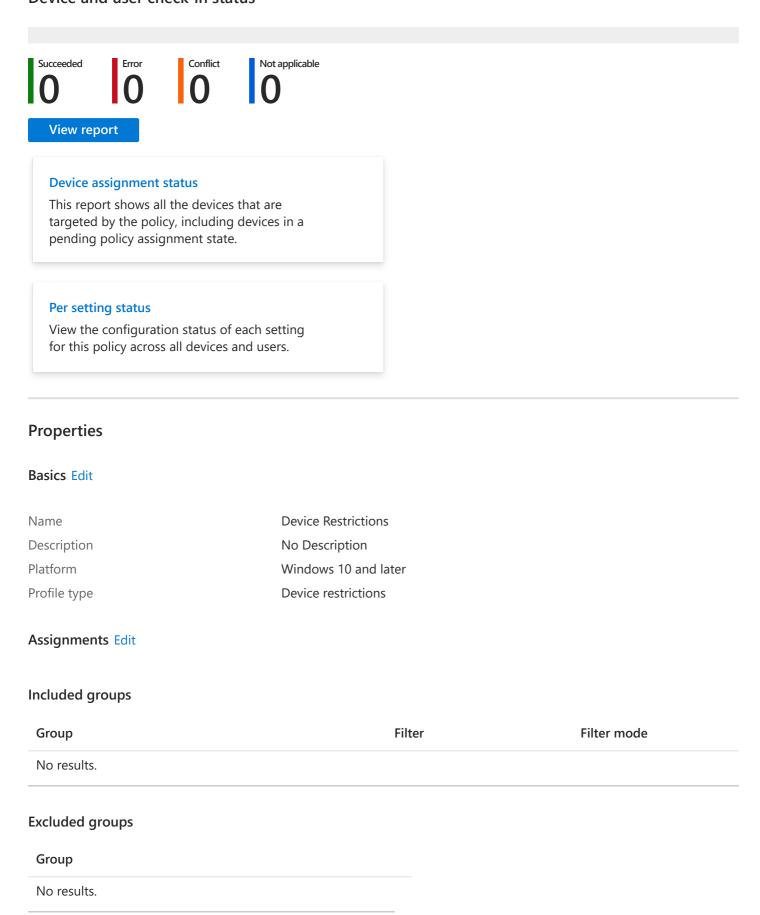


Device and user check-in status



Scope tags Edit

Default

Configuration settings Edit

∧ App Store

Trusted app installation Allow

Developer unlock Allow

Shared user app data Allow

Game DVR (desktop only) Block

Apps from store only Prefer Store

Cellular and connectivity

Automatically connect to Wi-Fi hotspots Block Wi-Fi scan interval (mobile only) 120

General

Screen capture (mobile only)

Phone reset

AntiTheft mode (mobile only)

Block

Cortana

Block

Device name modification (mobile only)

Block

SIM card error dialog (mobile only)

Block

Ink Workspace Disabled on lock screen

Autopilot Reset Allow
Direct Memory Access Block
End processes from Task Manager Block

Locked Screen Experience

Action center notifications (mobile only)

Cortana on locked screen (Desktop only)

Screen timeout (mobile only)

Voice activate apps from locked screen

Disabled

Password

Password Require

Required password type Alphanumeric

Password complexity Numbers and lowercase letters required

Minimum password length 8

Moderate

 $https://intune.microsoft.com/\#view/Microsoft_Intune_DeviceSettings/PolicySummaryReportBlade/policyId/2e66c2c5-fe07-44c1-852a-24554c531f...$

Safe Search (mobile only)

∧ Start

Recently opened items in Jump Lists **Block** Hibernate **Block** Documents on Start Show Downloads on Start Show File Explorer on Start Show HomeGroup on Start Hide Music on Start Show Network on Start Show Personal folder on Start Show Pictures on Start Show Show Settings on Start Videos on Start Hide

Microsoft Defender SmartScreen

Malicious site access

Unverified file download

Block

Block

Windows Spotlight

Windows Tips

Windows Spotlight in action center

Windows welcome experience

Apps suggestions in Ink workspace

Block

Block

Block

Microsoft Defender Antivirus

Real-time monitoring Enable Enable Behavior monitoring Network Inspection System (NIS) Enable Scan all downloads Enable Configure low CPU priority for scheduled Enabled Scan scripts loaded in Microsoft web Enable browsers Security intelligence update interval (in 8 hours) Days before deleting quarantined 15 malware CPU usage limit during a scan 10 Scan archive file Enable Scan incoming mail messages Enable

Scan removable drives during a full scan

Enable

Scan mapped network drives during a full Enable

scan

Cloud-delivered protection Enable

File Blocking Level High

Time extension for file scanning by the

cloud

10

Prompt users before sample submission
Always prompt

Time to perform a daily quick scan

Type of system scan to perform

Full scan

Day scheduled

Monday

Time scheduled

11 PM

Detect potentially unwanted applications

On Access Protection

Actions on detected malware threats

Enable

Low severity Quarantine

Moderate severity Quarantine

High severity Block

Severe severity Block

Power Settings

Battery level to turn Energy Saver on 35 Battery level to turn Energy Saver on 70 Lid close (mobile only) Sleep Lid close (mobile only) Sleep Power button Shutdown Power button Shutdown Sleep Sleep button Sleep button Sleep Hybrid sleep Disable Hybrid sleep Disable

Applicability Rules Edit