# Privileged Identity Management Implementation

**Completed By:** Manita Crawley

**Completion Period:** December 2025

This project was performed in a security lab environment using a Microsoft 365 Developer subscription. All users, roles, and configurations were created for learning and demonstration purposes.

## Executive Summary

This report demonstrates a Privileged Identity Management implementation for BookShop Enterprises which is a fictional e-commerce book store I created for this lab environment. The project is focused on addressing standing privileged access, which is one of the more common security gaps in identity management. The solution involved implementing Just-in-Time access controls, role governance, and periodic access reviews.

During the project activities, 21 admin roles were updated from permanent to eligible. This means users activate roles only when needed with a time limit on access windows. High-impact roles require approval before activation and quarterly access reviews are now in place. The result is a significantly reduced attack surface since privileged access now only exists when absolutely necessary with audit trails for compliance purposes.

## Scenario

BookShop Enterprises is an e-commerce company with 25 employees from different departments, including Executive, Technology, Finance, Human Resources, Marketing, and Store Operations. When considering the usage of PIM in the environment, there were several security gaps discovered in identity and access management:

- Admin accounts had permanent access to privileged roles around the clock
- No audit trail for when admin actions happened or why
- Possibility for privilege creep
- No separation of duties on high-impact admin changes
- Compliance gaps for PCI DSS 7.2 and SOX Section 404 identified in gap analysis

## Objective

The goal was to build a PIM solution that would:

1. Remove permanent privileged access through Just-in-Time role activation
2. Enforce the principle of least privilege for all admin roles
3. Implement approval workflows for high-impact admin changes
4. Create audit trails for all privileged access activities
5. Establish periodic access reviews for ongoing governance
6. Address compliance requirements for PCI DSS and SOX

## Environment Details

**Tenant:** Microsoft 365 Developer (mjsecuritylab.com)

**Directory Service:** Microsoft Entra ID

**License:** Microsoft 365 E5 Developer

**Total Users:** 25 users, 6 departments

**Admin Roles:** 21 Entra ID roles configured

**Break-Glass Accounts:** 2 accounts (bg-admin01, bg-admin02)

## Implementation Process

### Step 1: Identify Organizational Structure and Job Titles

The first step included reviewing the existing user base to understand the organizational structure. This meant exporting user data from Microsoft Entra ID and categorizing employees by department and job function.

| Department | Job Titles | Count |
|---|---|---|
| Executive | CEO, CTO, CFO, CMO | 4 |
| Technology | IT Manager, IT Ops Manager, Sr. Security Engineer, Sr. Security Analyst, Jr. Security Analyst, GRC Engineer, Help Desk Analyst (x2), Web Developer | 9 |
| Finance | Financial Analyst, Sr. Accountant | 2 |
| Human Resources | Recruiter, HR Generalist | 2 |
| Marketing | Communications Leader, Marketing Analyst | 2 |

| | | |
|---|---|---|
| Store Team | Store Manager, Asst. Manager, Team Lead, Associates | 6 |

## Step 2: Identify Job Functions Requiring Admin Roles

Not every employee needs admin access. The principle of least privilege involves permitting only the access needed for an employee's job functions. After assessing the different job responsibilities, the following roles were identified as needing admin capabilities:

- **Technology Team:** IT operations, security configuration, user management, compliance, application management, and help desk support
- **Executive (Limited):** Read-only access for oversight (CTO), financial management (CFO)
- **Other Departments:** No administrative roles required - standard user access only

**Decision:** C-suite executives do not automatically receive admin roles based on title. The CEO and CMO were determined to not require any Entra ID admin roles since their job functions do not include technical administration. Access should be based on job function if adhering to the principle of least privilege.

## Step 3: Configure Roles for the Environment

After reviewing and assessing the different job titles, 21 Entra ID roles were selected for PIM implementation. Each role was evaluated based on its functions and risk level to determine the necessary activation settings.

### High-Impact Roles (Approval Required)

These roles can make changes that impact the tenant, thus requiring approval before activation:

| Role | Capabilities | Duration |
|---|---|---|
| Global Administrator | Full access to all admin features | 1 hour |
| Privileged Role Administrator | Manage PIM settings and role assignments | 1 hour |
| Privileged Authentication Admin | Reset MFA for any user including admins | 1 hour |
| Security Administrator | Manage security features, Defender, Conditional Access policies | 4 hours |
| Conditional Access Administrator | Create and manage access policies | 4 hours |

**Operational Roles (Self-Activation)**

These roles are used for daily operations and can be self-activated with justification:

| Role | Capabilities | Duration |
|---|---|---|
| User Administrator | Create/manage users, reset passwords | 8 hours |
| Groups Administrator | Manage groups and membership | 8 hours |
| Helpdesk Administrator | Reset passwords for non-admin users | 8 hours |
| Authentication Administrator | Manage MFA for non-admin users | 4 hours |
| Application Administrator | Manage app registrations and enterprise apps | 4 hours |
| Intune Administrator | Manage devices and compliance policies | 4 hours |
| Exchange Administrator | Manage mail flow and Exchange settings | 4 hours |
| Security Operator | Respond to security alerts, investigate | 8 hours |
| Compliance Administrator | Manage DLP, retention, sensitivity labels | 4 hours |
| Compliance Data Administrator | Content searches, eDiscovery cases | 4 hours |

**Read-Only Roles (Executive Oversight)**

| Role | Capabilities | Duration |
|---|---|---|
| Global Reader | Read-only access to all admin centers | 8 hours |
| Security Reader | Read-only security reports and alerts | 8 hours |
| Reports Reader | View usage and adoption reports | 8 hours |
| Billing Administrator | Manage subscriptions and payments | 4 hours |

## Step 4: Apply the Principle of Least Privilege to User Roles

Each user was assigned only the roles necessary for their specific job function. This required analyzing daily tasks, responsibilities, and access patterns for each position.

| User | Job Title | Assigned Roles (Rationale) |
|---|---|---|
| Chippy Munk | IT Manager | Global Admin, Privileged Role Admin, Privileged Auth Admin, License Admin - Primary administrator responsible for tenant management |
| Reg Gae | IT Ops Manager | User Admin, Groups Admin, Authentication Admin - User lifecycle management and group administration |
| Paul Lynn | Sr. Security Engineer | Security Admin, CA Admin, Attack Sim Admin, Intune Admin, Exchange Admin - Security configuration across all platforms |
| Hip Hoppen | Sr. Security Analyst | Security Operator - Incident response and alert investigation |
| Rhythm Blues | Jr. Security Analyst | Security Operator, Helpdesk Admin - Tier 1 security ops and password resets for compromised accounts |
| Straw Berry | GRC Engineer | Compliance Admin, Compliance Data Admin - DLP policies and compliance management |
| Dance Hall | Help Desk Analyst | Helpdesk Admin, Authentication Admin - Password resets and MFA support |
| Countree Muzeek | Help Desk Analyst | Helpdesk Admin, Authentication Admin - Password resets and MFA support |
| Bar Chata | Web Developer | Application Admin - Manage app registrations for web application |
| Nin Tendo | CTO | Global Reader, Security Reader, Reports Reader - Executive oversight without modification rights |
| Keys Board | CFO | Billing Admin - Financial management of M365 subscriptions |
| BG-Admin01/02 | Break-Glass | Global Admin (PERMANENT) - Emergency access accounts |

## Step 5: Determine Active vs. Eligible Assignments

One of the key decisions in PIM implementation is determining which assignments should be Active versus Eligible. Active assignments are permanent and always-on, while Eligible assignments require activation when needed. The goal is to minimize standing privileges without hindering operational capability.

| Assignment Type | Behavior | Use Case |
|---|---|---|
| Active (Permanent) | User has the role all the time, no activation needed | Only for break-glass emergency accounts |

|  |  |  |
|---|---|---|
| Eligible | User requests activation when they need it | All normal admin accounts |

**Assignment Decisions**

- **Active Assignments:** Only bg-admin01 and bg-admin02 have permanent Global Administrator role. These accounts are primarily for emergency situations where PIM, MFA, or approvers are unavailable.
- **Eligible Assignments:** All other admin roles are set as Eligible. Users must explicitly activate their role, provide justification, and the role automatically expires after the selected duration.

## Step 6: Establish Approval Workflows

For high-impact roles such as Security Administrator, approval workflows ensure separation of duties and create an additional point of control before approving privileged access. Approvers were selected based on role responsibility and separation of concerns.

**Approver Selection Criteria**

- The person approving shouldn't be the same person requesting (separation of duties)
- Approvers need enough information to determine whether the request makes sense
- Multiple approvers when possible so someone's always available
- Approvers don't need to hold the role themselves

**Final Approval Configuration**

| Role | Activation Type | Approver(s) |
|---|---|---|
| Global Administrator | Require Approval | R.Gae (IT Ops Manager) |
| Privileged Role Administrator | Require Approval | R.Gae (IT Ops Manager) |
| Privileged Authentication Admin | Require Approval | R.Gae (IT Ops Manager) |
| Security Administrator | Require Approval | R.Gae, Chippy (IT Manager) |
| Conditional Access Administrator | Require Approval | R.Gae, Chippy (IT Manager) |
| All Other Roles | Self-Activate | None (justification required) |

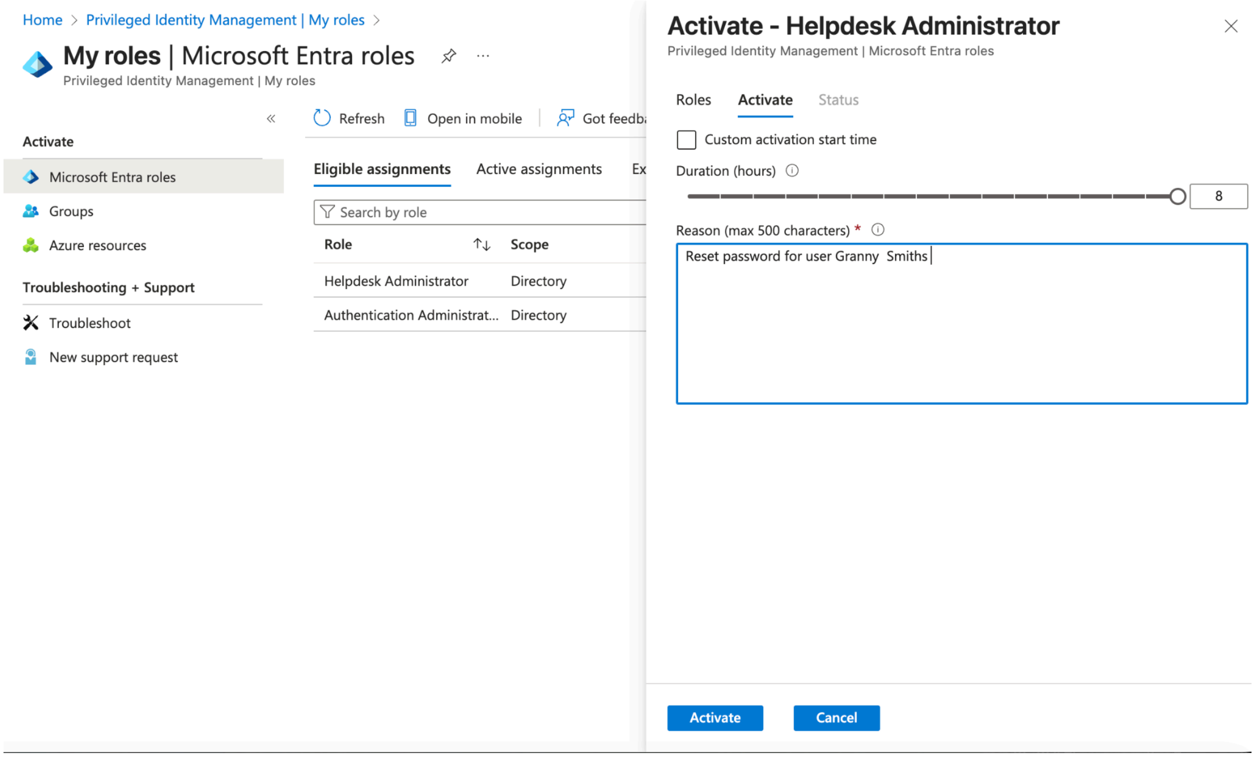
## Step 7: Testing and Validation

During testing, the PIM configurations were validated and ensured role boundaries were correctly enforced.

### Test 1: Self-Activation Workflow

**Objective:** Ensure eligible users can activate their roles when needed and that the justification requirement works.

- Logged in as Countree Muzeek (Help Desk Analyst)
- Navigated to PIM > My roles > Eligible assignments
- Requested Helpdesk Administrator activation
- Provided justification: "Need to reset password for an HR employee"
- Role activated right away since it's self-activation, no approval needed


Home > Privileged Identity Management | My roles >
My roles | Microsoft Entra roles
Privileged Identity Management | My roles
Activate
Microsoft Entra roles
Groups
Azure resources
Troubleshooting + Support
Troubleshoot
New support request
Refresh
Open in mobile
Got feedb
Eligible assignments
Active assignments
Ex
Search by role
Activate - Helpdesk Administrator
Privileged Identity Management | Microsoft Entra roles
Roles
Activate
Status
Activate
Cancel

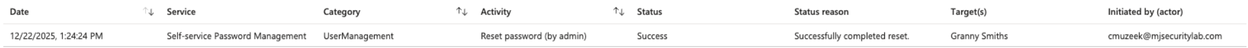
| Role | Scope |
|---|---|
| Helpdesk Administrator | Directory |
| Authentication Administrat... | Directory |

□ Custom activation start time

Duration (hours) 8

Reason (max 500 characters) *

Reset password for user Granny Smiths



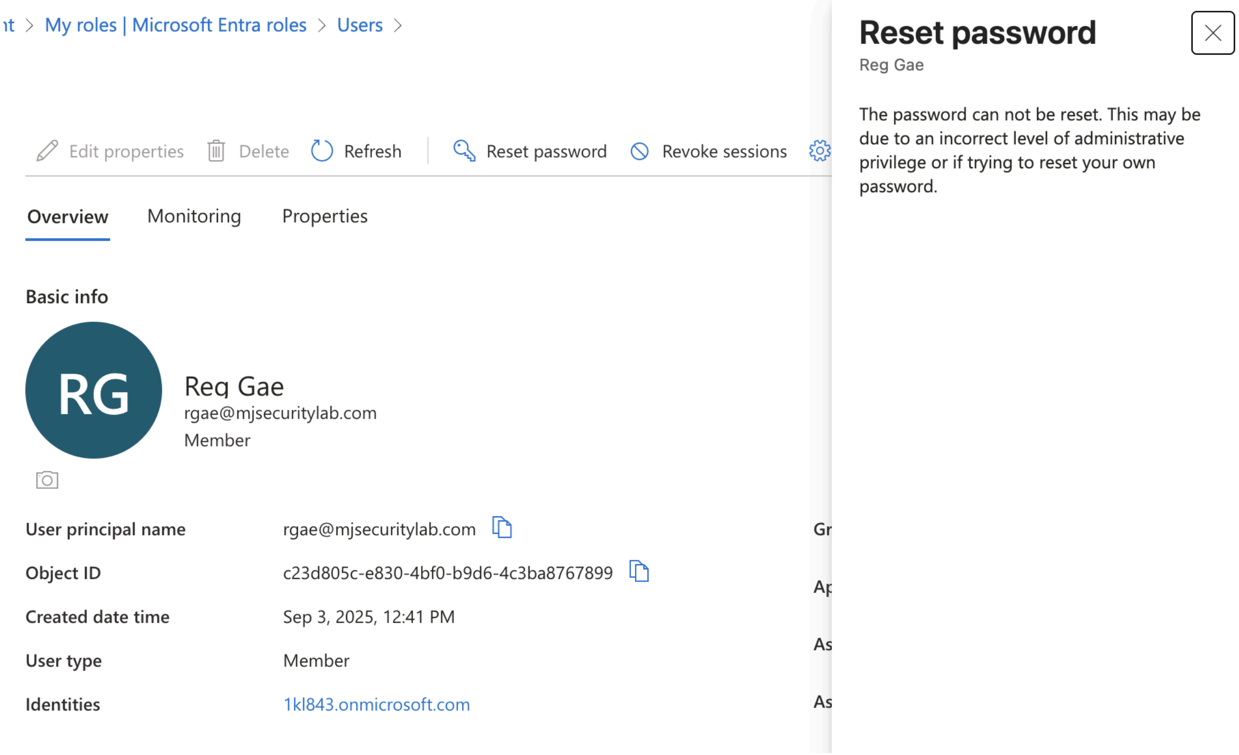
| Date | Service | Category | Activity | Status | Status reason | Target(s) | Initiated by (actor) |
|---|---|---|---|---|---|---|---|
| 12/22/2025, 1:24:24 PM | Self-service Password Management | UserManagement | Reset password (by admin) | Success | Successfully completed reset. | Granny Smiths | cmuzeek@mjsecuritylab.com |

**Result:** PASS - Role came up, audit trail got created

### Test 2: Role Boundary Enforcement

**Objective:** Confirm the role hierarchy prevents privilege escalation.

- With Helpdesk Admin active a password reset was attempted for Granny Smiths from HR.
- The password reset button was available, which confirms proper permissions
- The password reset was attempted for the IT Operations Manager, Reg Gae
- Received an error indicating that permissions were insufficient for this action



**Reset password**

Reg Gae

The password can not be reset. This may be due to an incorrect level of administrative privilege or if trying to reset your own password.

Reg Gae
rgae@mjsecuritylab.com
Member

| | |
|---|---|
| User principal name | rgae@mjsecuritylab.com |
| Object ID | c23d805c-e830-4bf0-b9d6-4c3ba8767899 |
| Created date time | Sep 3, 2025, 12:41 PM |
| User type | Member |
| Identities | 1kl843.onmicrosoft.com |

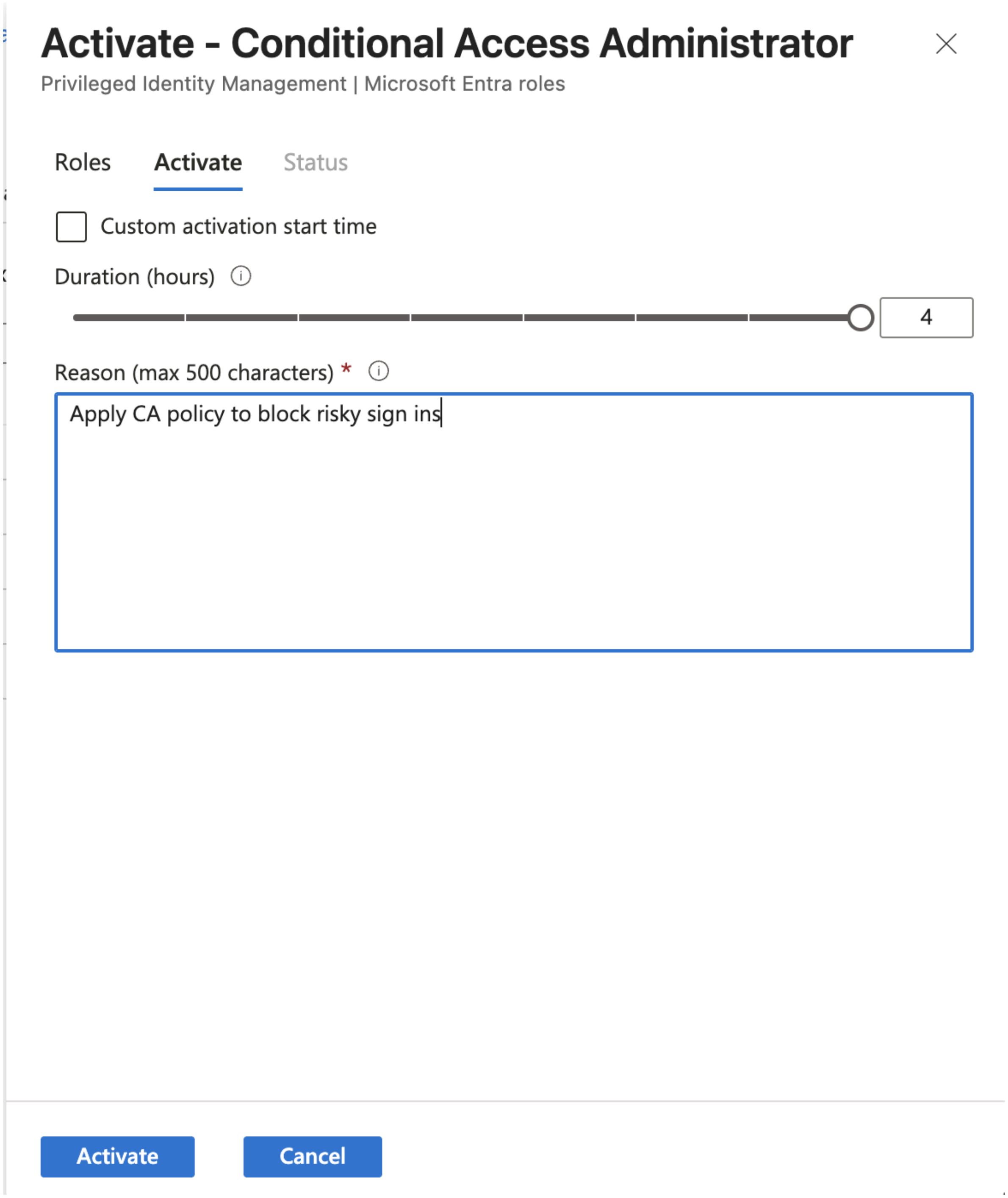
**Result:** PASS - Helpdesk Admin got blocked trying to reset an admin's password. Escalation prevented

### Test 3: Approval Workflow

**Objective:** Confirm that request-approval workflow runs as expected for roles with approvers.

- Signed in as Paul Lynn (Sr. Security Engineer)
- Requested activation for the Security Administrator role
- Provided justification for the request
- Request was created with status "Pending Approval"
- Signed in as Chippy Munk (a designated approver for this role)
- Navigated to PIM > Approve requests

- Reviewed and approved the request
- Paul Lynn's Security Administrator role was activated



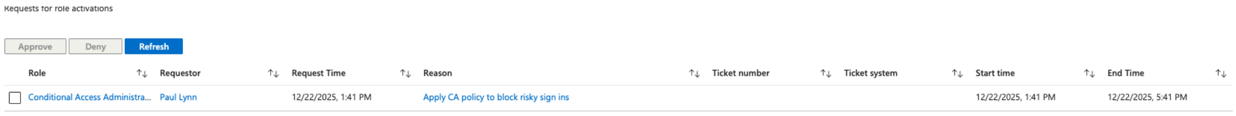
# Activate - Conditional Access Administrator

Privileged Identity Management | Microsoft Entra roles

□ Custom activation start time

Duration (hours): 4

Reason (max 500 characters) *: Apply CA policy to block risky sign ins



Requests for role activations

| Role | Requestor | Request Time | Reason | Ticket number | Ticket system | Start time | End Time |
|---|---|---|---|---|---|---|---|
| □ Conditional Access Administra... | Paul Lynn | 12/22/2025, 1:41 PM | Apply CA policy to block risky sign ins | | | 12/22/2025, 1:41 PM | 12/22/2025, 5:41 PM |

**Result:** PASS - Approval workflow ran as expected, notifications were sent, and audit trail the events

#### Test 4: Role Deactivation

**Objective:** Confirm users can deactivate their own roles.

Paul Lynn manually deactivated the Security Administrator role through PIM > My roles > Active assignments. The role was immediately revoked with an audit log entry created.

**Result:** PASS - Manual deactivation executed successfully

## Step 8: Configure and Execute Access Reviews

Access reviews provide periodic review of roles to verify users still require their assigned privileges. This is important to avoid privilege creep to prevent users from accumulating roles they no longer need over time.

#### Access Review Configuration

| Setting | Value |
|---|---|
| Review Name | Quarterly PIM Role Review - Q1 2025 |
| Scope | Helpdesk Administrator role (test) |
| Reviewers | Chippy Munk (IT Manager) |
| Recurrence | Quarterly |
| Duration | 14 days for reviewer response |
| Assignment Types | Eligible and Active |

#### Access Review Execution

The access review showed three users for evaluation: Rhythm Blues, Dance Hall, and Countree Muzeek. Each user was reviewed based on their current job function and whether continued access is still needed.

#### Review Decisions

| User | Decision | Justification |
|---|---|---|
| Rhythm Blues | Approved | Active Jr. Security Analyst - requires Helpdesk Admin for password resets on compromised accounts |
| Dance Hall | Approved | Active Help Desk Analyst - access required for daily support tasks |
| Countree Muzeek | Approved | Active Help Desk Analyst - access required for daily support tasks |

## Situational Exceptions

Two exceptions were made for this testing environment that would be handled differently in production:

**Exception 1: Chippy Munk Active Global Administrator**

The primary configuration account (Chippy Munk) maintains an Active Global Administrator assignment rather than Eligible. This was necessary because converting the account to Eligible while actively configuring PIM would require activating the role for every configuration change, which adds unnecessary complexity during implementation. In a production environment, this account would be converted to Eligible as a final step after all configurations are complete and tested.

**Exception 2: MFA Disabled for Role Activation**

MFA requirement for role activation was tested on one account and confirmed working correctly, but was not enforced across all accounts to reduce complexity in this testing environment. In a live environment, MFA would be required for all role activations as a baseline security control. A review of the audit records confirmed that MFA integration worked when enabled.

## Risk Assessment & Business Impact

### Security Gaps Addressed

| Gap ID | Issue | PIM Resolution | Risk Reduction |
|---|---|---|---|
| I2 | Static privilege assignment, 24/7 admin access | JIT activation with time limits | High |
| I4 | Accounts audited only when events occur | Scheduled quarterly access reviews | Medium |

| | | | |
|---|---|---|---|
| PCI 7.2 | Least privileges for job function | Role-based assignments with justification | High |
| SOX 404 | Internal controls over privileged access | Approval workflows and audit logs | High |

**Impact**

- **Attack Surface Reduction:** Standing access went from 24/7 to only when someone activates it. This now significantly reduces the potential exposure based on how often users will activate roles per week to perform their duties.
- **Audit Coverage:** All privileged role activations are now logged with justification, an approver, a timestamp, and duration
- **Compliance Posture:** Audit logs provide evidence of least privilege controls for PCI DSS 7.2 and SOX 404 audits

# Improvement Areas

While the implementation addressed core privileged access challenges, the following improvements would further strengthen the security posture:

### 1. Ensure Multiple Approvers for Each Role

Currently, some high-impact roles have only a single approver set. If that approver is unavailable due to vacation, illness, or account compromise, activation requests could be delayed or blocked. Each role requiring approval should have at least two designated approvers for coverage and business continuity. This also provides redundancy when an approver needs to recuse themselves due to conflict of interest.

### 2. Expand Access Reviews to All PIM-Enabled Roles

The initial access review was configured as a pilot for the Helpdesk Administrator role only. In a live implementation, access reviews would cover all 21 PIM-enabled roles. Different review frequencies may be appropriate based on role sensitivity. For example, quarterly reviews work well for high-impact roles like Global Admin, Security Admin, and Privileged Role Admin. Whereas, semi-annual reviews may be best for operational roles like User Admin, Groups Admin, and Application Admin.

### 3. Implement Time-of-Day Restrictions

Certain high-impact roles could benefit from time-of-day restrictions that limit activation to business hours only. Global Administrator activation at 3:00 AM on a Sunday is suspicious and more likely indicates compromised credentials than a legitimate admin needs. This would require additional configuration through Conditional Access policies integrated with PIM, to create an additional layer of defense against off-hours attacks. Emergency access is always available through break-glass accounts and should continue to bypass PIM controls.

# Conclusion

This Privileged Identity Management implementation for BookShop Enterprises sufficiently addresses the standing privilege problem. By converting permanent roles to eligible assignments with Just-in-Time activation and audit logging, a significant reduction of the attack surface is expected without hindering operations.

Key objectives met include implementation of 21 admin roles with the necessary activation settings, approval workflows for 5 high-impact roles, validation of role boundaries to prevent privilege escalation, and quarterly access reviews for ongoing audits.

This project shows a practical application of the principle of least privilege, separation of duties, and defense-in-depth using Microsoft's native identity governance tools.

# References

- Microsoft Learn: Deploy Microsoft Entra Privileged Identity Management
- Microsoft Learn: Configure Entra role settings in PIM
- NIST SP 800-53: AC-2 Account Management
- CIS Controls v8: Control 5 (Account Management), Control 6 (Access Control)
- PCI DSS v4.0: Requirement 7 - Restrict Access by Business Need-to-Know
- SOX Section 404: Internal Controls over Privileged Access
- ISO 27001:2022: A.9.2 Access Rights Management

# Appendix

### Appendix A: Role Assignment Progression Spreadsheet

The accompanying spreadsheet (PIM-Role_Assignments.xlsx) documents the complete progression of role assignments throughout this implementation. The spreadsheet contains three tabs:

**Tab 1: Initial-Role Assignments**

Documents the "before state" of role assignments exported from Microsoft Entra ID prior to PIM implementation. This tab shows the permanent role assignments that existed before any changes were made, including the test account (Rhythm Blues) with 22 permanent roles that were cleaned up.

**Tab 2: Planned-Role Assignments**

Contains the user inventory with job titles, departments, and the planned role assignments based on the principle of least privilege. This tab maps each user's job function to the specific roles they require.

### Tab 3: Role Assignments w/ Approvers

The final PIM configuration showing each role, max activation duration, assigned users, and whether the role requires approval or allows self-activation. This tab serves as the role governance matrix for ongoing administration.

### Tab 4: Final-PIM Roles (After)

The "after state" exported from Entra ID post-PIM implementation. This tab shows the final role assignments with Assignment State (Active or Eligible), pointing to the successful conversion from permanent assignments to JIT-eligible assignments. Only break-glass accounts (BG-Admin01, BG-Admin02) and the primary config account (Chippy Munk) maintain an Active status.