

# Unified audit logging enabled

Control ID: MS.EXO.8.1

## WHAT THIS RUNBOOK COVERS

Unified Audit Log enabled



## 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

---

**\*\*Unified audit logging enabled\*\*** is a **\*\*CRITICAL\*\*** severity control in the exchange domain.

**Expected Impact:** No disruption. Enables centralized audit logging across Microsoft 365 services. Required for security investigation and compliance.

## Compliance Mapping

---

This control satisfies requirements across the following frameworks:

Framework	Control Reference
CISA	MS.EXO.8.1
CIS	6.5.3
NIST	AC-3
NIST	AC-5
NIST	AC-6
NIST	AU-2
NIST	AU-6(1)
NIST	AU-7
NIST	CA-9
NIST	IR-4(1)
NIST	MP-2
NIST	SC-7
NIST	SI-4(2)
NIST	SI-4(5)
ISO27001	A.5.10
ISO27001	A.5.14
ISO27001	A.5.15
ISO27001	A.5.3
ISO27001	A.5.33
ISO27001	A.7.10
ISO27001	A.7.7
ISO27001	A.8.15
ISO27001	A.8.16
ISO27001	A.8.18
ISO27001	A.8.2
ISO27001	A.8.20
ISO27001	A.8.22

Framework	Control Reference
ISO27001	A.8.23
ISO27001	A.8.26
ISO27001	A.8.3
ISO27001	A.8.4
CSF	DE.CM-1
CSF	ID.AM-3
CSF	PR.AC-4
CSF	PR.AC-5
CSF	PR.DS-1
CSF	PR.DS-5
CSF	PR.PT-1
CSF	PR.PT-2
CSF	PR.PT-3
CSF	PR.PT-4
CSF	RS.AN-3
GDPR	Art.32
GDPR	Art.33
GDPR	Art.5(1)(f)
SOC2	CC6.1
SOC2	CC6.4
SOC2	CC7.2
SOC2	CC7.4
405D	8.M.A
HIPAA	§164.312(b) - Audit Controls (Required)

## Prerequisites

\*\*Required Licenses:\*\* - Exchange Online (included in M365 E3/E5)

## What This Control Checks

**Compliance Test ID:** `CISA.MS.EXO.8.1`

## Remediation Steps

### Option A: Admin Portal (GUI)

1. Sign in to the [Microsoft Purview compliance portal](https://compliance.microsoft.com) with **Compliance Administrator** or **Global Administrator** role. 2. Navigate to **Audit**. 3. In Microsoft Purview compliance portal > Audit, ensure auditing is turned on. Or use PowerShell: Set-AdminAuditLogConfig -UnifiedAuditLogIngestionEnabled \$true 4. Click **Save**.

### Option B: PowerShell / Graph API

```
```powershell # Connect to Exchange Online Connect-ExchangeOnline
```

## Apply the remediation

```
Set-AdminAuditLogConfig -UnifiedAuditLogIngestionEnabled $true
```

**Option C: Automated Remediation**

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.EXO.8.1`.
4. Review the required permissions and approve the remediation.
5. The platform will deploy the fix and confirm the result.

**Verification**

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.EXO.8.1` shows status `pass`.
3. **Verify via Exchange Online PowerShell:**

```
```powershell
Connect-ExchangeOnline
Get-AdminAuditLogConfig
```

**Expected:** UnifiedAuditLogIngestionEnabled eq true

## 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.EXO.8.1` - 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

---

**Exchange Audit Configuration** (scan only)

Permission	Scope	Purpose
Read (scan)	``	Read-only access for compliance scanning

### **Note:**

### **Microsoft permission references:**

- 

## References

---

- [Exchange Online documentation](https://learn.microsoft.com/en-us/exchange/exchange-online) - [Email authentication in Exchange Online](https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/email-authentication-about) - [CISA M365 Secure Configuration Baselines] (https://www.cisa.gov/resources-tools/services/secure-cloud-business-applications-scuba-project)