

# External access restricted to allowed domains only

Control ID: MS.TEAMS.2.1

## WHAT THIS RUNBOOK COVERS

Restrict Teams external federation



## 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

---

**\*\*External access restricted to allowed domains only\*\*** is a **\*\*CRITICAL\*\*** severity control in the teams domain.

**Expected Impact:** Restricts or disables federation with external organizations. Users cannot chat or call users from non-allowed external domains.

## Compliance Mapping

---

This control satisfies requirements across the following frameworks:

Framework	Control Reference
CISA	MS.TEAMS.2.1
CIS	8.2.4
NIST	AC-3
SOC2	CC6.1
ISO27001	A.5.15
ISO27001	A.5.33
ISO27001	A.8.18
ISO27001	A.8.20
ISO27001	A.8.26
ISO27001	A.8.3
ISO27001	A.8.4
CSF	PR.AC-4
CSF	PR.PT-3
GDPR	Art.32
GDPR	Art.5(1)(f)

## Prerequisites

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

## What This Control Checks

**\*\*Compliance Test ID:\*\*** `CISA.MS.TEAMS.2.1`

## Disruption Risk Assessment

**\*\*Risk Level:\*\*** HIGH - Significant operational impact expected

### What Could Break:

*Disables ALL Teams federation. Users cannot communicate with any external organization via Teams. Existing*

*external chats become inaccessible.*

### Quick Rollback:

```
Set-CsTenantFederationConfiguration -AllowFederatedUsers $true
```

## Remediation Steps

### Option A: Admin Portal (GUI)

### Teams Admin Center - External Access (Federation)

1. Sign in to the [Microsoft Teams admin center](#) with **Teams Administrator** or **Global Administrator** role.
2. Navigate to **Users > External access**.
3. Under **Teams and Skype for Business users in external organizations**:
  - Option 1 (most restrictive): Set to **Block all external domains** to disable federation entirely.
  - Option 2 (allow-list): Set to **Allow only specific external domains** and add only trusted partner domains.
4. Do **not** leave this set to *Allow all external domains* - this permits open federation with any Teams tenant.
5. Click **Save**.

**What this protects against:** *Open federation allows any external Teams user to contact your users, enabling social engineering, phishing, and data exfiltration through Teams chat.*

### Option B: PowerShell / Graph API

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

## Apply the remediation

```
Set-CsTenantFederationConfiguration -AllowFederatedUsers $false
```

## Verify the change

```
Get-CsTenantFederationConfiguration | 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.2.1`.
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.2.1` shows status `pass`.
3. **Verify via Teams PowerShell:**  
``powershell  
Connect-MicrosoftTeams  
Get-CsTenantFederationConfiguration

**Expected:** AllowFederatedUsers eq false OR AllowedDomains has specific domains (not open federation)

## 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.2.1` - 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 Federation Configuration**

Permission	Scope	Purpose	Data Accessed
Read (scan)	Teams Administrator role (cert-based app-only auth)	Read tenant federation settings.	Federation config (allowed domains, consumer access flags). No chat data.
Write (remediate)	Teams Administrator role (cert-based app-only auth)	Modify federation settings to restrict external communication.	Federation configuration only.

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 external access in Teams](https://learn.microsoft.com/en-us/microsoftteams/manage-external-access)  
- [Teams federation configuration](https://learn.microsoft.com/en-us/microsoftteams/trusted-organizations-external-meetings-chat) - [CISA M365 Secure Configuration Baselines](https://www.cisa.gov/resources-tools/services/secure-cloud-business-applications-scuba-project)

---