

Require MFA for all users

Control ID: MS.AAD.3.2

WHAT THIS RUNBOOK COVERS

MFA for all users



Veri-Tech

Generated by Veri-Docs · Not a template

Table of Contents

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

Overview

****Require MFA for all users**** is a ****CRITICAL**** severity control in the Identity & Access Management domain.
Expected Impact: All users prompted for MFA on next sign-in. Blocks 99.9% of account compromise attacks.
No service disruption â€” users enroll during next login.

Compliance Mapping

This control satisfies requirements across the following frameworks:

| Framework | Control Reference |
|-----------|-------------------|
| CISA | MS.AAD.3.2 |
| CIS | 1.1.1 |
| NIST | AC-6(2) |
| NIST | CM-1 |
| NIST | CM-2 |
| NIST | CM-6 |
| NIST | CM-7 |
| NIST | CM-7(1) |
| NIST | CM-9 |
| NIST | IA-2 |
| NIST | SA-10 |
| NIST | SA-3 |
| NIST | SA-8 |
| ISO27001 | A.5.1 |
| ISO27001 | A.5.16 |
| ISO27001 | A.5.2 |
| ISO27001 | A.5.31 |
| ISO27001 | A.5.36 |
| ISO27001 | A.5.37 |
| ISO27001 | A.5.4 |
| ISO27001 | A.5.8 |
| ISO27001 | A.8.19 |
| ISO27001 | A.8.25 |
| ISO27001 | A.8.27 |
| ISO27001 | A.8.28 |
| ISO27001 | A.8.30 |
| ISO27001 | A.8.31 |

| Framework | Control Reference |
|-----------|--|
| ISO27001 | A.8.32 |
| ISO27001 | A.8.9 |
| CSF | DE.AE-1 |
| CSF | ID.BE-5 |
| CSF | PR.AC-1 |
| CSF | PR.AC-6 |
| CSF | PR.AC-7 |
| CSF | PR.DS-7 |
| CSF | PR.DS-8 |
| CSF | PR.IP-1 |
| CSF | PR.IP-2 |
| CSF | PR.IP-3 |
| CSF | PR.PT-3 |
| GDPR | Art.24 |
| GDPR | Art.25 |
| GDPR | Art.32 |
| GDPR | Art.5(1)(f) |
| SOC2 | CC6.1 |
| SOC2 | CC6.3 |
| SOC2 | CC8.1 |
| 405D | 3.M.D |
| HIPAA | §164.312(d) - Person or Entity Authentication (Required) |

Prerequisites

****Required Licenses:**** - Entra ID P1 (included in EMS E3/M365 E3)

Required Entra Features:

- Conditional Access

What This Control Checks

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

| Property | Value |
|------------|--|
| Endpoint | <code>/identity/conditionalAccess/policies</code> |
| Validation | grantControls.builtInControls contains 'mfa' AND state eq 'enabled' AND conditions.users.includeUsers contains 'All' |

Compliance Test ID: CISA.MS.AAD.3.2

Microsoft Secure Score Action: MFARegistrationV2

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 ****Protection > Conditional Access > Policies****. 3. Click ****+ New policy**** (or ****New policy from template**** if using Microsoft templates). 4. If using templates, search for ****Require multifactor authentication for all users**** and select it. 5. Set the policy name to ****CISA - Require MFA for All Users****. 6. Under ****Assignments > Users****, select the target users/groups. 7. Under ****Cloud apps or actions****, select ****All cloud apps**** (or specific apps as needed). 8. Under ****Grant****, configure the required controls (e.g., Require MFA). 9. Set ****Enable policy**** to ****Report-only**** for initial testing. 10. Click ****Create****. 11. Monitor the ****Sign-in logs**** and ****CA Insights**** workbook for 7-14 days before enabling.

Option B: PowerShell / Graph API

```
``powershell # Connect with required scopes Connect-MgGraph -Scopes "Policy.ReadWrite.ConditionalAccess"
```

Get the Microsoft-managed CA template

```
Get-MgIdentityConditionalAccessTemplate -ConditionalAccessTemplateId 'a3d0a415-b068-4326-9251-f9cdf9feeb64'
```

Create the Conditional Access policy (report-only mode)

```
$params = @{ displayName = 'CISA - Require MFA for All Users' state = "enabledForReportingButNotEnforced"
conditions = @{ users = @{ includeUsers = @("All") } applications = @{ includeApplications = @("All") } }
```

```
grantControls = @{ operator = "OR" builtInControls = @("mfa") } } New-MgIdentityConditionalAccessPolicy -
BodyParameter $params
```

<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 `CISA-MS.AAD.3.2`.
4. Review the required permissions and approve the remediation.
5. The platform will deploy the fix and confirm the result.

Deployment Safeguards:

- Policy deployed in **report-only** mode (no user impact until enabled)
- Break-glass emergency access account automatically excluded

<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 `CISA-MS.AAD.3.2` 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/identity/conditionalAccess/polic
```

Confirm: grantControls.builtInControls contains 'mfa' AND state eq 'enabled' AND conditions.users.includeUsers contains 'All'

## Rollback Procedure

1. Navigate to **Protection > Conditional Access > Policies**. 2. Find **CISA - Require MFA for All Users** and click to open. 3. Set **Enable policy** to **Off**, or click **Delete**. 4. If the policy was enabled and users are locked out, disable or delete immediately.

## Required Permissions

**Conditional Access Policies**

| Permission        | Scope                                           | Purpose                                                                                                                            | Data Accessed                                                                                                      |
|-------------------|-------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------|
| Read (scan)       | <code>Policy.Read.All</code>                    | Read all tenant policies including Conditional Access rules, authentication methods, and authorization settings.                   | Policy configurations only - no user data, sign-in logs, or credentials.                                           |
| Write (remediate) | <code>Policy.ReadWrite.ConditionalAccess</code> | Create and modify Conditional Access policies. New policies are deployed in report-only mode (no user impact until admin enables). | Conditional Access policy configurations. Cannot read or modify user accounts, group memberships, or sign-in data. |

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

#### Microsoft permission references:

- [Policy.Read.All](#)
- [Policy.ReadWrite.ConditionalAccess](#)

## References

- [Microsoft Entra ID documentation](https://learn.microsoft.com/en-us/entra/identity/) - [Plan a Conditional Access deployment](https://learn.microsoft.com/en-us/entra/identity/conditional-access/plan-conditional-access) - [Conditional Access policy templates](https://learn.microsoft.com/en-us/entra/identity/conditional-access/concept-conditional-access-policy-common) - [CISA M365 Secure Configuration Baselines](https://www.cisa.gov/resources-tools/services/secure-cloud-business-applications-scuba-project)