

Privileged Identity Management enabled for Global Administrator role

Control ID: 1.1.5

WHAT THIS RUNBOOK COVERS

PIM for Global Administrators

Table of Contents

- Overview
- Compliance Mapping
- Prerequisites
- What This Control Checks
- Disruption Risk Assessment
- Remediation Steps
 - Option A: Admin Portal (GUI)
 - Option B: PowerShell / Graph API
 - Option C: Automated Remediation
- Verification
- Rollback Procedure
- Required Permissions
- References

Overview

****Privileged Identity Management enabled for Global Administrator role**** is a ****HIGH**** severity control in the Identity & Access Management domain.

Expected Impact: Enables just-in-time privileged access for Global Administrators. Reduces the attack surface by eliminating permanent standing access for most admin users.

Compliance Mapping

This control satisfies requirements across the following frameworks:

Framework	Control Reference
CIS	1.1.5
NIST	AC-6(7)
ISO27001	A.8.2
GDPR	Art.32
SOC2	CC6.3
405D	3.L.B
HIPAA	§164.308(a)(4)(ii)(B) - Access Authorization (Addressable)

Prerequisites

****Required Licenses:**** - Entra ID P2

Required Entra Features:

- Privileged Identity Management

What This Control Checks

****Detection Method:**** Graph API query

Property	Value
Endpoint	<code>/roleManagement/directory/roleEligibilityScheduleInstances</code>
Filter	<code>roleDefinitionId eq '62e90394-69f5-4237-9190-012177145e10'</code>
Validation	at least one PIM eligible assignment exists for Global Administrator role

Disruption Risk Assessment

Risk Level: LOW - Minimal operational impact

Remediation Steps

Option A: Admin Portal (GUI)

1. Sign in to [Microsoft Entra admin center](https://entra.microsoft.com) with Global Administrator or appropriate admin role. 2. Navigate to **Identity Governance > Privileged Identity Management > Entra roles**. 3. Select **Roles** and click **Global Administrator**. 4. Click **Assignments** to see current permanent and eligible assignments. 5. For permanent assignments, click **Remove** and re-add them as **Eligible** assignments. 6. Set an activation duration (e.g., 8 hours) and require justification + approval. 7. Keep only break-glass accounts as permanent; all others should be eligible-only.

Option B: PowerShell / Graph API

```
``powershell # Connect with PIM management scopes Connect-MgGraph -Scopes "RoleManagement.ReadWrite.Directory"
```

Get the role management policy for Global Administrator

```
$gaRoleId = "62e90394-69f5-4237-9190-012177145e10" $assignments = Invoke-MgGraphRequest -Uri  
"https://graph.microsoft.com/v1.0/policies/roleManagementPolicyAssignments?$filter=scopelid eq '/' and scopeType eq 'DirectoryRole' and roleDefinitionId eq  
'$gaRoleId'" $policyId = $assignments.value[0].policyId
```

Convert permanent assignments to eligible for Global Administrator

```
$permanentAssignments = Invoke-MgGraphRequest -Uri "https://graph.microsoft.com/v1.0/roleManagement/directory/roleAssignments?$filter=roleDefinitionId eq  
'$gaRoleId'"
```

For each permanent assignment (except break-glass), create an eligible assignment

```
$permanentAssignments.value | ForEach-Object {
```

```
$body = @{
```

```
action = "adminAssign"
```

```
roleDefinitionId = $gaRoleId
```

```
directoryScopelId = "/"
```

```
principalId = $_.principalId
```

```
scheduleInfo = @{ expiration = @{ type = "afterDuration"; duration =  
"P365D" } }
```

```
}
```

```
Invoke-MgGraphRequest -Uri
```

```
"https://graph.microsoft.com/v1.0/roleManagement/directory/roleEligibility"
```

-Method POST -Body (\$body | ConvertTo-Json -Depth 5)

}

Verify current PIM configuration

Invoke-MgGraphRequest -Uri "https://graph.microsoft.com/v1.0/policies/roleManagementPolicies/\$policyId/rules" | Select-Object -ExpandProperty value | Format-List id, @{N="Setting";E={\$_ | ConvertTo-Json -Depth 3}}

```
<h3 id="option-c-automated-remediation">Option C: Automated Remediation</h3>
This control can be automatically remediated using the Veri-Guard compliance platform:

1. Open your compliance dashboard in the **Veri-Tech Portal**.
2. Navigate to the gap report for this assessment.
3. Select **Auto-Remediate** for control `CIS-1.1.5`.
4. Review the required permissions and approve the remediation.
5. The platform will deploy the fix and confirm the result.

<h2 id="verification">Verification</h2>
After remediation, verify the control is passing:

1. **Re-run the compliance scan** from the Veri-Tech Portal to confirm the control now passes.
2. **Check the updated gap report** - confirm `CIS-1.1.5` shows status `pass`.
3. **Verify directly via Graph API:**
  ``powershell
  Connect-MgGraph -Scopes "Policy.Read.All"
  Invoke-MgGraphRequest -Uri "https://graph.microsoft.com/v1.0/roleManagement/directory/roleEligibilityScheduleInstances"
```

Confirm: at least one PIM eligible assignment exists for Global Administrator role

Rollback Procedure

1. Open the **remediation report** from the Veri-Tech Portal (or the local JSON report if running standalone). 2. Find the entry for `CIS-1.1.5` - the `beforeValue` field contains the original state. 3. Use the PowerShell commands in Option B above, substituting the original values. 4. Re-run the compliance scan from the Veri-Tech Portal to confirm the rollback.

Required Permissions

PIM Role Eligibility (Entra ID P2)

Permission	Scope	Purpose	Data Accessed
Read (scan)	RoleManagement.Read.Directory	Read PIM role assignments and eligibility.	Role assignment metadata. No user data.
Write (remediate)	RoleManagement.ReadWrite.Directory	Create PIM eligible assignments (additive - does not remove permanent assignments).	Role eligibility schedules. No user credentials.

Both permissions require **admin consent** (cannot be user-consented).

Microsoft permission references:

- [RoleManagement.Read.Directory](#)
- [RoleManagement.ReadWrite.Directory](#)

References

- [Microsoft Entra ID documentation](https://learn.microsoft.com/en-us/entra/identity/) - [What is Privileged Identity Management?](https://learn.microsoft.com/en-us/entra/id-governance/privileged-identity-management/pim-configure) - [Assign Entra roles in PIM](https://learn.microsoft.com/en-us/entra/id-governance/privileged-identity-management/pim-how-to-add-role-to-user)