

# Auto-forwarding to external domains disabled

Control ID: MS.EXO.1.1

## WHAT THIS RUNBOOK COVERS

Block external auto-forward



**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

---

**\*\*Auto-forwarding to external domains disabled\*\*** is a **\*\*CRITICAL\*\*** severity control in the exchange domain.

**Expected Impact:** Blocks automatic email forwarding to external domains. Users with existing forwarding rules will have external forwards rejected. Internal forwarding is unaffected.

## Compliance Mapping

---

This control satisfies requirements across the following frameworks:

Framework	Control Reference
CISA	MS.EXO.1.1
CIS	6.2.1
NIST	AC-4
NIST	CM-6
ISO27001	A.5.14
ISO27001	A.8.22
ISO27001	A.8.23
ISO27001	A.8.9
CSF	DE.AE-1
CSF	ID.AM-3
CSF	PR.AC-5
CSF	PR.DS-5
CSF	PR.IP-1
GDPR	Art.25
GDPR	Art.32
GDPR	Art.5(1)(f)
SOC2	CC6.7
405D	1.M.A

## Prerequisites

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

## What This Control Checks

**\*\*Compliance Test ID:\*\*** `CISA.MS.EXO.1.1`

## Disruption Risk Assessment

---

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

### What Could Break:

*Creates transport rule blocking external auto-forwarding. Users with active external forwarding rules will silently stop receiving forwarded mail at external addresses.*

### Quick Rollback:

```
Remove-TransportRule -Identity "Block External Auto-Forwarding" -Confirm:$false
```

## Remediation Steps

---

### Option A: Admin Portal (GUI)

1. Sign in to [Exchange admin center](https://admin.exchange.microsoft.com) with Global Administrator or appropriate admin role. 2. Navigate to **(See control-specific steps below)**. 3. Navigate to **Mail flow > Remote domains**. 4. Select the **Default** remote domain. 5. Under **Automatic replies**, find **Allow automatic forwarding**. 6. Set **Allow automatic forwarding** to **Off**. 7. Click **Save**.

**What this protects against:** *Disabling auto-forwarding at the remote domain level prevents users from setting up mailbox rules that forward email to external addresses, which is a common data exfiltration technique.*

### Option B: PowerShell / Graph API

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

## Disable automatic forwarding at the remote domain level

---

```
Set-RemoteDomain -Identity Default -AutoForwardEnabled $false
```

## Verify the change

---

```
Get-RemoteDomain -Identity Default | Select-Object Identity, AutoForwardEnabled
```

### <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.EXO.1.1`.
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.EXO.1.1` shows status `pass`.
3. **Verify via Exchange Online PowerShell:**  
``powershell  
Connect-ExchangeOnline  
Get-TransportRule

**Expected:** No transport rule allows auto-forwarding to external domains

## 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.1.1` - 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 Transport Rules** (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>)

---

*Generated by Veri-Docs Policy Library | 2026-04-27 | Remediation Runbook | Registry v2.1.0*