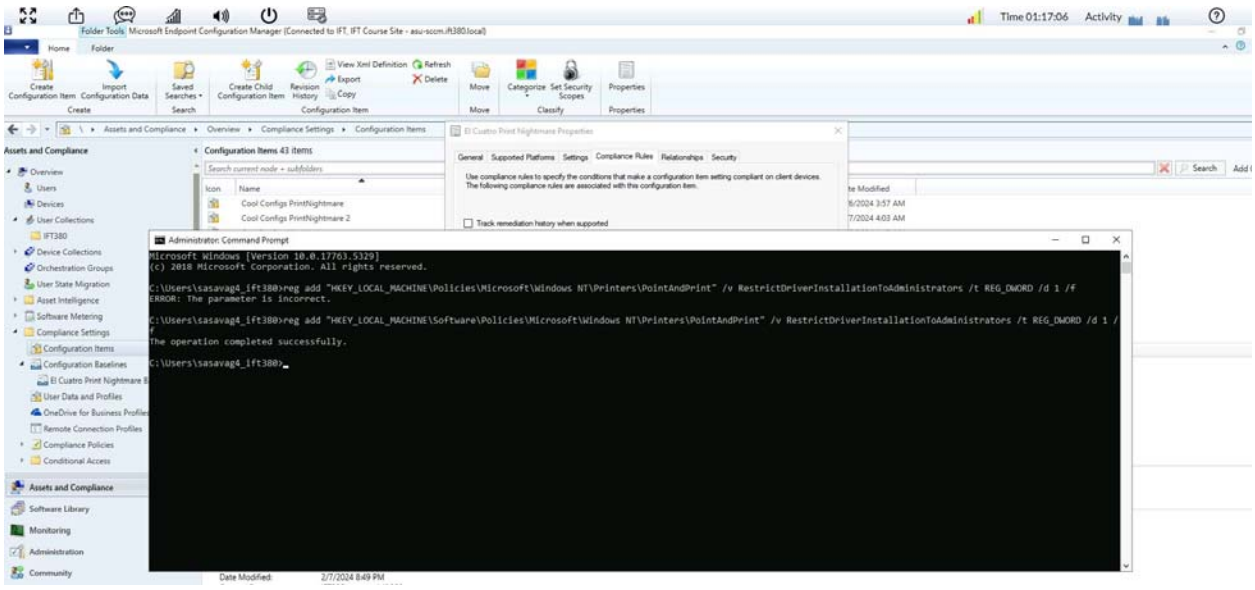
2/7/2024
Group: El Cuatro
Steven Rojas, Scott Deveraux,
Yengkong Sayaovong, Scott Savage

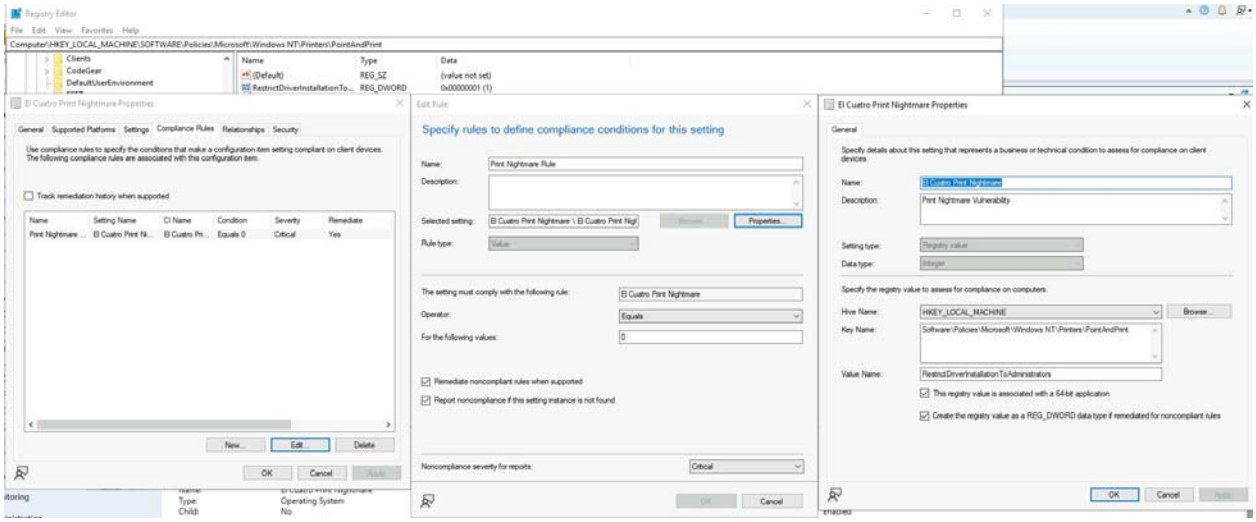
Group Lab 2 - Configuration Baseline

For Print Nightmare, Scott Deveraux and Scott Savage teamed up with Scott Savage handling the configuration item setup. After Initially failing several attempts at the configuration item for print nightmare both Scott D. and Scott S. began troubleshooting the Configuration Item and the configuration Baseline.

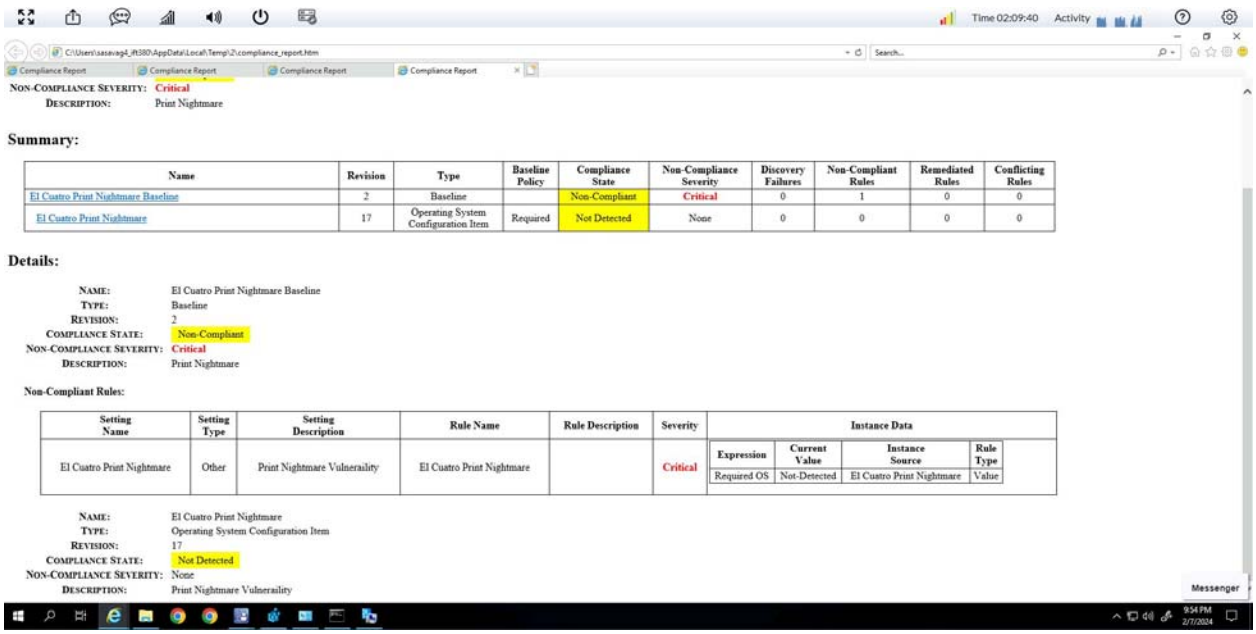
After reading a class announcement and conversing with the professor Scott S. confirmed the path was not correct. It was wrong and incomplete. I found a CMD line in the resources that will actually create the correct path , key and value rather than doing it in the reg edit GUI.



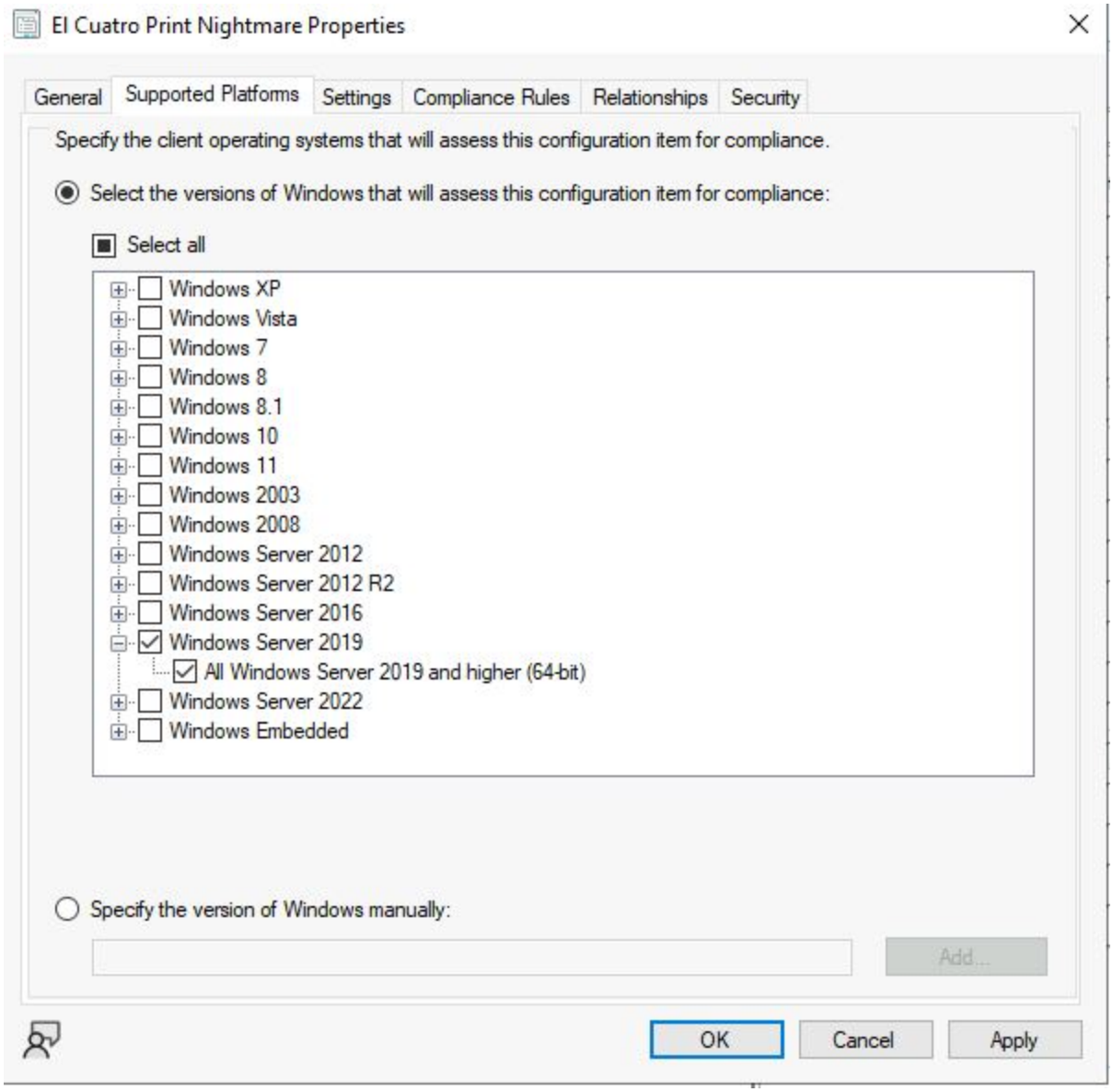
After that I was able to review my path and configuration setup:



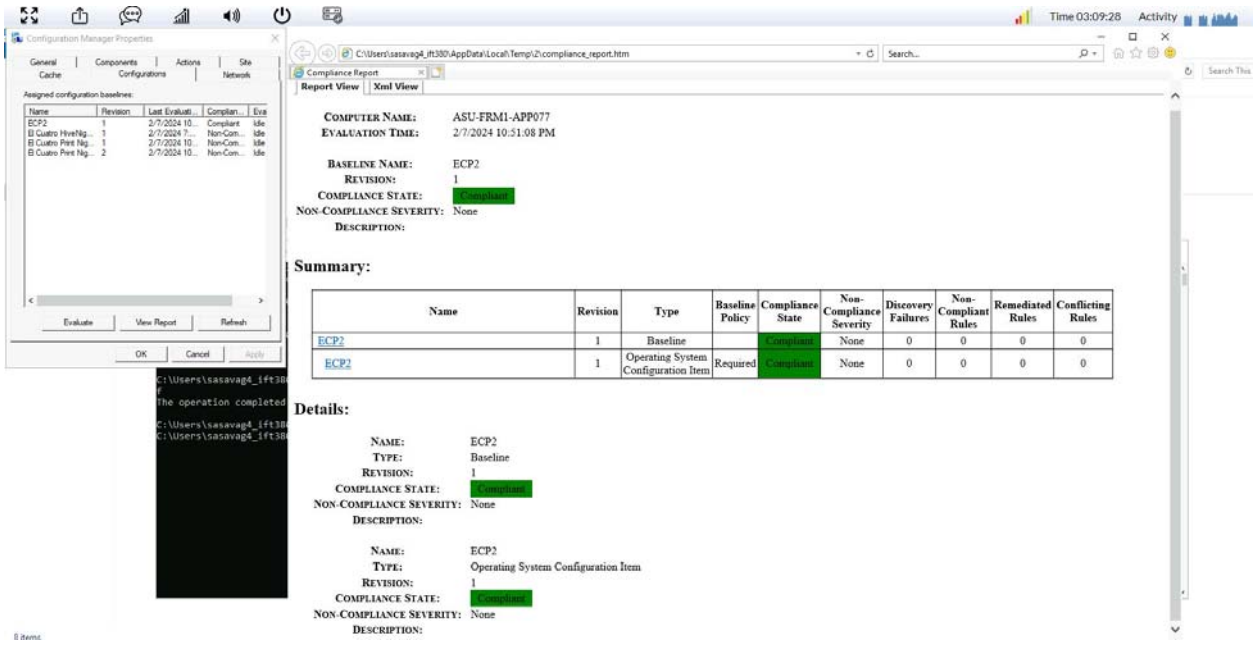
However when I evaluated these changes I still got non compliant, in fact it was detecting at all.



So that's when I realized I had the wrong OS selected and changed it from windows 10 to windows server 19:

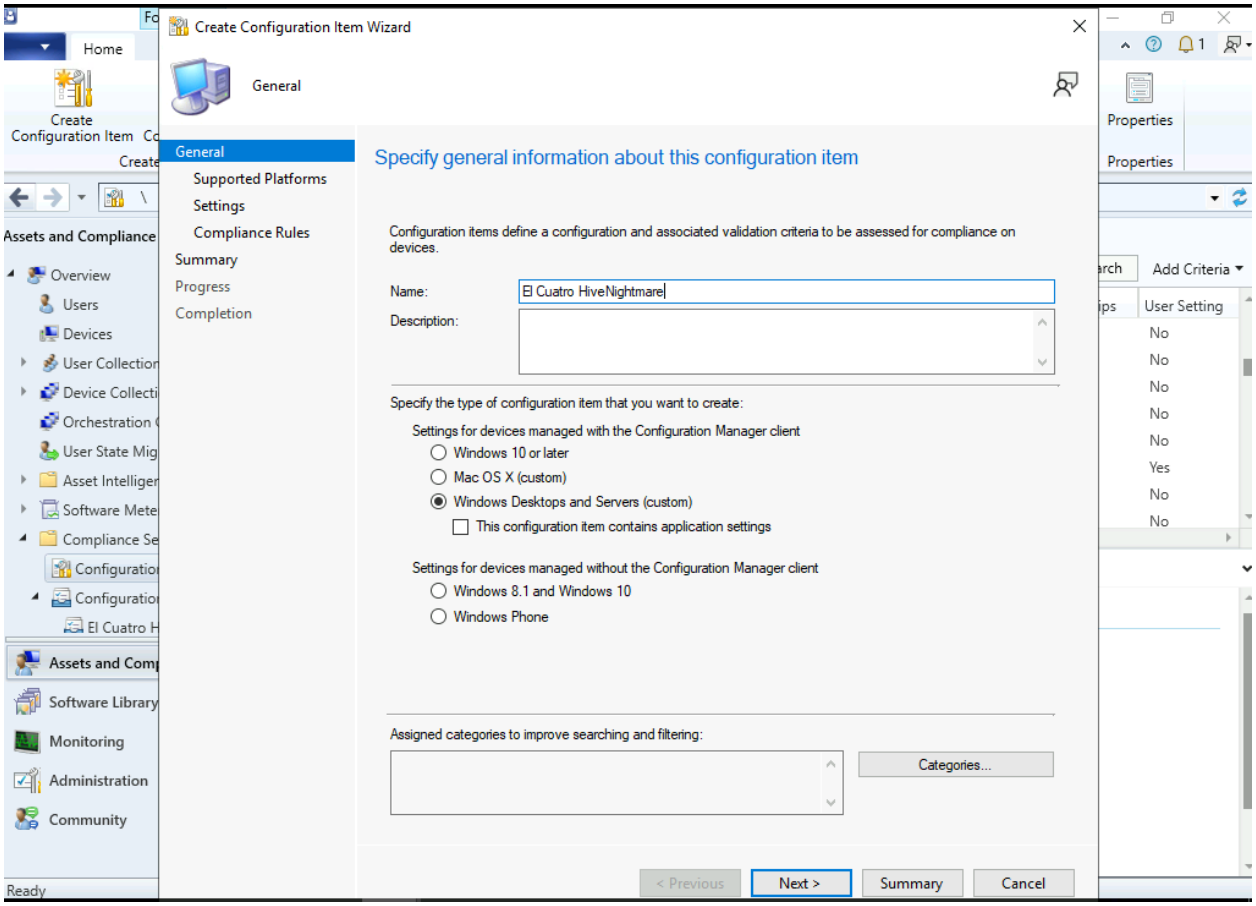


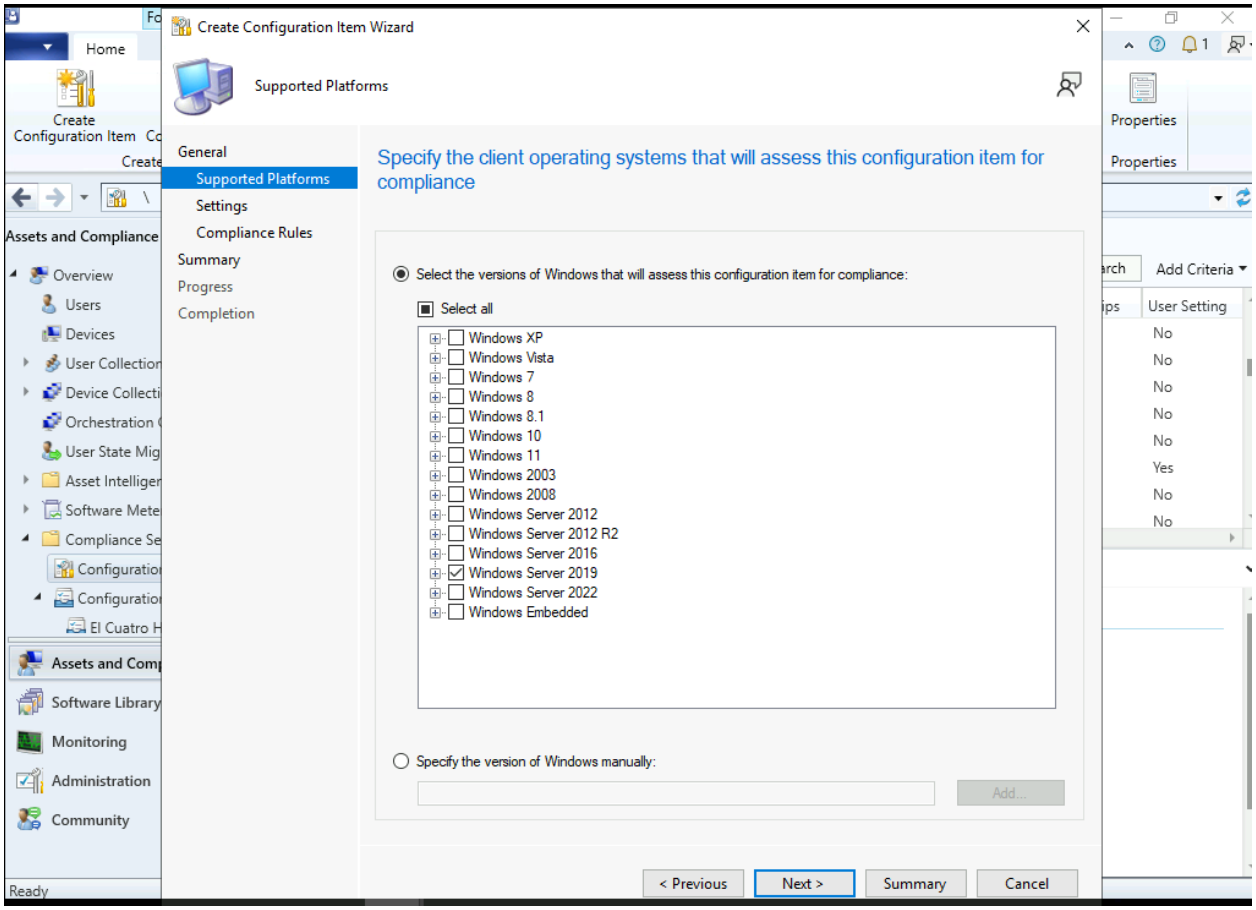
From here I was able to re-evaluate and get a compliant report:

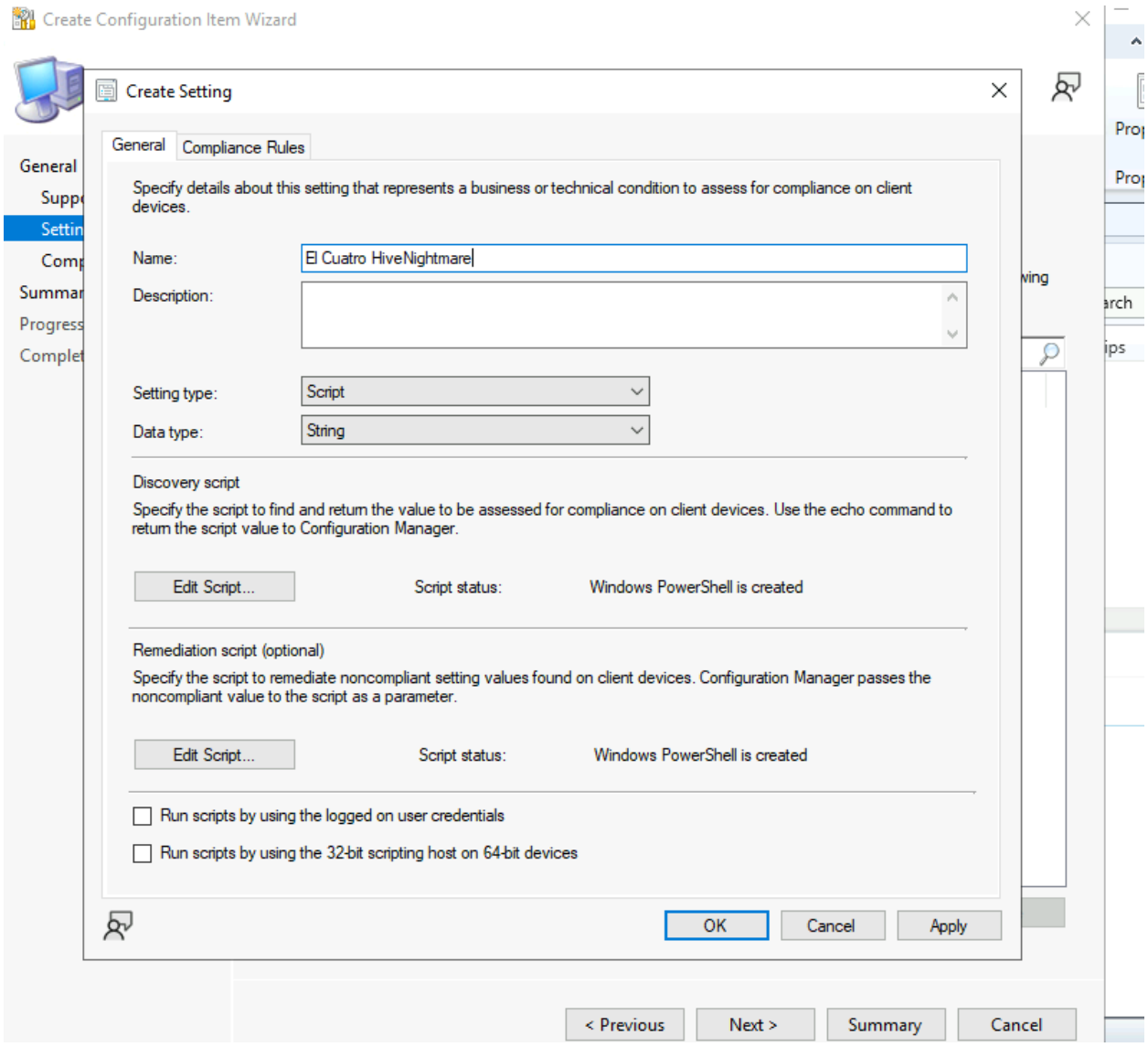


HiveNightmare:

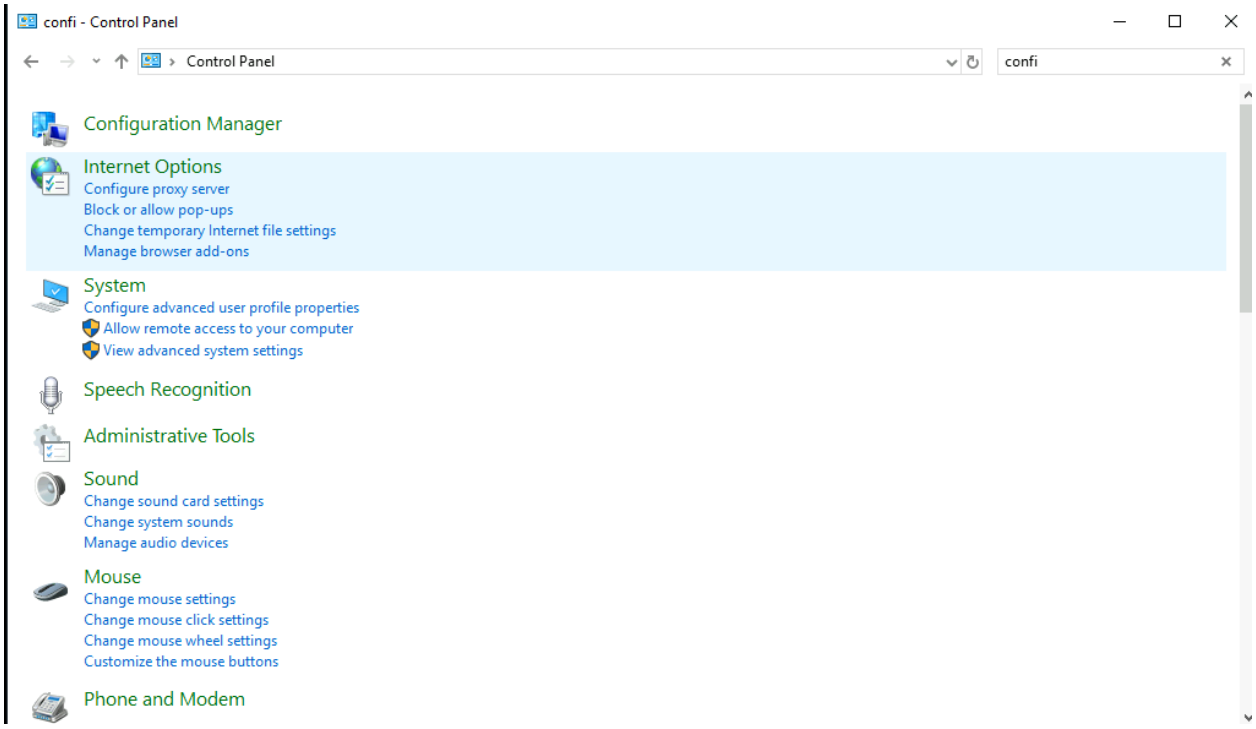
Yengkong went to create configuration items and went through the steps to create the HiveNightmare. We had issues doing HiveNightmare at first as we followed the video that was provided on the module and selected Windows 10. Scott S, Scott D and Steven helped with the troubleshooting and revising of the hive from Windows 10 to Windows 19 in order to get the report to be compliant.

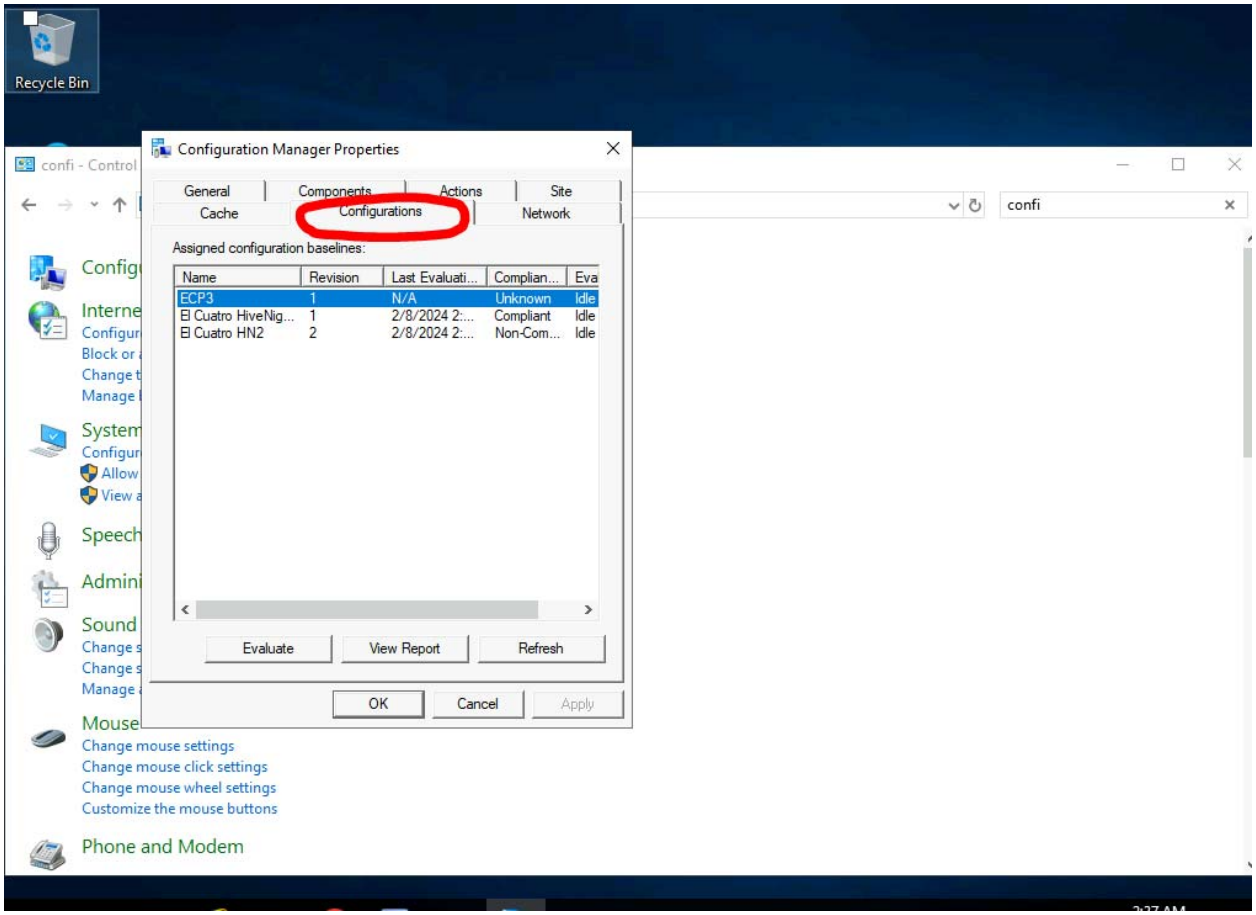

Create Configuration Item Wizard
General
General
Supported Platforms
Settings
Compliance Rules
Summary
Progress
Completion
Specify general information about this configuration item
Configuration items define a configuration and associated validation criteria to be assessed for compliance on devices.
Name:
El Cuatro HiveNightmare
Description:
Specify the type of configuration item that you want to create:
Settings for devices managed with the Configuration Manager client
Windows 10 or later
Mac OS X (custom)
Windows Desktops and Servers (custom)
This configuration item contains application settings
Settings for devices managed without the Configuration Manager client
Windows 8.1 and Windows 10
Windows Phone
Assigned categories to improve searching and filtering:
Categories...
< Previous
Next >
Summary
Cancel
Home
Create Configuration Item
Properties
Assets and Compliance
Overview
Users
Devices
Add Criteria
User Setting
Software Library
Monitoring
Administration
Community
Ready


Create Configuration Item Wizard
Supported Platforms
General
Supported Platforms
Settings
Compliance Rules
Summary
Progress
Completion
Specify the client operating systems that will assess this configuration item for compliance
Select the versions of Windows that will assess this configuration item for compliance:
Select all
Windows XP
Windows Vista
Windows 7
Windows 8
Windows 8.1
Windows 10
Windows 11
Windows 2003
Windows 2008
Windows Server 2012
Windows Server 2012 R2
Windows Server 2016
Windows Server 2019
Windows Server 2022
Windows Embedded
Specify the version of Windows manually:
Add...
< Previous
Next >
Summary
Cancel
Home
Create Configuration Item
Properties
Assets and Compliance
Overview
Users
Devices
Software Library
Monitoring
Administration
Community
Ready
Add Criteria
User Setting

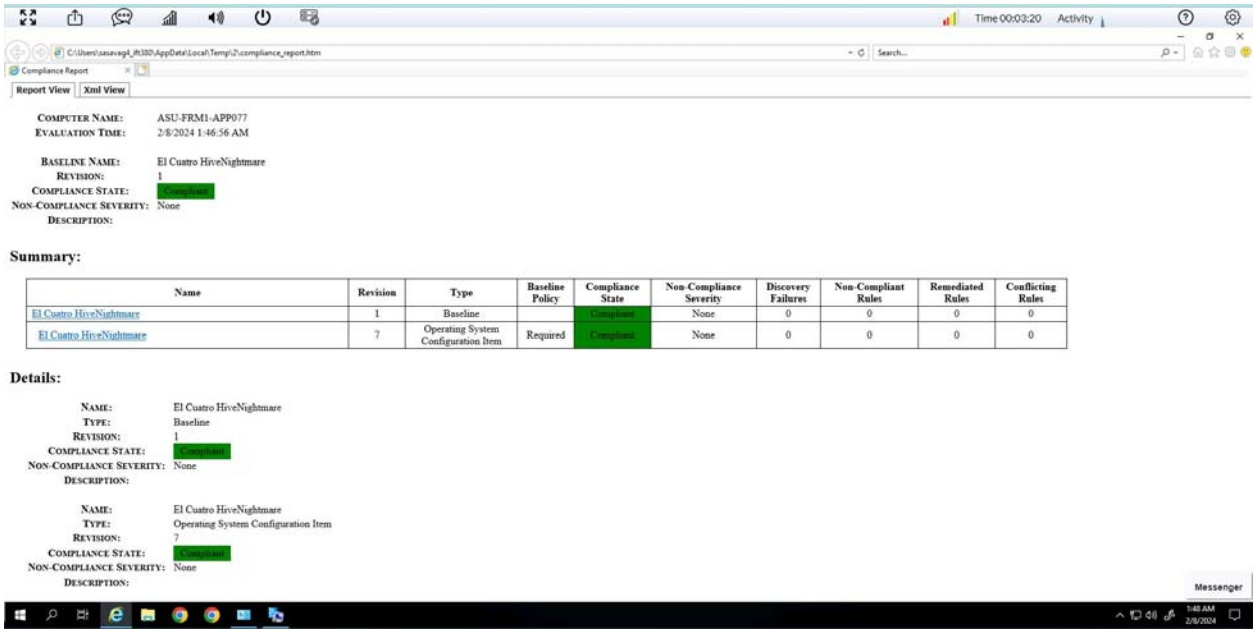


To test the HiveNightmare, we went into the control panel and under the configuration manager. On the configuration manager properties we went under the configurations tab and selected the report that we wanted and clicked evaluate then view report to see if we got compliant or non-compliant.


confi - Control Panel
Control Panel
confi
Configuration Manager
Internet Options
Configure proxy server
Block or allow pop-ups
Change temporary Internet file settings
Manage browser add-ons
System
Configure advanced user profile properties
Allow remote access to your computer
View advanced system settings
Speech Recognition
Administrative Tools
Sound
Change sound card settings
Change system sounds
Manage audio devices
Mouse
Change mouse settings
Change mouse click settings
Change mouse wheel settings
Customize the mouse buttons
Phone and Modem


Recycle Bin
Configuration Manager Properties
General
Components
Actions
Site
Cache
Configurations
Network
Assigned configuration baselines:
Name
Revision
Last Evaluati...
Complian...
Eva
ECP3
1
N/A
Unknown
Idle
Cuatro HiveNig...
1
2/8/2024 2:...
Compliant
Idle
Cuatro HN2
2
2/8/2024 2:...
Non-Com...
Idle
Evaluate
View Report
Refresh
OK
Cancel
Apply
confi
Change mouse settings
Change mouse click settings
Change mouse wheel settings
Customize the mouse buttons
Phone and Modem

After some troubleshooting we were able to evaluate and have it return compliant:



Compliance Report

Report View | Xml View

COMPUTER NAME: ASU-FRM1-APP077
EVALUATION TIME: 2/8/2024 1:46:56 AM

BASELINE NAME: El Cuatro HiveNightmare
REVISION: 1
COMPLIANCE STATE: Compliant
NON-COMPLIANCE SEVERITY: None
DESCRIPTION:

Summary:

Name	Revision	Type	Baseline Policy	Compliance State	Non-Compliance Severity	Discovery Failures	Non-Compliant Rules	Remediated Rules	Conflicting Rules
El Cuatro HiveNightmare	1	Baseline		Compliant	None	0	0	0	0
El Cuatro HiveNightmare	7	Operating System Configuration Item	Required	Compliant	None	0	0	0	0

Details:

NAME: El Cuatro HiveNightmare
TYPE: Baseline
REVISION: 1
COMPLIANCE STATE: Compliant
NON-COMPLIANCE SEVERITY: None
DESCRIPTION:

NAME: El Cuatro HiveNightmare
TYPE: Operating System Configuration Item
REVISION: 7
COMPLIANCE STATE: Compliant
NON-COMPLIANCE SEVERITY: None
DESCRIPTION:

Work detail Summary:

Scott Savage: Planning, Research, Print Nightmare Configuration Item, Print Nightmare Baseline, testing and writeup

Yengkong Sayaovong: Planning, Research, Hive Nightmare Configuration Item, Hive Nightmare Baseline, testing and writeup

Steven Rojas: Planning, Research, Hive Nightmare detection Script, Hive Nightmare remediation Script and testing

Scott Deveraux: Planning, Research, Print Nightmare Configuration Item, Print Nightmare Baseline, testing