Integrate compliance policy with Conditional Access policies

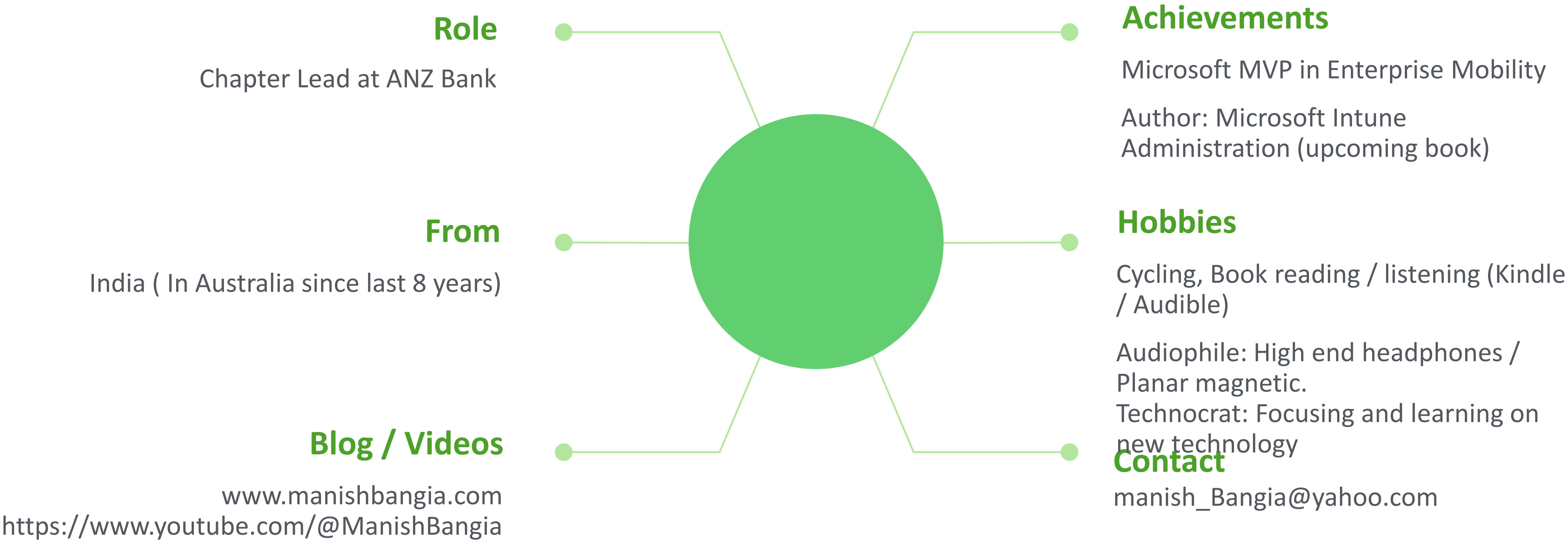
Workplace Ninjas Australia

Thank you Sponsors

Microsoft

DEVICIE

About Manish Bangia



Role

Chapter Lead at ANZ Bank

From

India (In Australia since last 8 years)

Blog / Videos

www.manishbangia.com
https://www.youtube.com/@ManishBangia

Achievements

Microsoft MVP in Enterprise Mobility

Author: Microsoft Intune Administration (upcoming book)

Hobbies

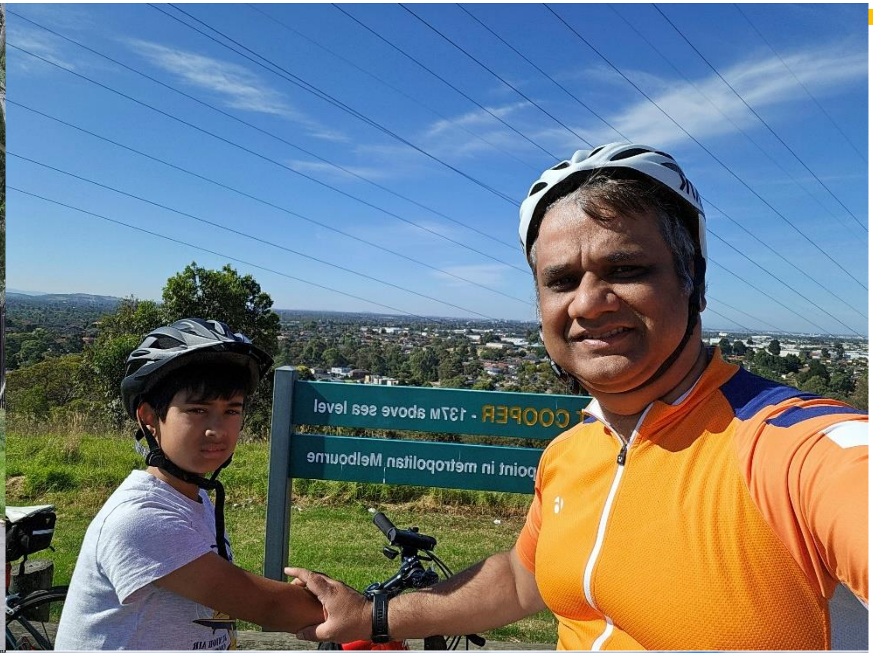
Cycling, Book reading / listening (Kindle / Audible)

Audiophile: High end headphones / Planar magnetic.
Technocrat: Focusing and learning on new technology

Contact

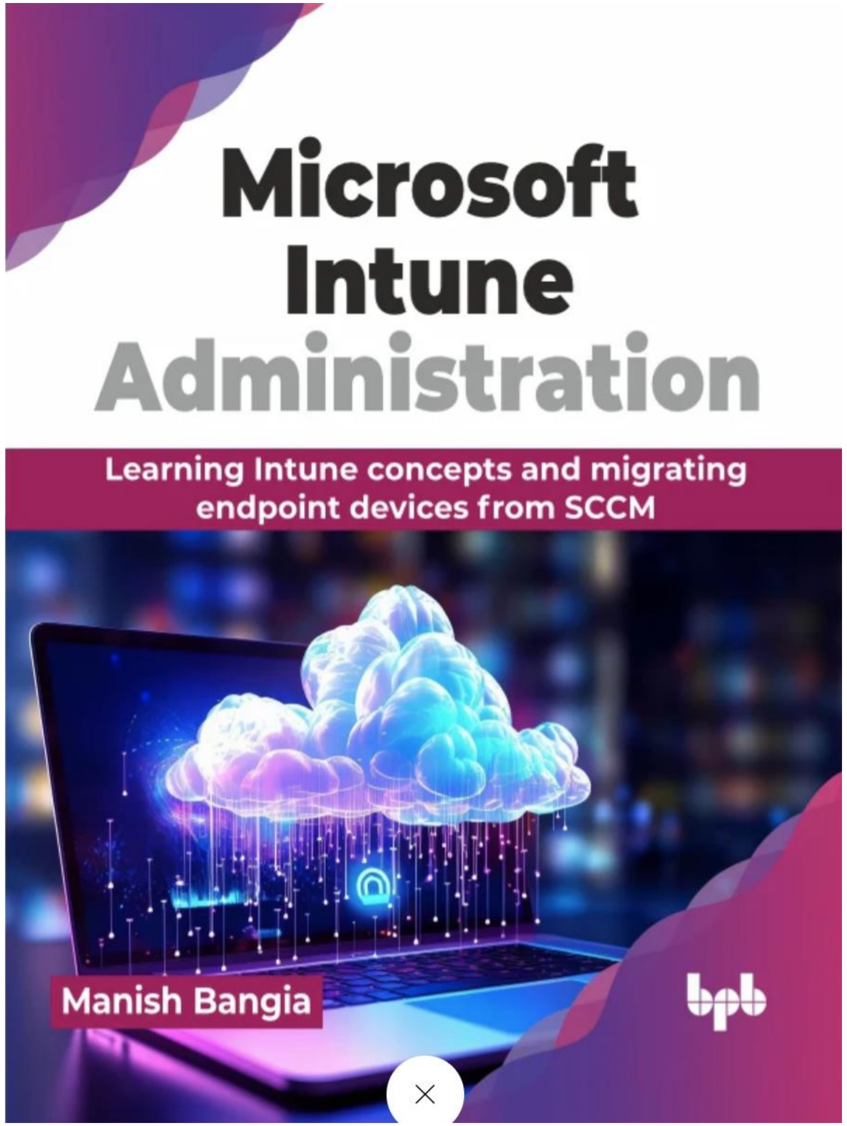
manish_Bangia@yahoo.com

Random Pics



COOPER - 137M above sea level
point in metropolitan Melbourne

Book



Microsoft Intune Administration

Learning Intune concepts and migrating endpoint devices from SCCM

Manish Bangia

bpb

Agenda

Compliance policies

- What is Compliance policy

Compliance policy areas

- Tenant-wide configuration
- Device Compliance settings

Compliance policy rules and settings

- Built-in rules and settings
- Custom rules – consists of Discovery script and JSON file

Conditional access policies

Demo

Integrate compliance policy with Conditional Access policies

What is Compliance policy

- Rules to evaluate the specific configuration on managed devices.
- Examples: BitLocker, Secure Boot, TPM, Minimum OS version, Defender endpoint rules etc.
- The purpose is to secure the device by setting up the minimum configuration required by the organization.

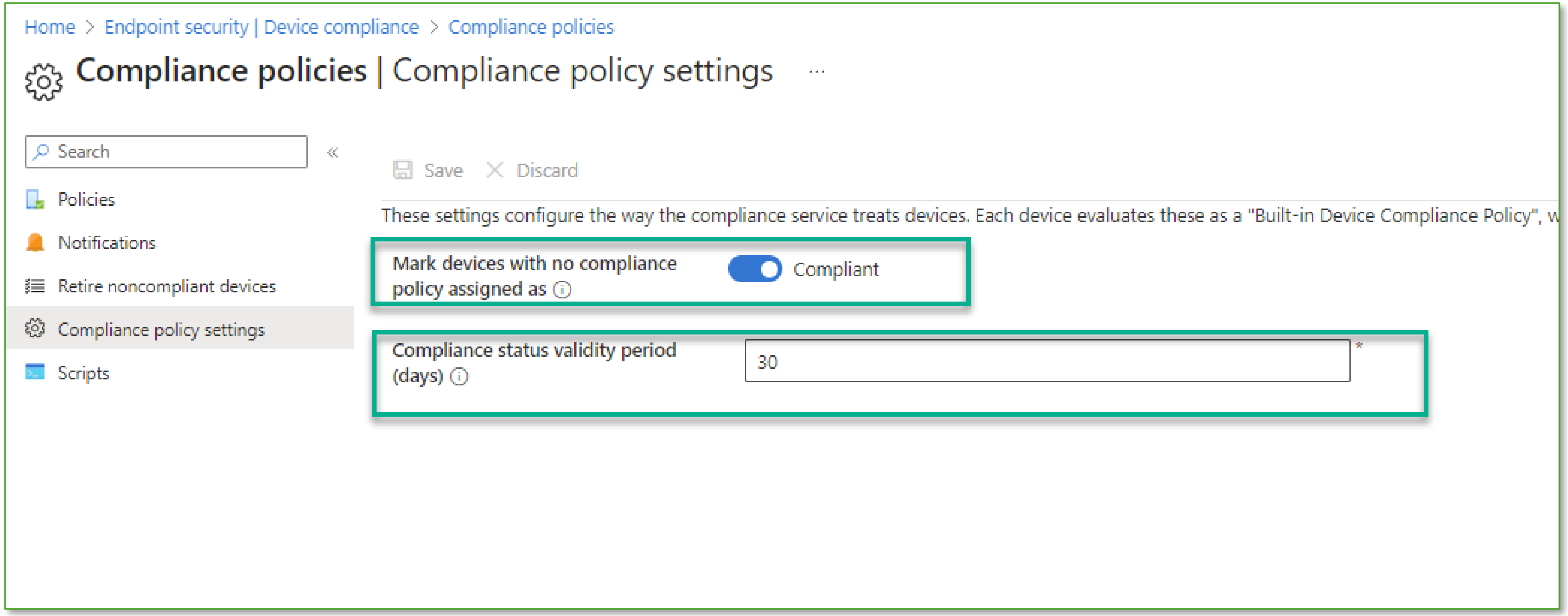
Compliance policy areas

- **Tenant-wide configuration:** These are Built-in device compliance policy. It applies to all devices.
- **Device Compliance settings:** The policy which you are going to create manually.

Compliance policy area

Tenant-wide configuration

- **Mark devices with no compliance policy assigned as:** Compliant / Non-compliant
- **Compliance status validity period:** 30



Home > Endpoint security | Device compliance > Compliance policies

Compliance policies | Compliance policy settings ...

These settings configure the way the compliance service treats devices. Each device evaluates these as a "Built-in Device Compliance Policy", w

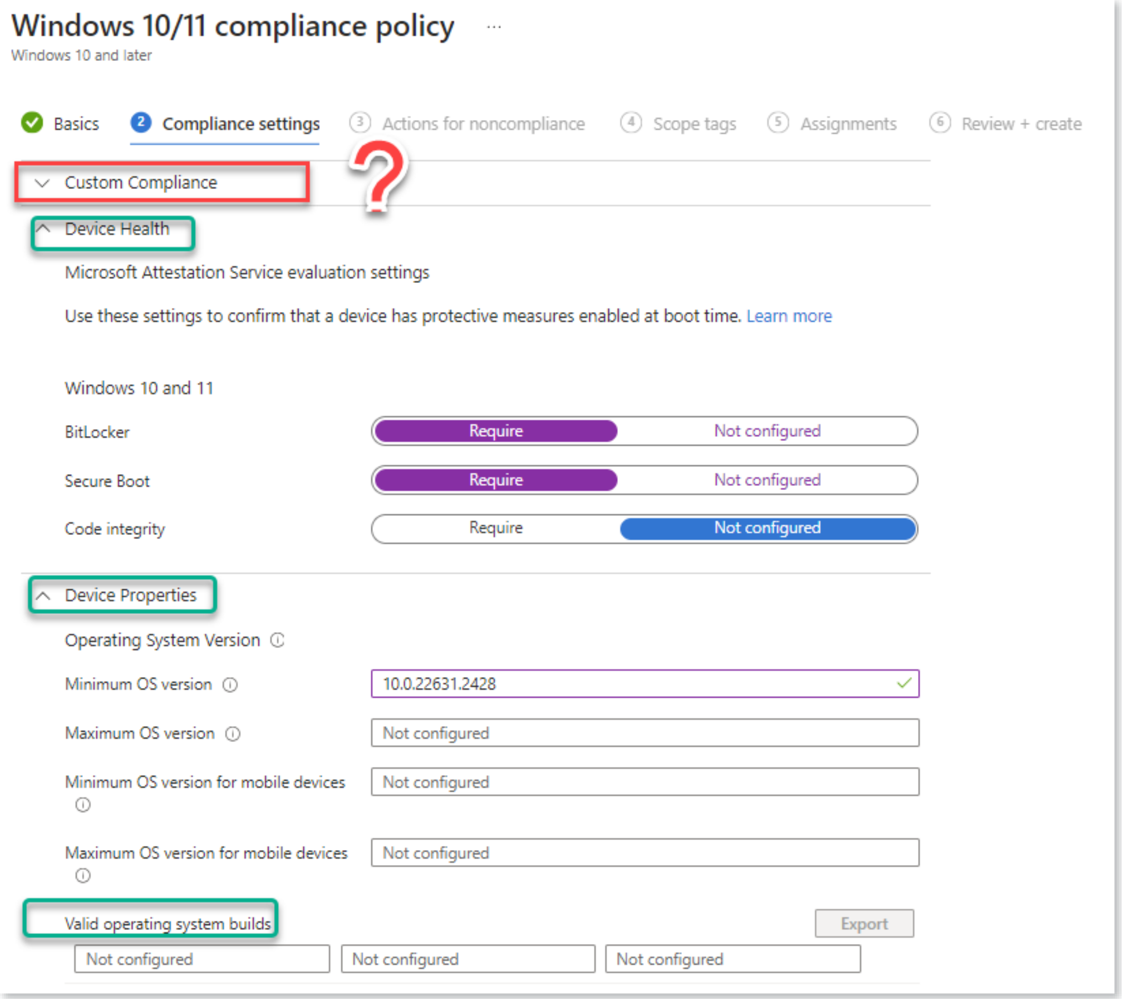
Mark devices with no compliance policy assigned as ⓘ ● Compliant

Compliance status validity period (days) ⓘ 30 *

Compliance policy area

Compliance policy settings – Readily available rules

- Available rules and settings for compliance policies.
- The settings are grouped in various categories:
  - Device Health
  - Device Properties
  - Configuration Manager Compliance
  - System Security
  - Microsoft Defender for Endpoint



Windows 10/11 compliance policy ...

Windows 10 and later

Custom Compliance

Device Health

Microsoft Attestation Service evaluation settings

Use these settings to confirm that a device has protective measures enabled at boot time. Learn more

Windows 10 and 11

BitLocker: Require (selected) | Not configured

Secure Boot: Require (selected) | Not configured

Code integrity: Require | Not configured (selected)

Device Properties

Operating System Version ⓘ

Minimum OS version ⓘ: 10.0.22631.2428 ✓

Maximum OS version ⓘ: Not configured

Minimum OS version for mobile devices ⓘ: Not configured

Maximum OS version for mobile devices ⓘ: Not configured

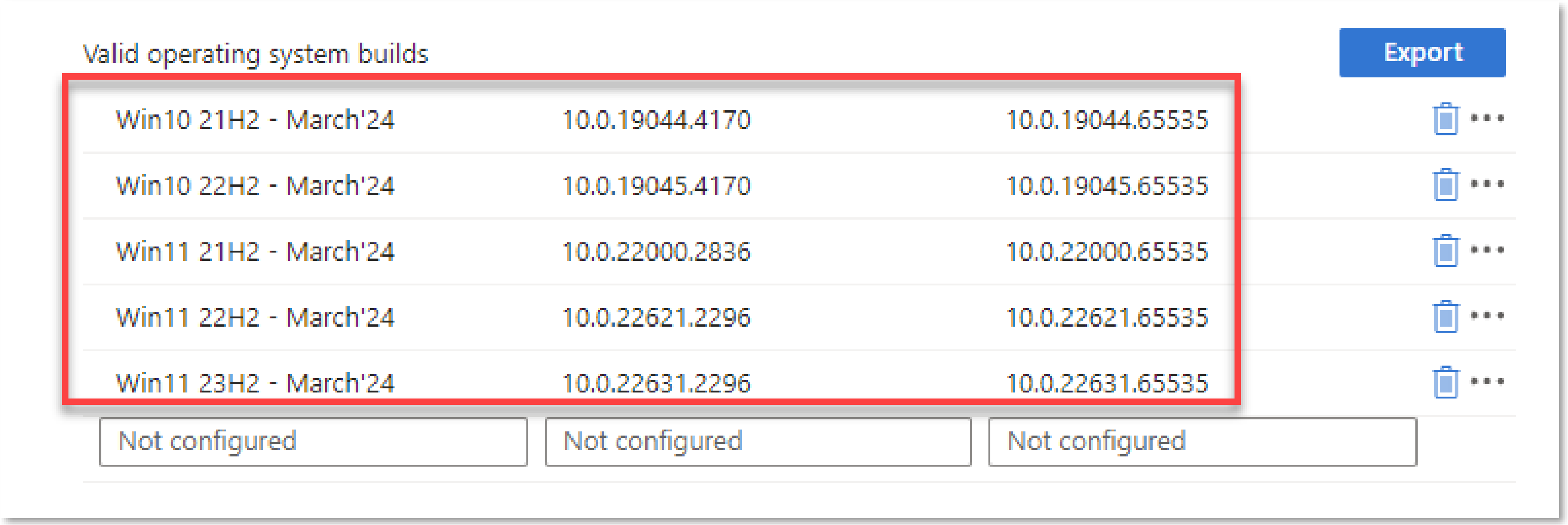
Valid operating system builds

Export

Not configured | Not configured | Not configured

Compliance policy area

Example: Valid operating system builds



Valid operating system builds

Win10 21H2 - March'24	10.0.19044.4170	10.0.19044.65535
Win10 22H2 - March'24	10.0.19045.4170	10.0.19045.65535
Win11 21H2 - March'24	10.0.22000.2836	10.0.22000.65535
Win11 22H2 - March'24	10.0.22621.2296	10.0.22621.65535
Win11 23H2 - March'24	10.0.22631.2296	10.0.22631.65535
Not configured	Not configured	Not configured

Major.minor.build.version:

- **Major.minor**: 10.0 (For Windows 10 and 11)
- **Build:**

19044	Win10 21H2
19045	Win10 22H2
22000	Win11 21H2
22621	Win11 22H2
22631	Win11 23H2

- **Version:** patch version (increments with every new update release)

Search for:
Windows 11 Update history
Windows 11 Release information

Compliance policy area – custom rules

What if built-in rules are not available?

- Wait for the rules / settings to be released by Microsoft.

  Or

- Create your own custom rule.

Examples of custom compliance

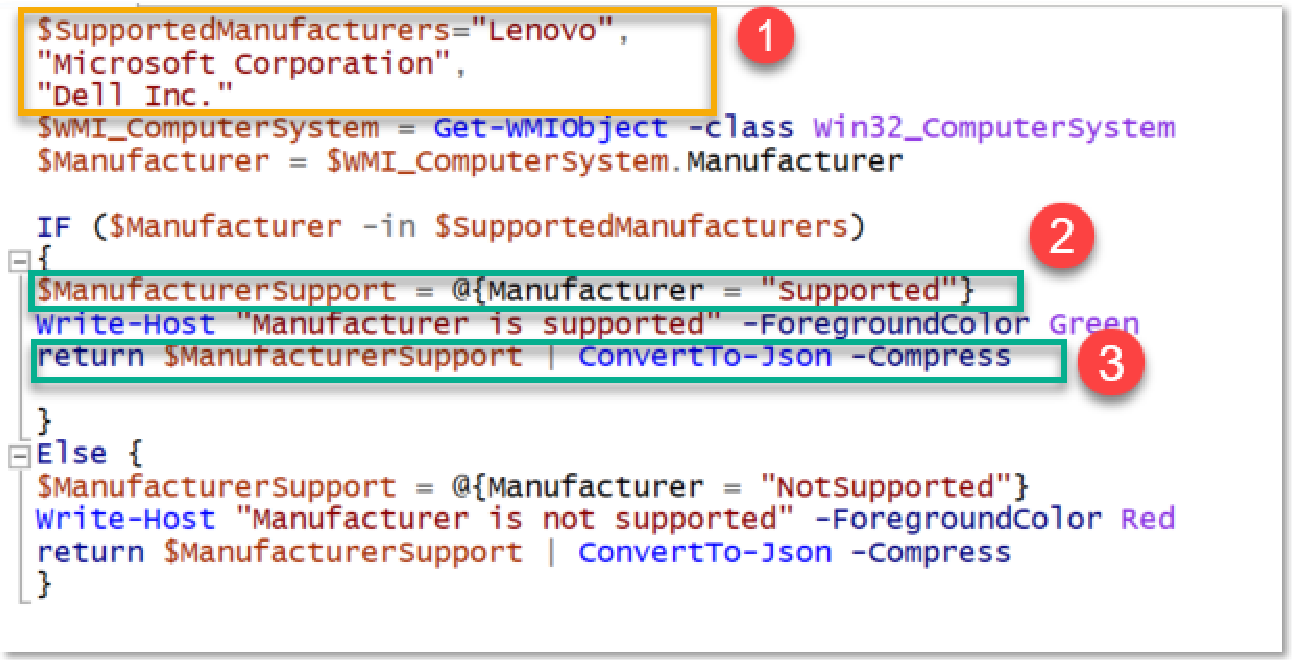
- Device having specific corporate make and model.
- Device should have specific version of Edge / Chrome installed.
- Should have minimum 20GB of disk space.

Custom compliance rule consists of:

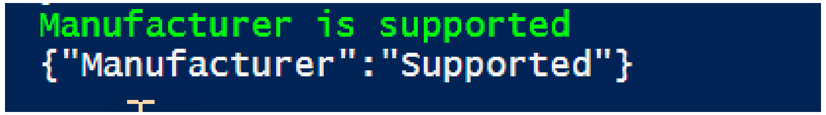
- **Discovery script:** It is a PowerShell script to discover and detect the setting. PowerShell’s last line includes the detection of output into JSON format. JSON file is a custom prepared file for the settings you are looking for.
- **JSON file:** We have to create JSON file which will include the settings you are looking for. JSON file will then be compared with Discovery script’s output. If the value doesn’t match, device will be marked as non-compliant.

Compliance policy area – custom rules

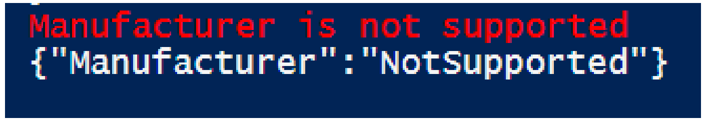
Discovery script (PowerShell) - Check certified Manufacturer



```
$SupportedManufacturers="Lenovo",
"Microsoft Corporation",
"Dell Inc."
$WMI_ComputerSystem = Get-WMIObject -class Win32_ComputerSystem
$Manufacturer = $WMI_ComputerSystem.Manufacturer

IF ($Manufacturer -in $SupportedManufacturers)
{
$ManufacturerSupport = @{Manufacturer = "Supported"}
Write-Host "Manufacturer is supported" -ForegroundColor Green
return $ManufacturerSupport | ConvertTo-Json -Compress

}
Else {
$ManufacturerSupport = @{Manufacturer = "NotSupported"}
Write-Host "Manufacturer is not supported" -ForegroundColor Red
return $ManufacturerSupport | ConvertTo-Json -Compress
}
```



```
Manufacturer is supported
{"Manufacturer":"Supported"}
```



```
Manufacturer is not supported
{"Manufacturer":"NotSupported"}
```

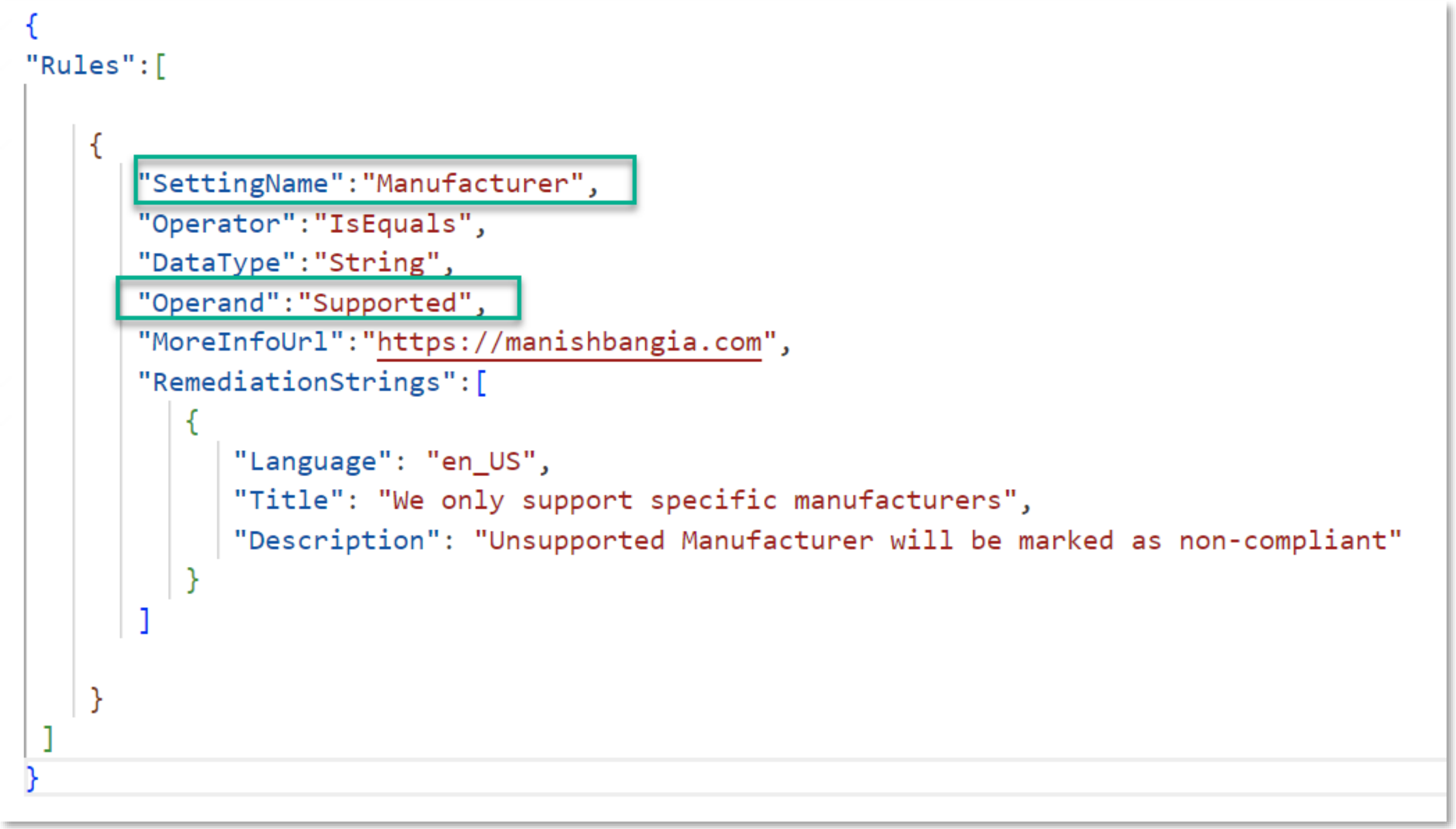
Notes:

- Manufacturer = Supported
- Converted to Json Format

wpninjas.au

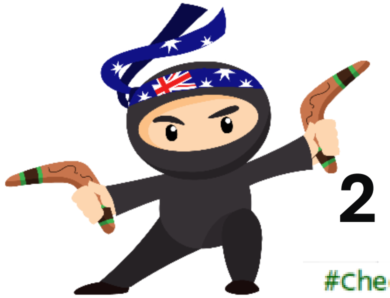
Compliance policy area – custom rules

JSON file



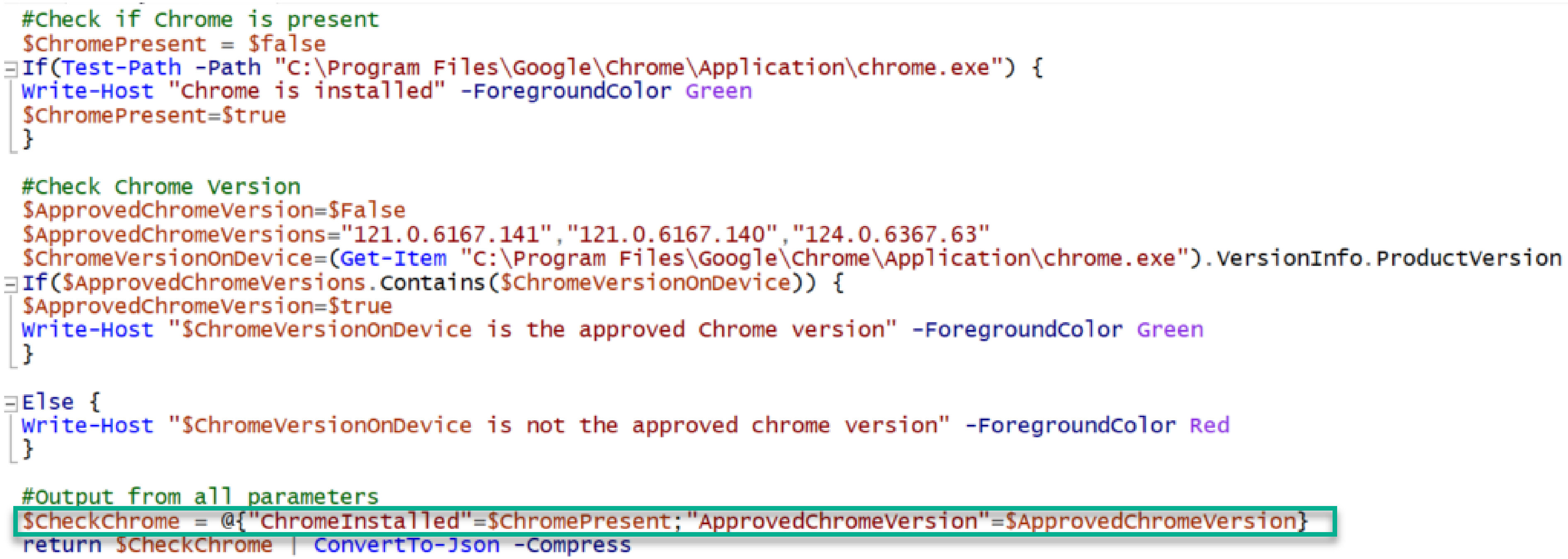
```
{
"Rules":[

    {
     "SettingName":"Manufacturer",
     "Operator":"IsEquals",
     "DataType":"String",
     "Operand":"Supported",
     "MoreInfoUrl":"https://manishbangia.com",
     "RemediationStrings":[
        {
           "Language": "en_US",
           "Title": "We only support specific manufacturers",
           "Description": "Unsupported Manufacturer will be marked as non-compliant"
        }
     ]

    }
 ]
}
```

Refer: https://learn.microsoft.com/en-us/mem/intune/protect/compliance-custom-json

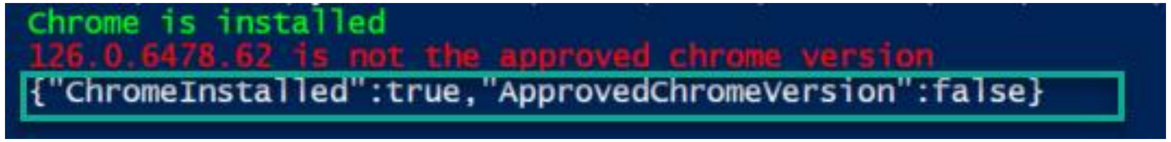


Compliance policy area – custom rules

2 rules – Chrome installed and check version



```
#Check if Chrome is present
$ChromePresent = $false
If(Test-Path -Path "C:\Program Files\Google\Chrome\Application\chrome.exe") {
Write-Host "Chrome is installed" -ForegroundColor Green
$ChromePresent=$true
}

#Check Chrome Version
$ApprovedChromeVersion=$False
$ApprovedChromeVersions="121.0.6167.141","121.0.6167.140","124.0.6367.63"
$ChromeVersionOnDevice=(Get-Item "C:\Program Files\Google\Chrome\Application\chrome.exe").VersionInfo.ProductVersion
If($ApprovedChromeVersions.Contains($ChromeVersionOnDevice)) {
$ApprovedChromeVersion=$true
Write-Host "$ChromeVersionOnDevice is the approved Chrome version" -ForegroundColor Green
}

Else {
Write-Host "$ChromeVersionOnDevice is not the approved chrome version" -ForegroundColor Red
}

#Output from all parameters
$CheckChrome = @{"ChromeInstalled"=$ChromePresent;"ApprovedChromeVersion"=$ApprovedChromeVersion}
return $CheckChrome | ConvertTo-Json -Compress
```



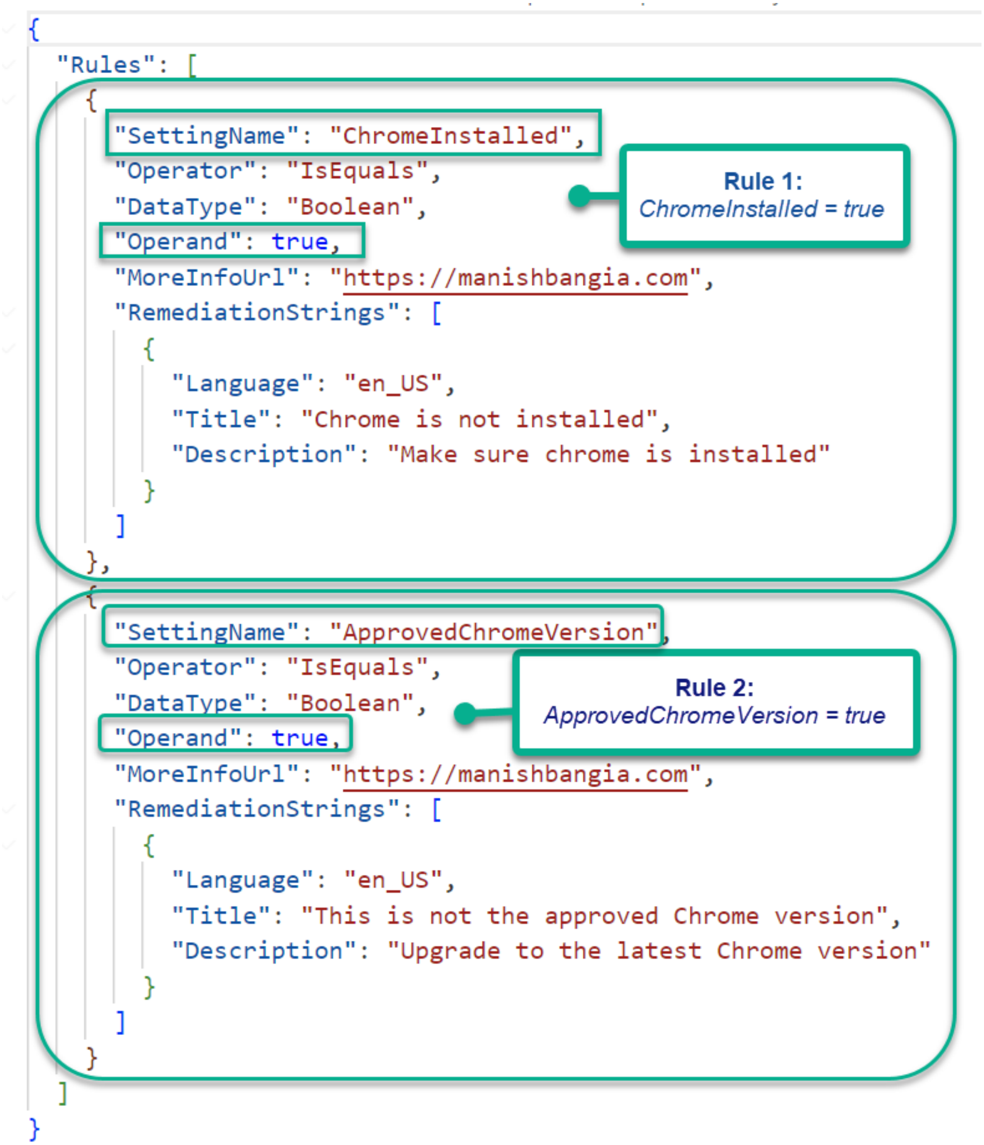
```
Chrome is installed
126.0.6478.62 is not the approved chrome version
{"ChromeInstalled":true,"ApprovedChromeVersion":false}
```

Notes:

- ChromeInstalled = true
- Approvedchromeversion = true
- Converted to Json Format

Compliance policy area – custom rules

JSON file – For Chrome detection



```
{
  "Rules": [
    {
      "SettingName": "ChromeInstalled",
      "Operator": "IsEquals",
      "DataType": "Boolean",
      "Operand": true,
      "MoreInfoUrl": "https://manishbangia.com",
      "RemediationStrings": [
        {
          "Language": "en_US",
          "Title": "Chrome is not installed",
          "Description": "Make sure chrome is installed"
        }
      ]
    },
    {
      "SettingName": "ApprovedChromeVersion",
      "Operator": "IsEquals",
      "DataType": "Boolean",
      "Operand": true,
      "MoreInfoUrl": "https://manishbangia.com",
      "RemediationStrings": [
        {
          "Language": "en_US",
          "Title": "This is not the approved Chrome version",
          "Description": "Upgrade to the latest Chrome version"
        }
      ]
    }
  ]
}
```

Rule 1:
ChromeInstalled = true

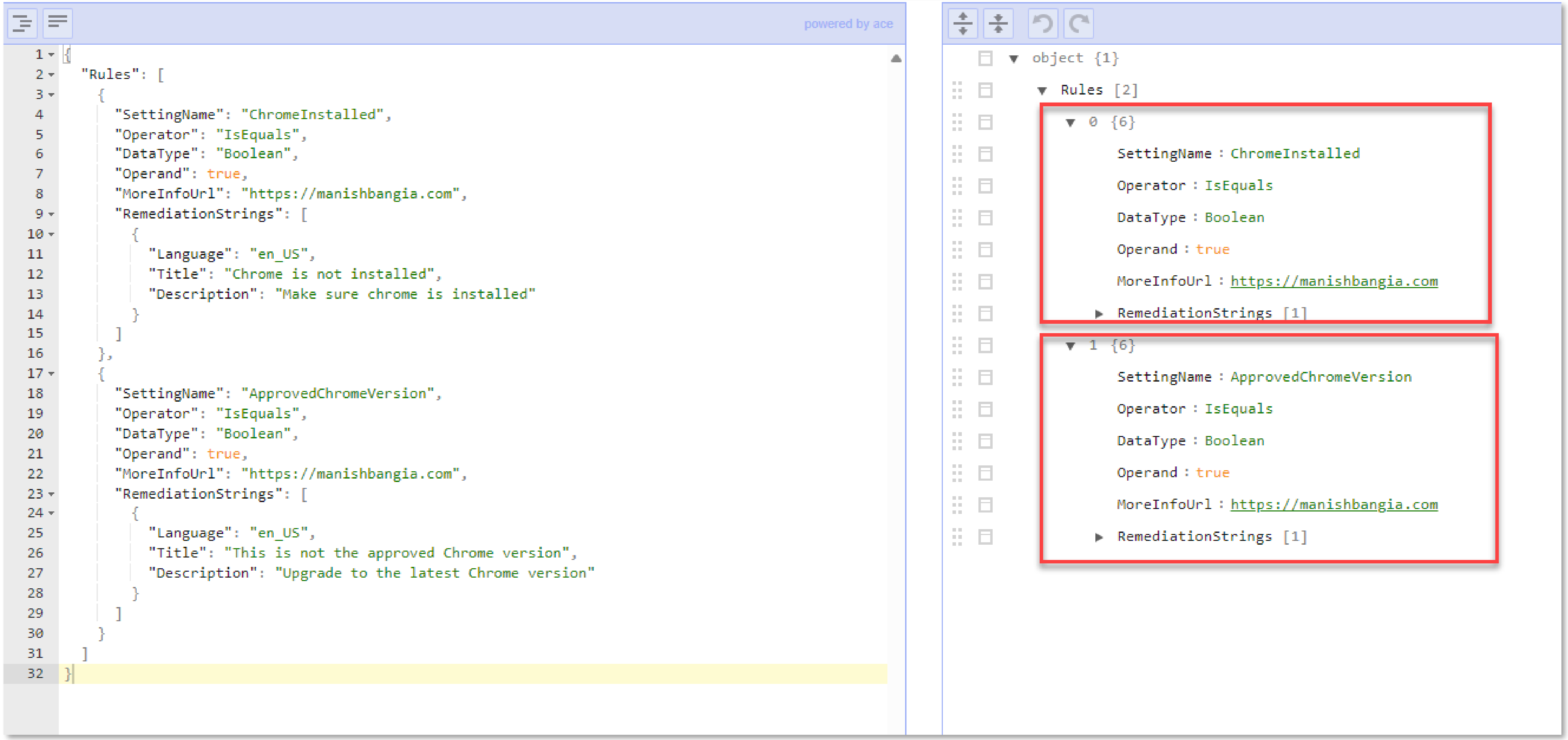
Rule 2:
ApprovedChromeVersion = true

JSON Viewer: https://jsonblob.com/

For more custom compliance policies check:
https://github/v-2maban

Compliance policy area – custom rules

JSON viewer – https://jsonblob.com



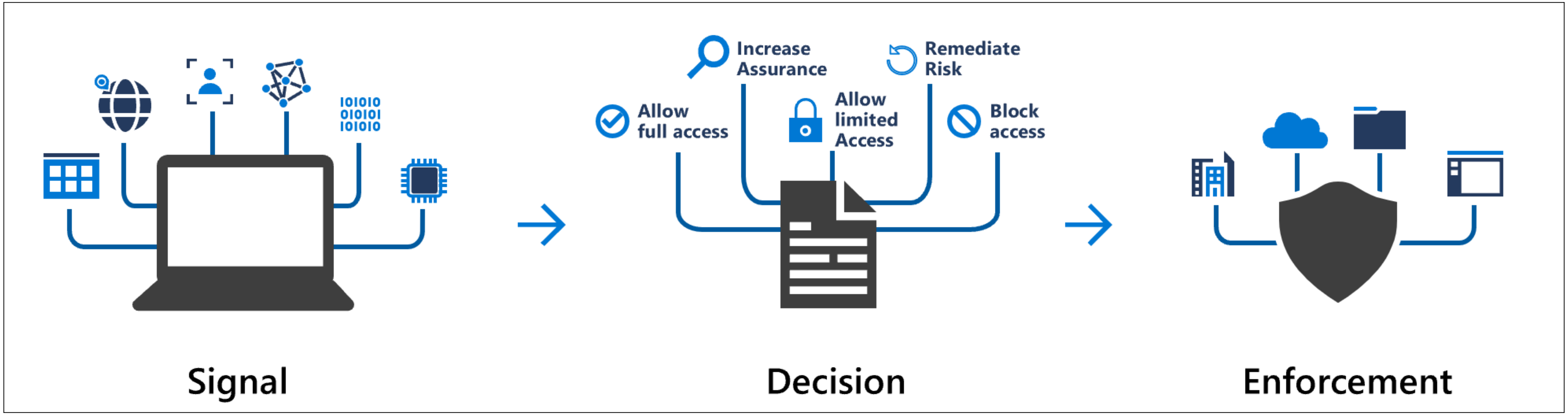
```
{
  "Rules": [
    {
      "SettingName": "ChromeInstalled",
      "Operator": "IsEquals",
      "DataType": "Boolean",
      "Operand": true,
      "MoreInfoUrl": "https://manishbangia.com",
      "RemediationStrings": [
        {
          "Language": "en_US",
          "Title": "Chrome is not installed",
          "Description": "Make sure chrome is installed"
        }
      ]
    },
    {
      "SettingName": "ApprovedChromeVersion",
      "Operator": "IsEquals",
      "DataType": "Boolean",
      "Operand": true,
      "MoreInfoUrl": "https://manishbangia.com",
      "RemediationStrings": [
        {
          "Language": "en_US",
          "Title": "This is not the approved Chrome version",
          "Description": "Upgrade to the latest Chrome version"
        }
      ]
    }
  ]
}
```

```
▼ object {1}
  ▼ Rules [2]
    ▼ 0 {6}
        SettingName : ChromeInstalled
        Operator : IsEquals
        DataType : Boolean
        Operand : true
        MoreInfoUrl : https://manishbangia.com
      ▶ RemediationStrings [1]
    ▼ 1 {6}
        SettingName : ApprovedChromeVersion
        Operator : IsEquals
        DataType : Boolean
        Operand : true
        MoreInfoUrl : https://manishbangia.com
      ▶ RemediationStrings [1]
```

Conditional access policies

What is Conditional access policies

- To secure the organizations network and its data.
- Helps aligning organizations with zero trust architecture.
- It is the capability built into Microsoft Entra (Requires Microsoft Entra ID P1 or P2).

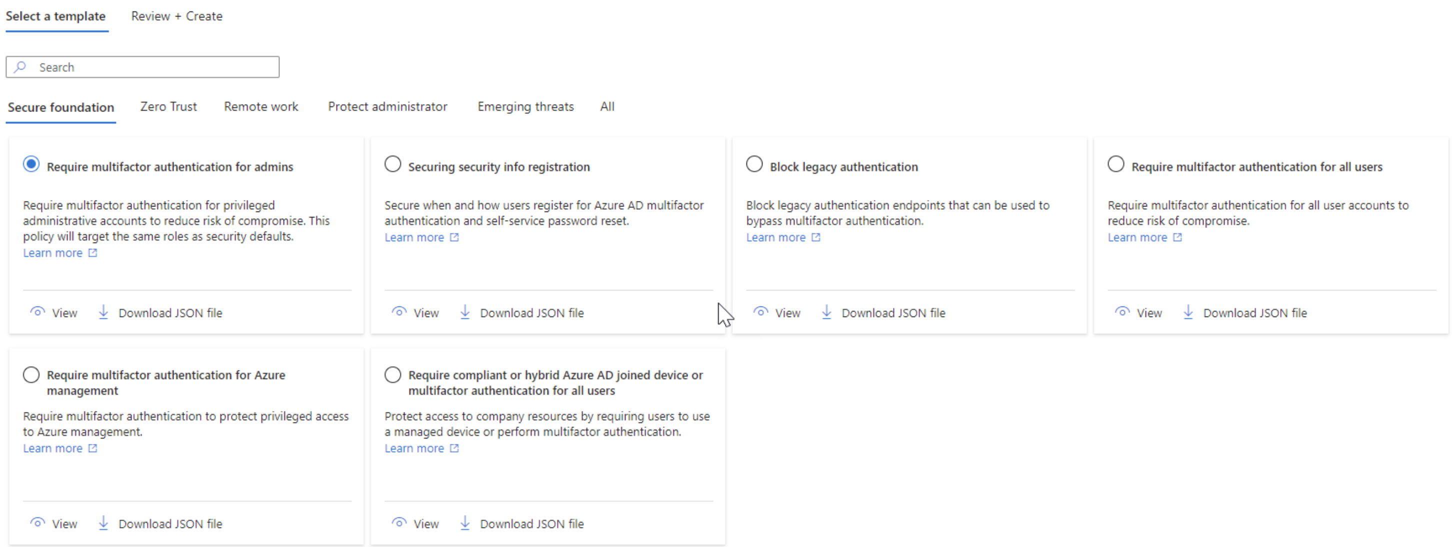


Conditional access policies

wpninjas.au

Exploring the CA policies

- Readily available policy templates such as:
  - Require multifactor authentication for all users
  - Block legacy authentication
  - Require compliant or Microsoft Entra hybrid joined device or MFA for all users
- Create the new policy from scratch.
- Test the policy via **Report-only** setting.



Select a template   Review + Create

Search

Secure foundation   Zero Trust   Remote work   Protect administrator   Emerging threats   All

● Require multifactor authentication for admins

Require multifactor authentication for privileged administrative accounts to reduce risk of compromise. This policy will target the same roles as security defaults.
Learn more

View   Download JSON file

○ Securing security info registration

Secure when and how users register for Azure AD multifactor authentication and self-service password reset.
Learn more

View   Download JSON file

○ Block legacy authentication

Block legacy authentication endpoints that can be used to bypass multifactor authentication.
Learn more

View   Download JSON file

○ Require multifactor authentication for all users

Require multifactor authentication for all user accounts to reduce risk of compromise.
Learn more

View   Download JSON file

○ Require multifactor authentication for Azure management

Require multifactor authentication to protect privileged access to Azure management.
Learn more

View   Download JSON file

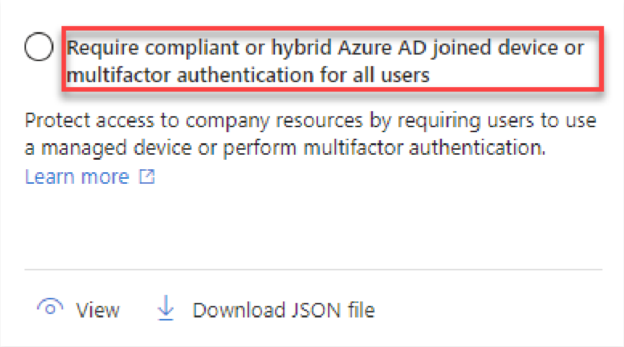
○ Require compliant or hybrid Azure AD joined device or multifactor authentication for all users

Protect access to company resources by requiring users to use a managed device or perform multifactor authentication.
Learn more

View   Download JSON file

Conditional access policies

- Create policy using from scratch or use template



○ Require compliant or hybrid Azure AD joined device or multifactor authentication for all users

Protect access to company resources by requiring users to use a managed device or perform multifactor authentication.
Learn more

- Don’t get locked out because of wrong CA policy implemented
  - Target on few test users only.
  - Exclude yourself (or others) from the policy.
  - Target policy using report-only mode

Demo

1. Create Compliance policies

2. Create conditional access policy

- Block O365 app if device is not compliant

3. Verify Compliance status and Conditional policy status

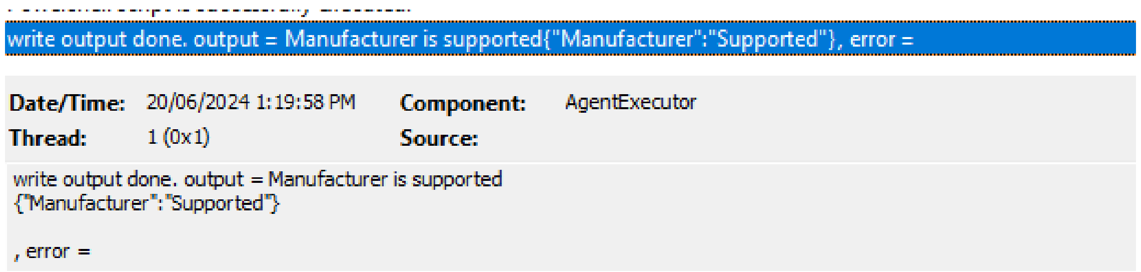
Compliance policy verification

- **Monitor via Intune admin center**
- **Via log files on device**

  Log files location: c:\programdata\Microsoft\IntuneManagementExtension\Logs

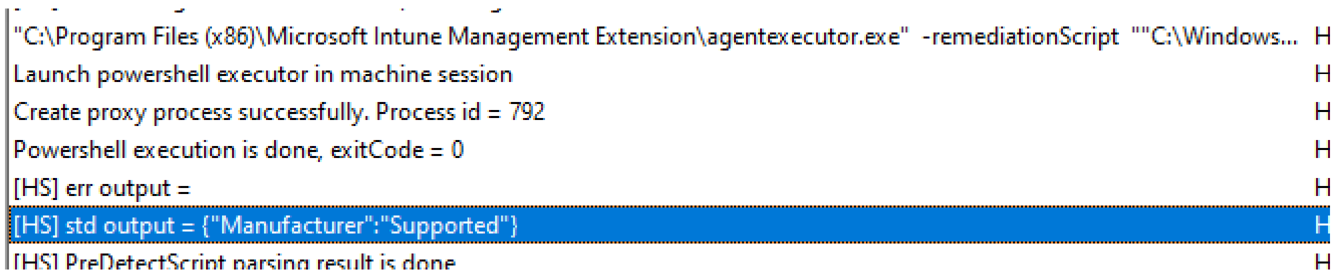
- **Log files:**

  AgentExecutor.log



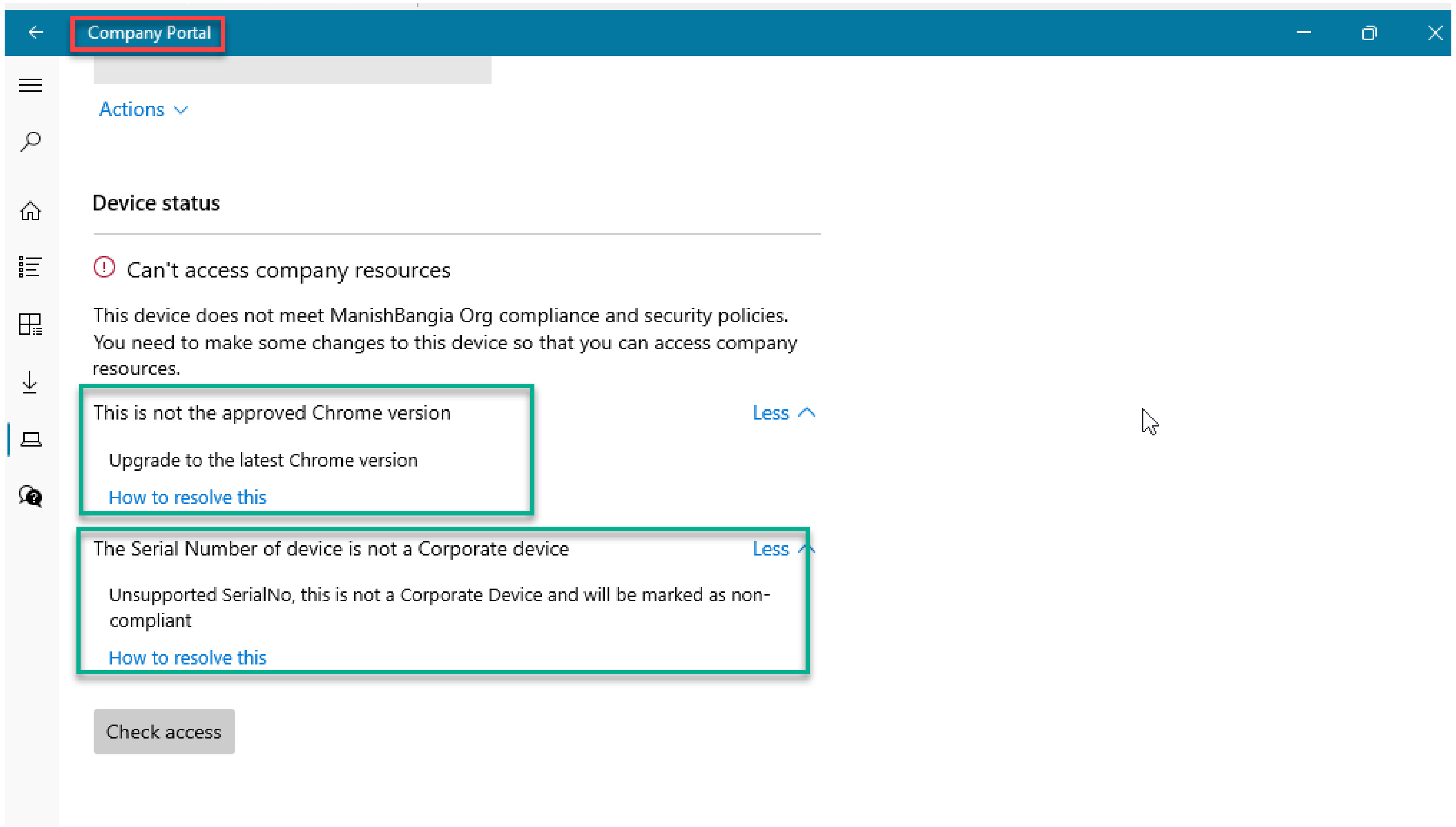
```
write output done. output = Manufacturer is supported{"Manufacturer":"Supported"}, error =

Date/Time:  20/06/2024 1:19:58 PM      Component:  AgentExecutor
Thread:     1 (0x1)                    Source:

write output done. output = Manufacturer is supported
{"Manufacturer":"Supported"}

, error =
```

  HealthScripts.log



```
"C:\Program Files (x86)\Microsoft Intune Management Extension\agentexecutor.exe"  -remediationScript  ""C:\Windows...  H
Launch powershell executor in machine session                                                                          H
Create proxy process successfully. Process id = 792                                                                    H
Powershell execution is done, exitCode = 0                                                                             H
[HS] err output =                                                                                                      H
[HS] std output = {"Manufacturer":"Supported"}                                                                         H
[HS] PreDetectScript parsing result is done                                                                            H
```

Compliance policy verification – Company Portal



Device status

Can't access company resources

This device does not meet ManishBangia Org compliance and security policies. You need to make some changes to this device so that you can access company resources.

This is not the approved Chrome version

Less

Upgrade to the latest Chrome version

How to resolve this

The Serial Number of device is not a Corporate device

Less

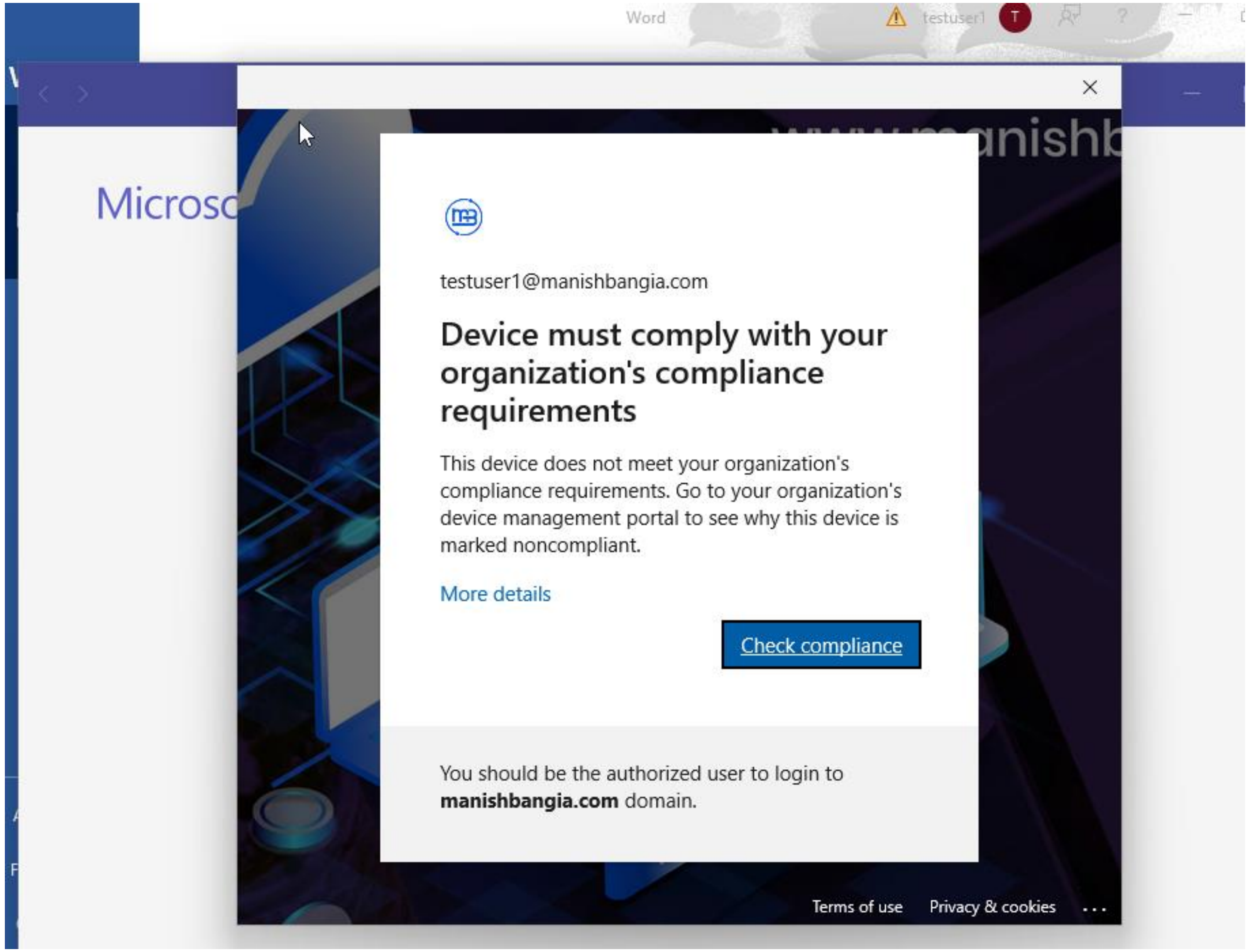
Unsupported SerialNo, this is not a Corporate Device and will be marked as non-compliant

How to resolve this

Check access

wpninjas.au

Conditional access policy verification



testuser1@manishbangia.com

Device must comply with your organization's compliance requirements

This device does not meet your organization's compliance requirements. Go to your organization's device management portal to see why this device is marked noncompliant.

You should be the authorized user to login to **manishbangia.com** domain.

Thank You