Indiana VPN Posture Requirements and Technical Details

Anti-Malware/Anti-Virus

IOT is not specifying any specific AM/Virus software, only that it is there and up to date, and we can read the settings. The functionality is built into the posture assessment, so no custom policies are required. A list of compatible AM software may be found here:

https://www.in.gov/iot/nts/Shared Documents/VPN/Posture/compatibility.pdf

The columns for "Definition State Check" and "Application Running Check" must be "yes".

Device Lock Settings

Devices must be set to lock at 15 minutes of idle time and require password immediately to unlock

For Windows

IOT is checking for these values in registry:

Preferred Method: Inactivity timeout for locking computer

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System

Inactivitytimeoutsecs <= 900 (this is the Decimal setting. The Hexidecimal setting is 384)

-OR-

Legacy Method: Inactivity timeout to enable secure screen saver

The settings below which could be found in either of these key locations:

HKCU\Control Panel\Desktop
HKCU\Software\Policies\Microsoft\Windows\Control Panel\Desktop

“screensaveactive” = 1
“screensaverissecure” = 1
“screensavetimeout” <= 900

-OR-

Emerging Method: Inactivity Timeout for locking computer managed in InTune

HKLM\SOFTWARE\Microsoft\PolicyManager\current\Device\DeviceLock

MaxInactivityTimeDeviceLock <= 15

Continued on next page

For Macbook

Ivanti (State MDM) places the settings in /Library/Managed Preferences/com.apple.screensaver.plist. IOT is checking the following in that property list:

“askForPassword” key exists
“askForPasswordDelay” = 0
“idleTime” <= 900 OR “loginWindowIdleTime” <= 900

We are also accepting the following combination of settings:

/Library/Managed Preferences/com.apple.screensaver.plist

“askForPassword” key exists
“askForPasswordDelay” = 0

AND

/Library/Managed Preferences/com.apple.screensaver.user.plist with “idleTime” <= 900

Apple buries the settings in the keychain if the device is not managed by MDM, so we are unable to read the settings.

If a user using an MDM that places the settings in another location or words them differently, we can work with them to accommodate if we can read the settings.

Operating System

IOT is accepting Windows versions higher than build number 19041, based on the link and the versions currently use in the IOT managed environment.

https://learn.microsoft.com/en-us/windows/release-health/release-information#windows-10-release-history

The settings are found in the registry at “SOFTWARE\Microsoft\Windows NT\CurrentVersion”, key “CurrentBuildNumber” >= 19041

IOT is accepting MacOS greater than 13.x.

The settings are found in “Library/Preferences/com.apple.updatesettings.plist”, key “UpdateSettingsRunStamp/majorVersion” >= 13

Continued on next page

Internet Connect Sharing

Internet Connection Sharing must be disabled

For Windows, IOT is checking for the “SharedAccess” application “Not Running”. The application will not run until enabled for the first time. Once the application is running, it cannot be terminated without stopping the “Internet Connection Sharing” service and setting its Startup Type to “Disabled”

For Mac, IOT is checking that “Library/Preferences/SystemConfiguration/com.apple.nat.plist” does not exist. If “Library/Preferences/SystemConfiguration/com.apple.nat.plist” does exist, IOT checks key “NAT/Enabled” = 0.

Firewall

The device firewall must be enabled and active. The functionality is built into the posture assessment, so no custom policies are required.

Mobile Device Management

IOT is not specifying any specific MDM. The requirement for MDM is for the desktop lock set to 15 minutes with password required immediately and that we can read the settings. See **Device Lock Requirements** for technical details.

Caveats

Users that connect to VPN using a “Home” version of Windows will no longer be able to connect to VPN

Users that connect to VPN using a version of Linux will no longer be able to connect to VPN

Users that connect to VPN using an unmanaged Mac device will no longer be able to connect to VPN

Updated September 9, 2024