

Standard and strict preset security policies enabled

Control ID: MS.DEFENDER.1.1

WHAT THIS RUNBOOK COVERS

Defender preset security policies



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

****Standard and strict preset security policies enabled**** is a ****CRITICAL**** severity control in the defender domain.

Expected Impact: Enables standard and strict anti-spam, anti-malware, and anti-phishing protections. Standard applies safe defaults; strict uses aggressive detection thresholds.

Compliance Mapping

This control satisfies requirements across the following frameworks:

Framework	Control Reference
CISA	MS.DEFENDER.1.1
NIST	CM-6
NIST	SI-3
SOC2	CC6.1
ISO27001	A.8.7
ISO27001	A.8.9
CSF	DE.CM-4
CSF	DE.DP-3
CSF	PR.IP-1
GDPR	Art.25
GDPR	Art.32
HIPAA	§164.308(a)(5)(ii)(B) - Protection from Malicious Software (Addressable)

Prerequisites

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

What This Control Checks

****Compliance Test ID:**** `CISA.MS.DEFENDER.1.1`

Disruption Risk Assessment

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

Remediation Steps

Option A: Admin Portal (GUI)

Microsoft Defender Portal - Preset Security Policies

1. Sign in to the [Microsoft Defender portal](#) with **Security Administrator** or **Global Administrator** role.

2. Navigate to **Email & collaboration > Policies & rules > Threat policies > Preset security policies**.
3. Under **Standard protection**, click **Manage protection settings**.
4. Review the protection settings - Standard protection includes anti-spam, anti-malware, anti-phishing, Safe Links, and Safe Attachments with Microsoft-recommended settings.
5. Click **Confirm** to enable Standard protection.
6. Repeat for **Strict protection** - click **Manage protection settings** under the Strict section.
7. Strict protection applies more aggressive filtering thresholds and actions (quarantine instead of junk folder, etc.).
8. Click **Confirm** to enable Strict protection.

***Note:** Standard and Strict preset policies take precedence over custom policies. Microsoft maintains and updates the protection settings automatically.*

Option B: PowerShell / Graph API

```
```powershell # Connect to Exchange Online (required for preset security policy cmdlets) Connect-ExchangeOnline
```

## Check current preset security policy state

```
Get-EOPProtectionPolicyRule | Format-List Name, State, SentTo, RecipientDomains
Get-ATPPProtectionPolicyRule | Format-List Name, State, SentTo, RecipientDomains
```

## Enable Standard preset security policy

```
Enable-EOPProtectionPolicyRule -Identity "Standard Preset Security Policy"
Enable-ATPPProtectionPolicyRule -Identity "Standard Preset Security Policy"
```

## Enable Strict preset security policy

```
Enable-EOPProtectionPolicyRule -Identity "Strict Preset Security Policy"
Enable-ATPPProtectionPolicyRule -Identity "Strict Preset Security Policy"
```

## Verify the changes

```
Get-EOPProtectionPolicyRule | Format-List Name, State, SentTo, RecipientDomains
Get-ATPPProtectionPolicyRule | Format-List Name, State, SentTo, RecipientDomains
```

### <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.DEFENDER.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.DEFENDER.1.1` shows status `pass`.
3. **Verify via Defender/EOP PowerShell:**  
``powershell  
Connect-ExchangeOnline  
Get-EOPProtectionPolicyRule

**Expected:** Standard and Strict preset EOP rules exist and are enabled (State eq Enabled)

## 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.DEFENDER.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

**Defender Preset Security Policies**

Permission	Scope	Purpose	Data Accessed
Read (scan)	Exchange.ManageAsApp (+ Exchange Administrator role)	Read preset security policy rule configurations and scope.	Preset policy rules, enabled state, and recipient scope. No email content.
Write (remediate)	Exchange.ManageAsApp (+ Exchange Administrator role)	Enable preset policies and configure recipient scope (all users or specific groups).	Preset security policy configurations.

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

**Microsoft permission references:**

- [Exchange.ManageAsApp](#) (+ Exchange Administrator role)
- [Exchange.ManageAsApp](#) (+ Exchange Administrator role)

## References

---

- [Microsoft Defender for Office 365 documentation](<https://learn.microsoft.com/en-us/defender-office-365/mdo-about>) - [Preset security policies in EOP and Defender for O365](<https://learn.microsoft.com/en-us/defender-office-365/preset-security-policies>) - [Configure protection policies](<https://learn.microsoft.com/en-us/defender-office-365/mdo-deployment-guide>) - [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*