Experts Live Netherlands

Maester

Microsoft Identity Masterclass
Experts Live Netherlands 2026

Experts Live Netherlands

Stephan van Rooij

Software developer & Microsoft MVP in Security

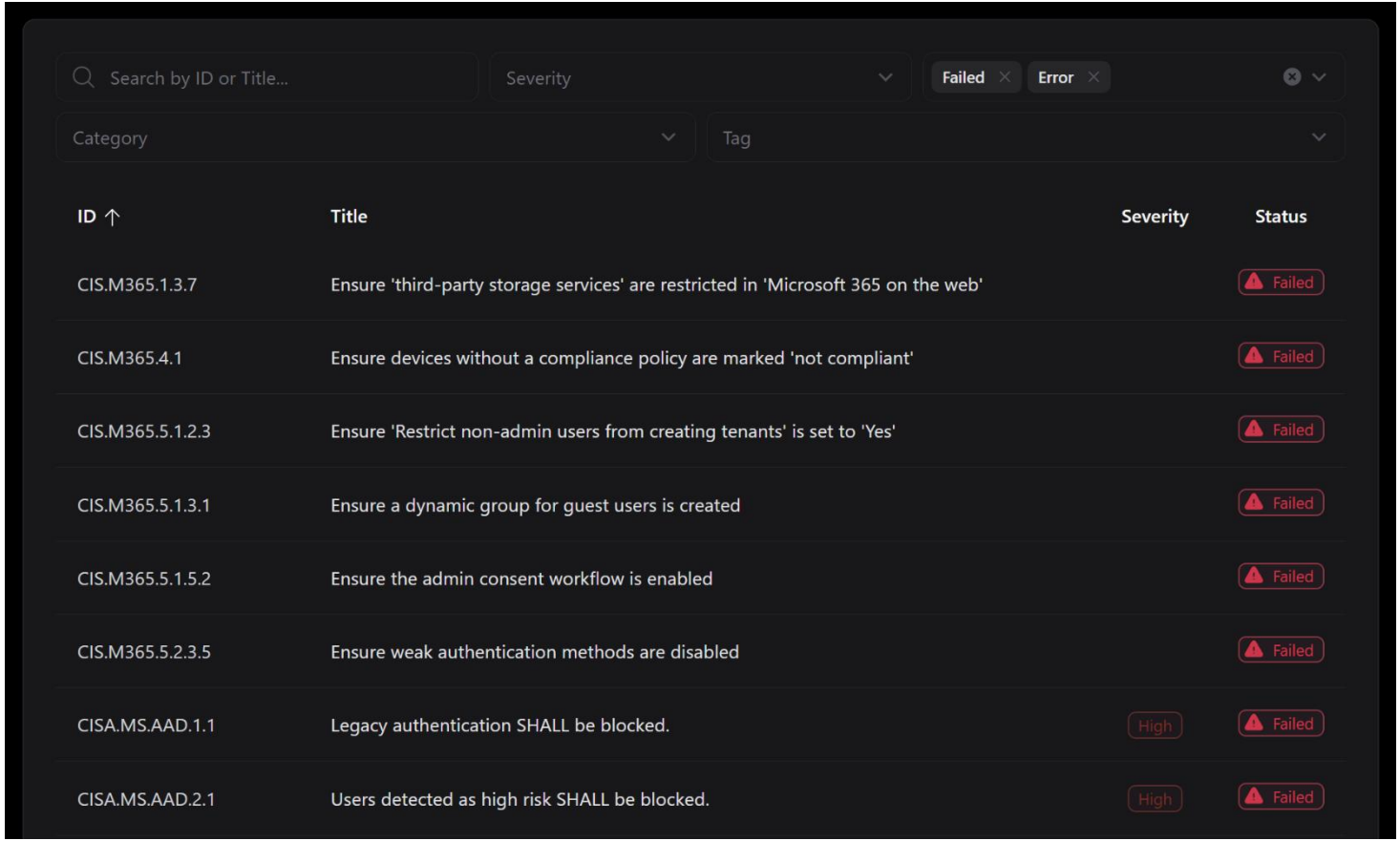
Microsoft SOFTWARE CENTRAL Capgemini inforcer DELL Technologies nerdio SUPER VISION INTERSTELLAR kpn Partner Network INSPARK

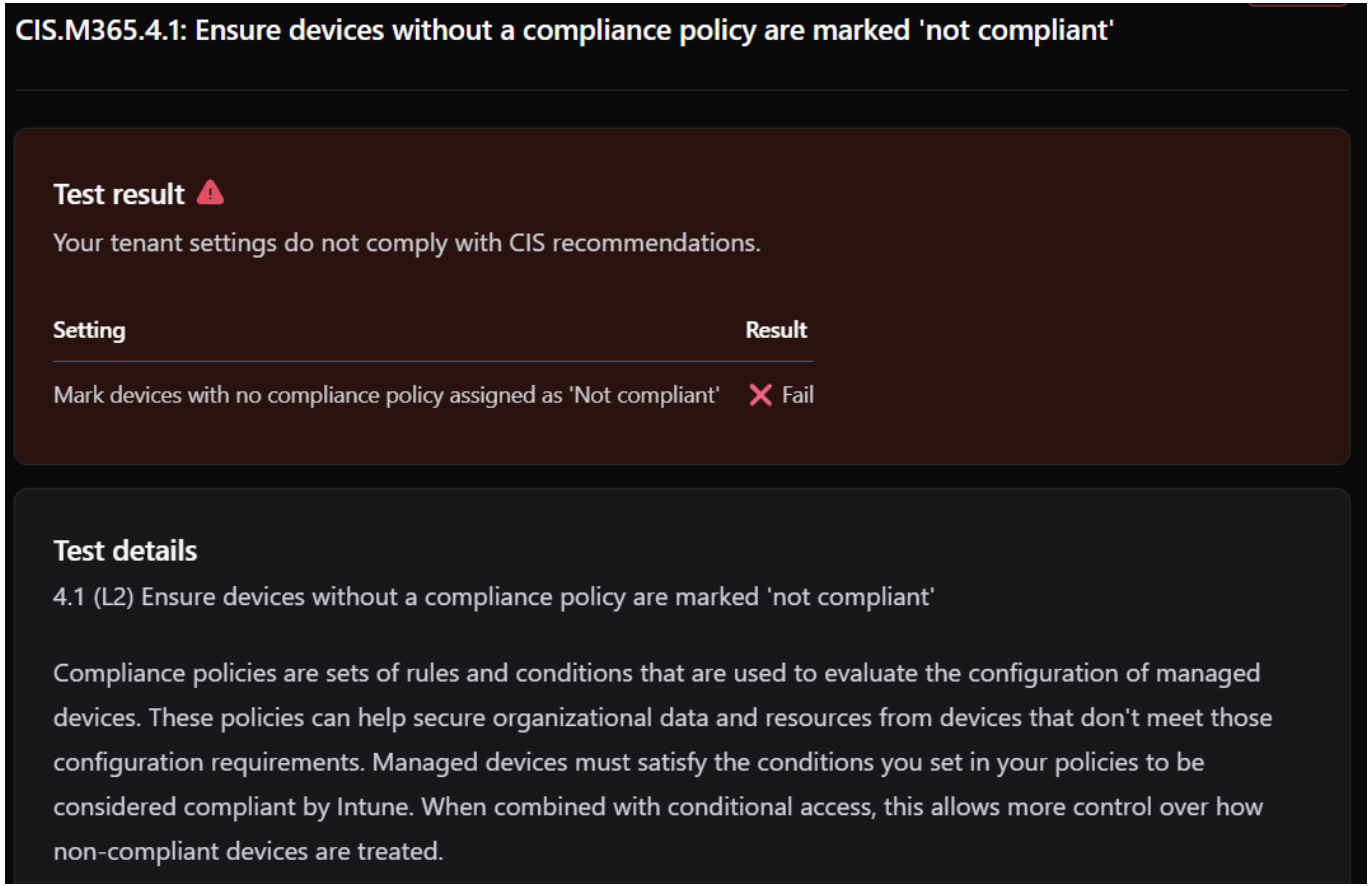
Experts Live Netherlands

Maester

- Security configuration scanner
- Actionable report
- Only **read access** required
- PowerShell open-source

Microsoft · SOFTWARE CENTRAL · Capgemini · inforcer · DELL Technologies · nerdio · SUPER VISION · INTERSTELLAR · kpn Partner Network · INSPARK


Search by ID or Title...
Severity
Failed
Error
Category
Tag
ID
Title
Severity
Status
CIS.M365.1.3.7
Ensure 'third-party storage services' are restricted in 'Microsoft 365 on the web'
Failed
CIS.M365.4.1
Ensure devices without a compliance policy are marked 'not compliant'
Failed
CIS.M365.5.1.2.3
Ensure 'Restrict non-admin users from creating tenants' is set to 'Yes'
Failed
CIS.M365.5.1.3.1
Ensure a dynamic group for guest users is created
Failed
CIS.M365.5.1.5.2
Ensure the admin consent workflow is enabled
Failed
CIS.M365.5.2.3.5
Ensure weak authentication methods are disabled
Failed
CISA.MS.AAD.1.1
Legacy authentication SHALL be blocked.
High
Failed
CISA.MS.AAD.2.1
Users detected as high risk SHALL be blocked.
High
Failed


CIS.M365.4.1: Ensure devices without a compliance policy are marked 'not compliant'
Test result
Your tenant settings do not comply with CIS recommendations.
Setting
Result
Mark devices with no compliance policy assigned as 'Not compliant'
Fail
Test details
4.1 (L2) Ensure devices without a compliance policy are marked 'not compliant'
Compliance policies are sets of rules and conditions that are used to evaluate the configuration of managed devices. These policies can help secure organizational data and resources from devices that don't meet those configuration requirements. Managed devices must satisfy the conditions you set in your policies to be considered compliant by Intune. When combined with conditional access, this allows more control over how non-compliant devices are treated.

considered compliant by Intune. When combined with conditional access, this allows more control over how non-compliant devices are treated.

The recommended state is **Mark devices with no compliance policy assigned as Not compliant**

Rationale

Implementing this setting is a first step in adopting compliance policies for devices. When used in together with Conditional Access policies the attack surface can be reduced by forcing an action to be taken for non-compliant devices.

> ***"Note: This section does not focus on which compliance policies to use, only that an organization should adopt and enforce them to their needs."***

Impact

Any devices without a compliance policy will be marked not compliant. Care should be taken to first deploy any new compliance policies with a Conditional Access (CA) policy that is in the Report-only state. After the environment's device compliance is better understood it is then appropriate to finally align with **Mark devices with no compliance policy assigned as** and enable any CA policies that enforce actions based on device compliance.

considered not compliant.

Remediation action:

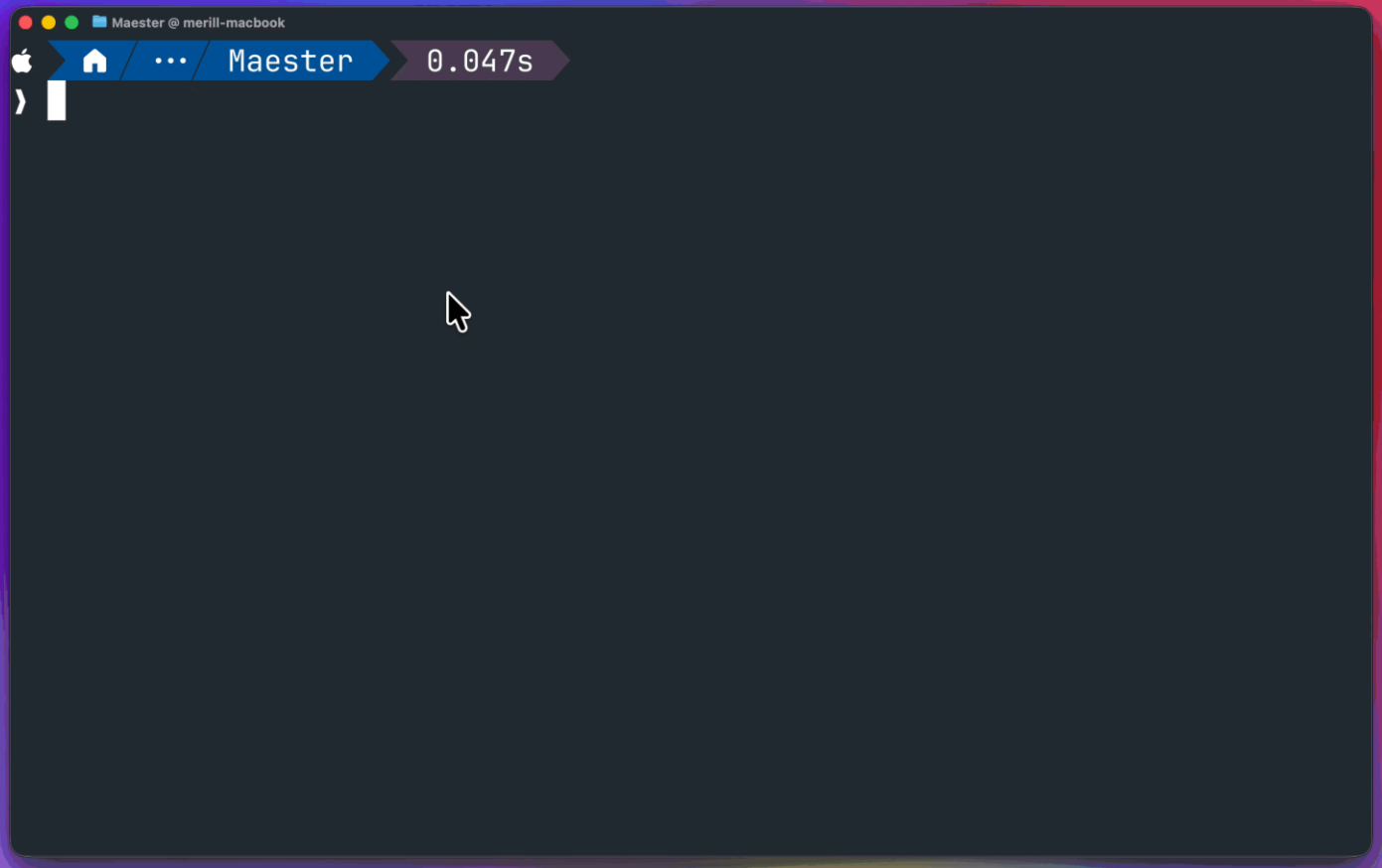
1. Navigate to **Microsoft Intune admin center**.
2. Click on **Devices** and then under **Managed devices** on **Compliance**.
3. Click **Compliance settings**.
4. Ensure **Mark devices with no compliance policy assigned as** set to **Not compliant**

PowerShell

1. Connect to Microsoft Graph using **`Connect-MgGraph -Scopes "DeviceManagementConfiguration.ReadWrite.All"`**
2. Run the following commands:

```
$Uri = 'https://graph.microsoft.com/v1.0/deviceManagement'
$Body = @{
    settings = @{
        secureByDefault = $true
    }
} | ConvertTo-Json
```


Experts Live Netherlands
Erik Scherder
Dept. of Clinical Neuropsychology
VU university
Amsterdam, the Netherlands
Demo
Microsoft
SOFTWARE CENTRAL
Capgemini
inforcer
DELL Technologies
nerdio
SUPER VISION
INTERSTELLAR
kpn Partner Network
INSPARK



Expe

Microsoft SOFTWARE CENTRAL Capgemini inforcer DELL Technologies nerdio SUPER VISION INTERSTELLAR kpn Partner Network INSPARK

Experts Live Netherlands

Maester Workshop goals

1. Install Maester
2. Install built-in tests
3. Run Maester
4. (maybe) Schedule Maester on GitHub Actions
5. Deploy Maester report to Static Web App with auth


Experts Live Netherlands
https://github.com/IdentityMan/MasterclassELNL26/
Questions?
Microsoft
SOFTWARE CENTRAL
Capgemini
inforcer
DELL Technologies
nerdio
SUPER VISION
INTERSTELLAR
kpn Partner Network
INSPARK