<a href="#">setup.exe</a>	Wireshark Foundation	admin@...	Revoked	10/14/25, 10:50 AM
<a href="#">setup.exe</a>	Wireshark Foundation	admin@...	Revoked	10/14/25, 10:26 AM

# Why this approval workflow?

The screenshot displays the Microsoft Intune admin center interface. The left sidebar shows the navigation menu with 'Endpoint security' selected. The main content area is titled 'Elevation request properties' and shows details for a request for 'setup.exe' from 'Wireshark Foundation'. The request status is 'Denied'.

**Elevation request properties**

+ Create a rule with these file details

File	setup.exe
Publisher	Wireshark Foundation
Username	[REDACTED]
Device	[REDACTED]
Intune compliant	true

**Request details**

Status	Denied
By	logic-epm-approval-identity
Last modified	10/14/25, 11:40 AM
User's justification	Final request for the second time!
Approval expiration	10/21/25, 11:37 AM
Admin's reason	Denied via Teams by MOD Administrator

**File information**

File path	C:\Users\MODAdministrator\Downloads
Hash value	AAEC7ABD3879E0F336722AB868193B8F5175FED125D
Version	4.6.0.0
File description	Wireshark installer for Windows on x64
Product name	Wireshark
Internal name	

Approve Deny



# 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

```
# 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
<b>Steps Required</b>	10+ manual steps	1 command
<b>Time to Deploy</b>	20-30 minutes	2 minutes
<b>Error Prone</b>	High (copy/paste IDs)	Low (validated)
<b>Repeatable</b>	No	Yes

```
# 1 Configure Teams IDs in main.bicepparam
param teamsTeamId = '12345678-90ab-cdef-1234-567890abcdef'
param teamsChannelId = '19:abc...@thread.tacv2'
param tenantId = 'your-tenant-id'

# 2 Deploy everything with one command
.\deploy.ps1

# 🕒 Deployment completes in ~2 minutes
# ✅ Logic App running
# ✅ Graph permissions assigned
# ✅ Ready to approve EPM requests from Teams
```

# 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
<b>Logic App</b>	Consumption (Pay-per-execution)	Runs every 5 minutes = ~8,640 executions/month	~\$0.50
<b>Managed Identity</b>	User-Assigned	Always included	\$0 (Free)
<b>Teams API Connection</b>	Standard	Included with M365	\$0 (Free)
<b>Log Analytics (Optional)</b>	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!

### ✓ Request APPROVED

**Request ID:** b5d06c5a-db63-4995-add4-7c566a9f91de  
**Requester:** admin@M365x98460517.onmicrosoft.com  
**Device Name:**  
**Application:** setup.exe  
**File Path:** C:\Users\MODAdministrator\Downloads  
**Product:** Wireshark  
**Publisher:** Wireshark Foundation  
**Approved By:** MOD Administrator  
**Approved At:** 10/14/2025 14:59:17  
**Expires At:** 10/15/2025 14:59:17

#### Justification

Demo for an approval message!

#### Elevation Valid for 24 Hours

This elevation will automatically expire 24 hours from approval time.

### ✗ Request DENIED

**Request ID:** 113754eb-36a1-465c-bf22-88644be8b1e3  
**Requester:** admin@M365x98460517.onmicrosoft.com  
**Device Name:**  
**Application:** setup.exe  
**File Path:** C:\Users\MODAdministrator\Downloads  
**Product:** Wireshark  
**Publisher:** Wireshark Foundation  
**Denied By:** MOD Administrator  
**Denied At:** 10/14/2025 09:40:12

#### Original Justification

Final request for the second time!

#### ✗ Access Denied

The elevation request has been denied. The user will not receive elevated privileges for this application.

# Q&A

M C  $\square^2$



# We would love to hear your feedback!

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



# Thank You!

