

# Anonymous users cannot start meetings

Control ID: MS.TEAMS.1.2

## WHAT THIS RUNBOOK COVERS

Anonymous cannot start Teams meetings



## 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

---

**\*\*Anonymous users cannot start meetings\*\*** is a **\*\*CRITICAL\*\*** severity control in the teams domain.

**Expected Impact:** Anonymous users cannot initiate meetings. They must wait for an authenticated organizer to start the meeting.

## Compliance Mapping

---

This control satisfies requirements across the following frameworks:

| Framework | Control Reference |
|-----------|-------------------|
| CISA      | MS.TEAMS.1.2      |
| CIS       | 8.2.1             |
| SOC2      | CC6.1             |
| NIST      | CM-6              |
| NIST      | SC-15a            |
| ISO27001  | A.8.9             |
| CSF       | PR.IP-1           |
| GDPR      | Art.25            |
| GDPR      | Art.32            |

## Prerequisites

**\*\*Required Licenses:\*\*** - Microsoft Teams (included in M365 E3/E5)

## What This Control Checks

**\*\*Compliance Test ID:\*\*** `CISA.MS.TEAMS.1.2`

## Disruption Risk Assessment

**\*\*Risk Level:\*\*** LOW - Minimal operational impact

### What Could Break:

*Restricts who can bypass the meeting lobby.*

## Remediation Steps

### Option A: Admin Portal (GUI)

### Teams Admin Center - Meeting Policy

1. Sign in to the [Microsoft Teams admin center](#) with **Teams Administrator** or **Global Administrator** role.
2. Navigate to **Meetings > Meeting policies > Global (Org-wide default)**.

3. Scroll to the **Meeting join & lobby** section.
4. Set **Anonymous users can join a meeting** to **On** (if needed for external collaboration) but ensure **Anonymous users and dial-in callers can start a meeting** is set to **Off**.
5. Click **Save**.

**What this protects against:** Prevents anonymous users from starting meetings before authenticated organizers arrive, eliminating the risk of unauthorized meetings under your tenant.

## Option B: PowerShell / Graph API

```
``powershell # Connect to Microsoft Teams Connect-MicrosoftTeams
```

## Apply the remediation

```
Set-CsTeamsMeetingPolicy -Identity Global -AllowAnonymousUsersToStartMeeting $false
```

## Verify the change

```
Get-CsTeamsMeetingPolicy | Format-List
```

<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.TEAMS.1.2`.
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 `CISA-MS.TEAMS.1.2` shows status `pass`.
3. **Verify via Teams PowerShell:**

```
``powershell
Connect-MicrosoftTeams
Get-CsTeamsMeetingPolicy -Identity Global
```

**Expected:** AllowAnonymousUsersToStartMeeting eq false

## 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 `CISA-MS.TEAMS.1.2` - 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

**Teams Meeting Policies**

| Permission        | Scope   | Purpose   | Data Accessed  |
|-------------------|---|---|--|
| Read (scan)       | Teams Administrator role (cert-based app-only auth) | Read Teams meeting policy configurations.                           | Meeting policy settings only. No meeting content, chat messages, or user data. |
| Write (remediate) | Teams Administrator role (cert-based app-only auth) | Modify Teams meeting policies (lobby, recording, anonymous access). | Meeting policy configurations.   |

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

**Microsoft permission references:**

- Teams Administrator role (cert-based app-only auth)
- Teams Administrator role (cert-based app-only auth)

## References

- [Microsoft Teams administration](https://learn.microsoft.com/en-us/microsoftteams/teams-overview) - [Manage meeting policies in Teams](https://learn.microsoft.com/en-us/microsoftteams/meeting-policies-overview) - [Teams meeting security](https://learn.microsoft.com/en-us/microsoftteams/teams-security-guide) - [CISA M365 Secure Configuration Baselines](https://www.cisa.gov/resources-tools/services/secure-cloud-business-applications-scuba-project)