

# Legacy authentication protocols disabled for SharePoint

Control ID: MS.SHAREPOINT.1.2

## WHAT THIS RUNBOOK COVERS

Block legacy auth, SharePoint



**Veri-Tech**

*Generated by Veri-Docs · Not a template*

## 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

---

**\*\*Legacy authentication protocols disabled for SharePoint\*\*** is a **\*\*HIGH\*\*** severity control in the SharePoint & Collaboration domain.

**Expected Impact:** Older client applications that rely on legacy authentication will lose access. Modern Office apps (2016+) and browser access are unaffected.

## Compliance Mapping

---

This control satisfies requirements across the following frameworks:

Framework	Control Reference
CISA	MS.SHAREPOINT.1.2
CIS	3.8
NIST	IA-2(6)
ISO27001	A.8.5
GDPR	Art.32
SOC2	CC6.1

## Prerequisites

**\*\*Required Licenses:\*\*** - SharePoint Online (included in M365)

## What This Control Checks

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

Property	Value
Endpoint	<code>/admin/sharepoint/settings</code>
Validation	isLegacyAuthProtocolsEnabled eq false

## Disruption Risk Assessment

**\*\*Risk Level:\*\*** MEDIUM - Some users or workflows may be affected

### What Could Break:

*Restricts OneDrive external sharing to existing external users only. Users cannot share files with new external recipients.*

## Remediation Steps

### Option A: Admin Portal (GUI)

1. Sign in to [SharePoint admin center](https://admin.microsoft.com/sharepoint) with Global Administrator or appropriate admin role. 2. Navigate to **\*\*Policies > Sharing\*\***. 3. Locate the setting for **\*\*Legacy authentication**

protocols\*\* ('isLegacyAuthProtocolsEnabled'). 4. Change the value to **Disabled**. 5. Click **Save**.

## Option B: PowerShell / Graph API

```
```powershell # Connect with required scopes Connect-MgGraph -Scopes  
"SharePointTenantSettings.ReadWrite.All"
```

# Update setting: isLegacyAuthProtocolsEnabled = False

```
$body = @{ isLegacyAuthProtocolsEnabled = $False } | ConvertTo-Json
```

```
Invoke-MgGraphRequest -Uri "https://graph.microsoft.com/v1.0/admin/sharepoint/settings" -Method PATCH -  
Body $body
```

<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.SHAREPOINT.1.2'.
4. Review the required permissions and approve the remediation.
5. The platform will deploy the fix and confirm the result.

#### **Deployment Safeguards:**

- Before-state captured in remediation report for **rollback**
- Changes applied immediately via PATCH/PUT

<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.SHAREPOINT.1.2' 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/admin/sharepoint/settings"
```

Confirm: isLegacyAuthProtocolsEnabled 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.SHAREPOINT.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

**SharePoint Tenant Settings**

Permission	Scope	Purpose	Data Accessed
Read (scan)	<code>SharePointTenantSettings.Read.All</code>	Read SharePoint tenant-level sharing and access configuration.	SharePoint admin settings only - no access to site contents, files, or user activity.
Write (remediate)	<code>SharePointTenantSettings.ReadWrite.All</code>	Modify SharePoint sharing defaults, external access levels, and guest policies.	SharePoint tenant configuration. Cannot access site contents, files, libraries, or user permissions on specific sites.

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

### Microsoft permission references:

- [SharePointTenantSettings.Read.All](#)
- [SharePointTenantSettings.ReadWrite.All](#)

## References

- [SharePoint administration](https://learn.microsoft.com/en-us/sharepoint/sharepoint-online) - [Manage sharing settings](https://learn.microsoft.com/en-us/sharepoint/turn-external-sharing-on-or-off) - [CISA M365 Secure Configuration Baselines](https://www.cisa.gov/resources-tools/services/secure-cloud-business-applications-scuba-project)