

## **Configuration Baseline**

Alex Batker

## PrintNightmare

Create a new Configuration item named 'CABB PrintNightmare'

The screenshot shows the 'Create Configuration Item Wizard' dialog box, General tab. The wizard is titled 'Create Configuration Item Wizard' and has a 'General' tab selected. The left sidebar shows the progression: General, Supported Platforms, Settings, Compliance Rules, Summary, Progress, and Completion. The main area is titled 'Specify general information about this configuration item'. It contains a 'Name' field with the text 'CABB PrintNightmare' and a 'Description' field. Below these fields, there is a section titled 'Specify the type of configuration item that you want to create:'. It has two main sections: 'Settings for devices managed with the Configuration Manager client' and 'Settings for devices managed without the Configuration Manager client'. The first section has three radio buttons: 'Windows 10 or later', 'Mac OS X (custom)', and 'Windows Desktops and Servers (custom)'. The second section has two radio buttons: 'Windows 8.1 and Windows 10' and 'Windows Phone'. At the bottom, there is a section titled 'Assigned categories to improve searching and filtering:' with a list box and a 'Categories...' button. The 'Next >' button is highlighted.

Create Configuration Item Wizard

General

Specify general information about this configuration item

Configuration items define a configuration and associated validation criteria to be assessed for compliance on devices.

Name: CABB PrintNightmare

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

Checking if point and print registry exists in Registry Editor:

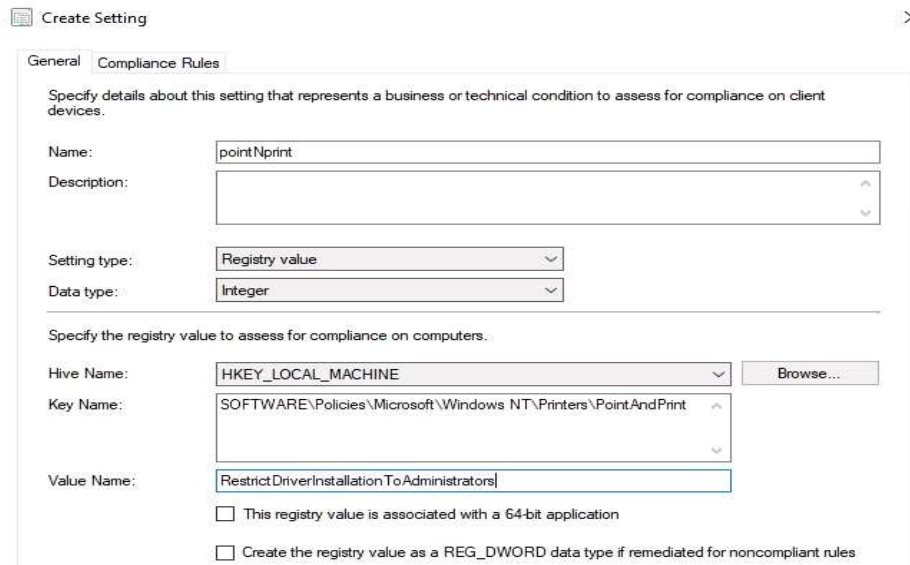
Here I can verify that this registry key(SOFTWARE\Policies\Microsoft\Windows NT\Printers\PointAndPoint) does not exist on my windows system.

The screenshot shows the Windows Registry Editor. The left pane displays the tree structure of the registry. The path 'Computer\HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT' is selected. The right pane shows the data for the selected path. There is one value named '(Default)' of type 'REG\_SZ' with the data '(value not set)'.

Name	Type	Data
(Default)	REG_SZ	(value not set)

## Configuring key settings:

Key Name: SOFTWARE\Policies\Microsoft\Windows NT\Printers\PointAndPrint



The 'Create Setting' dialog box is shown with the 'General' tab selected. It contains fields for Name, Description, Setting type, Data type, Hive Name, Key Name, and Value Name. The 'Compliance Rules' tab is also visible.

**Create Setting**

General Compliance Rules

Specify details about this setting that represents a business or technical condition to assess for compliance on client devices.

Name: pointNprint

Description:

Setting type: Registry value

Data type: Integer

Specify the registry value to assess for compliance on computers.

Hive Name: HKEY\_LOCAL\_MACHINE

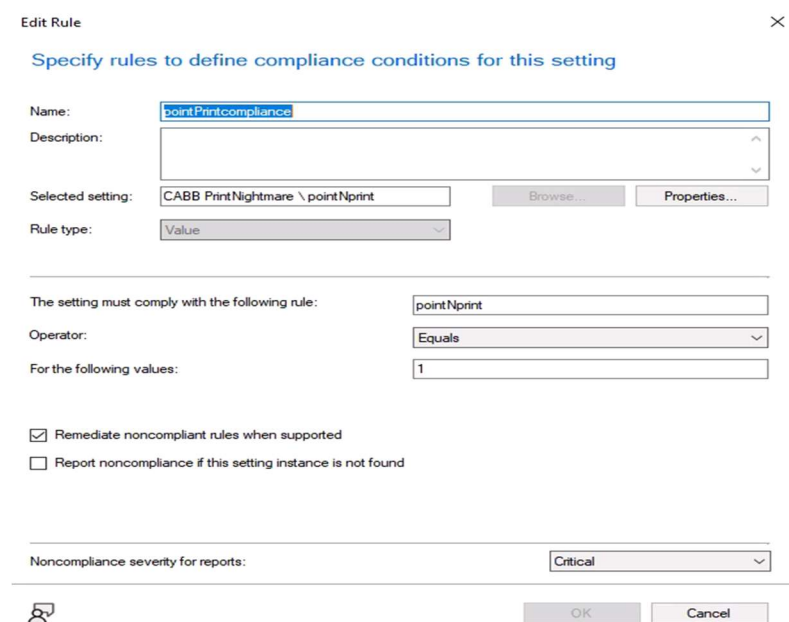
Key Name: SOFTWARE\Policies\Microsoft\Windows NT\Printers\PointAndPrint

Value Name: RestrictDriverInstallationToAdministrators

☐ This registry value is associated with a 64-bit application

☐ Create the registry value as a REG\_DWORD data type if remediated for noncompliant rules

## Configuring Compliance settings:



The 'Edit Rule' dialog box is shown with the 'Specify rules to define compliance conditions for this setting' section. It contains fields for Name, Description, Selected setting, Rule type, The setting must comply with the following rule, Operator, For the following values, Remediate noncompliant rules when supported, Report noncompliance if this setting instance is not found, and Noncompliance severity for reports.

**Edit Rule**

Specify rules to define compliance conditions for this setting

Name: pointPrintcompliance

Description:

Selected setting: CABB PrintNightmare \ pointNprint

Rule type: Value

The setting must comply with the following rule: pointNprint

Operator: Equals

For the following values: 1

☒ Remediate noncompliant rules when supported


☐ Report noncompliance if this setting instance is not found

Noncompliance severity for reports: Critical


OK Cancel

## Creating a configuration baseline:

Here I am using the configuration item 'CABB PrintNightmare'

 Create Configuration Baseline ✕

### Specify general information about this configuration baseline



Name:

CABB Print Nightmare

Description:

Select the configuration data (configuration items, configuration baselines, and software updates) to be evaluated for compliance by this configuration baseline. This configuration baseline will be assessed as compliant if all the items specified are compliant. Optional items are evaluated only if the relevant application is present on the client devices.

Configuration data:

Filter...

Name	Type	Purpose	Revision
CABB PrintNightmare	Operating System	Required	Latest

Add

Change Purpose

Change Revision


Remove

☐ Always apply this baseline even for co-managed clients

☐ Evaluate this baseline as part of compliance policy assessment

Assigned categories to improve searching and filtering:

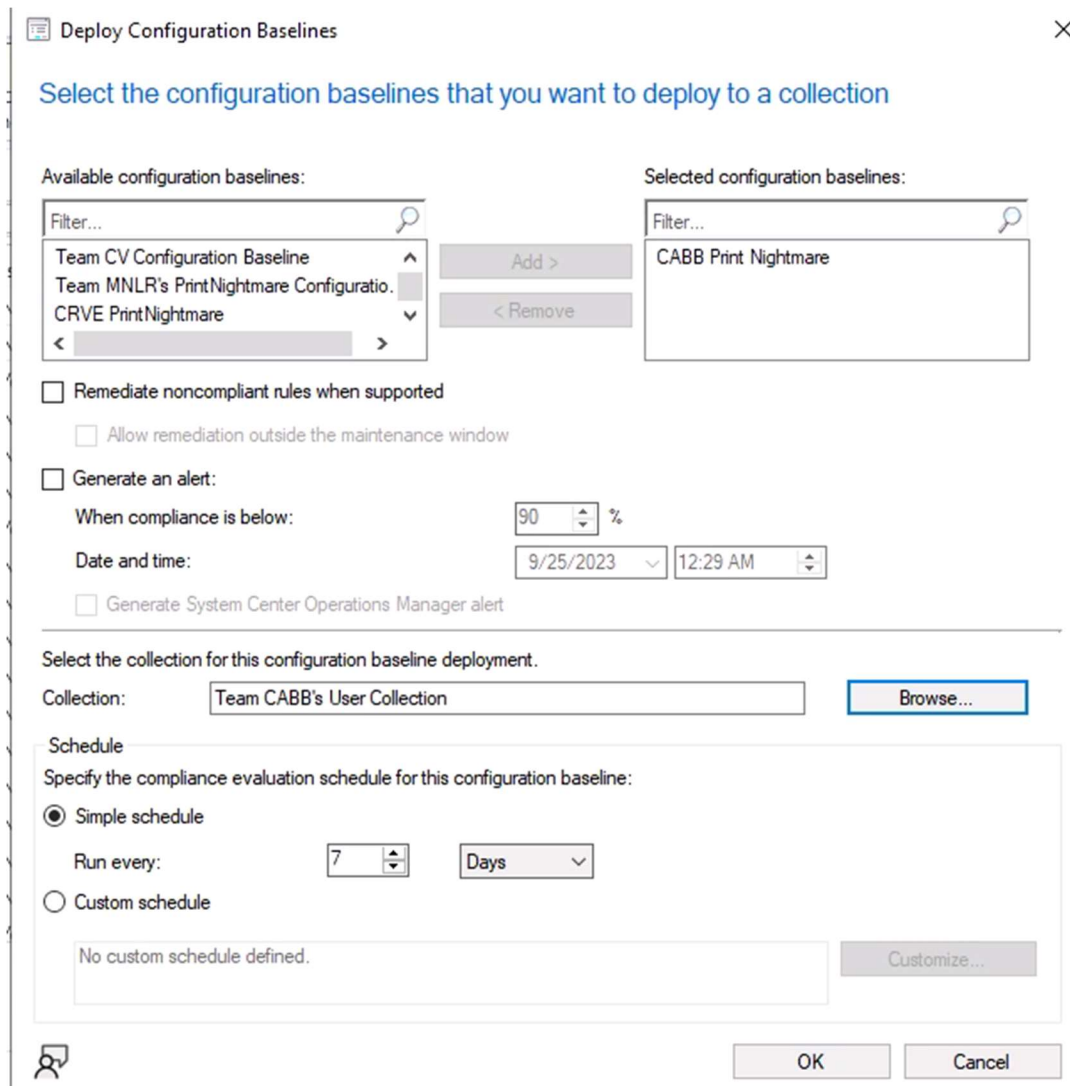
Categories...



OK

Cancel

## Deploying configuration baseline to team collection:



The dialog box is titled "Deploy Configuration Baselines" and contains the following sections:

- Select the configuration baselines that you want to deploy to a collection:** This section has two lists. The "Available configuration baselines:" list on the left contains "Team CV Configuration Baseline", "Team MNLR's PrintNightmare Configuratio.", and "CRVE PrintNightmare". The "Selected configuration baselines:" list on the right contains "CABB Print Nightmare". Between the lists are "Add >" and "< Remove" buttons.
- Remediate noncompliant rules when supported:** This section includes a checkbox for "Remediate noncompliant rules when supported", a sub-checkbox for "Allow remediation outside the maintenance window", a checkbox for "Generate an alert:", and a checkbox for "Generate System Center Operations Manager alert". The "Generate an alert:" section has a "When compliance is below:" dropdown set to "90 %", a "Date and time:" dropdown set to "9/25/2023 12:29 AM", and a "Customize..." button.
- Select the collection for this configuration baseline deployment:** This section has a "Collection:" dropdown set to "Team CABB's User Collection" and a "Browse..." button.
- Schedule:** This section has a "Specify the compliance evaluation schedule for this configuration baseline:" label, a "Simple schedule" radio button (selected), a "Run every:" dropdown set to "7", a "Days" dropdown, a "Custom schedule" radio button, and a "Customize..." button.

At the bottom of the dialog are "OK" and "Cancel" buttons.

## HiveNightmare

OS settings for our team's HiveNightmare Configuration Item.

General Supported Platforms Settings Compliance Rules Relationships Security

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 Vista
- ☒ Windows 7
- ☒ Windows 8
- ☒ Windows 8.1
- ☒ Windows 10
  - ☒ All Windows 10 (ARM64)
  - ☒ All Windows 10 Enterprise multi-session
  - ☒ All Windows 10 (64-bit)
  - ☒ All Windows 10 (32-bit)
- ☒ Windows 11
- ☒ Windows 2003
- ☒ Windows 2008
- ☒ Windows Server 2012
- ☒ Windows Server 2012 R2
- ☒ Windows Server 2016
- ☒ Windows Server 2019
- ☒ All Windows Server 2019 and higher (64-bit)

☐ Specify the version of Windows manually:

Add...




OK

Cancel

Apply

## Our detection and remediation scripts to our Configuration Item.

 Edit Discovery Script

Specify the script to find and return the value to be assessed for compliance on client devices. Use the echo command to return the script value to Configuration Manager.


Script language: Windows PowerShell Open... Clear

Script:

```
1 $detection = icacis $env:WINDIR\system32\config\sam
2
3
4 if ($detection.Contains("#BUILTIN\Users:(I)(RX)")){
5     "Not compliant"
6 }
7 else{
8     "Compliant"
9 }
```

Open in code editor...

OK Cancel

 Detection Rules Properties

General Compliance Rules

Specify details about this setting that represents a business or technical condition to assess for compliance on client devices.

Name: Detection Rules

Description:

Setting type: Script

Data type: String

Discovery script

Specify the script to find and return the value to be assessed for compliance on client devices. Use the echo command to return the script value to Configuration Manager.

Edit Script... Script status: Windows PowerShell is created

Remediation script (optional)


Specify the script to remediate noncompliant setting values found on client devices. Configuration Manager passes the noncompliant value to the script as a parameter.

Edit Script... Script status: Windows PowerShell is created

☐ Run scripts by using the logged on user credentials

☐ Run scripts by using the 32-bit scripting host on 64-bit devices

OK Cancel Apply

 Edit Remediation Script

Specify the script to remediate noncompliant setting values found on client devices. Configuration Manager can pass the compliant value to the script as a parameter.


Script language: Windows PowerShell Open... Clear

Script:

```
1 icacis %windir%\system32\config\*. * /inheritance:e
2
3 vssadmin delete shadows /all /quiet
4
5 $shadow = get-wmiobject win32_shadowcopy
6 "HiveNightmare remediated" -f $shadow.count
```

Open in code editor...

OK Cancel

 Detection Rules Properties

General Compliance Rules

Specify details about this setting that represents a business or technical condition to assess for compliance on client devices.

Name: Detection Rules

Description:

Setting type: Script

Data type: String

Discovery script

Specify the script to find and return the value to be assessed for compliance on client devices. Use the echo command to return the script value to Configuration Manager.

Edit Script... Script status: Windows PowerShell is created

Remediation script (optional)

Specify the script to remediate noncompliant setting values found on client devices. Configuration Manager passes the noncompliant value to the script as a parameter.

Edit Script... Script status: Windows PowerShell is created

☐ Run scripts by using the logged on user credentials

☐ Run scripts by using the 32-bit scripting host on 64-bit devices

OK Cancel Apply

Compliance conditions for our Configuration Item - the script reports back “Compliant” if it is compliant.

Edit Rule

Specify rules to define compliance conditions for this setting

Name:

Compliance

Description:

Selected setting:

CABB HiveNightmare \ Detection Rules

Browse...

Properties...

Rule type:

Value

The setting must comply with the following rule:

The value returned by the specified script:

Operator:

Equals

For the following values:

Compliant

☒ Run the specified remediation script when this setting is noncompliant

☐ Report noncompliance if this setting instance is not found

Noncompliance severity for reports:

Critical

OK

Cancel

9/25/2023 5:46 AM

CABB HiveNightmare Properties

General

Supported Platforms

Settings

Compliance Rules

Relationships

Security

Use compliance rules to specify the conditions that make a configuration item setting compliant on client devices.  
The following compliance rules are associated with this configuration item.

☒ Track remediation history when supported

Name	Setting Name	CI Name	Condition	Severity	Remediate
Compliance	Detection Rules	CABB Hive...	Equals Compl...	Critical	Yes

New ...

Edit ...

Delete

OK

Cancel

Apply



## Creating a Configuration Baseline for the Hive Nightmare deployment.

CABB Hive Nightmare Properties

General

Evaluation Conditions

Deployments

Security

Name: CABB Hive Nightmare

Description:

Status: Enabled

Relationships: No

Deployed: Yes

Date created: 9/24/2023 11:06 PM

Created by: IFT380\bhema77\_ft380

Date modified: 9/25/2023 12:57 AM

Modified by: IFT380\bhema77\_ft380

☒ Always apply this baseline even for co-managed clients

☒ Evaluate this baseline as part of compliance policy assessment

Assigned categories to improve searching and filtering:

Categories...

OK

Cancel

Apply

CABB Hive Nightmare Properties

General

Evaluation Conditions

Deployments

Security

Select the configuration data (configuration items, configuration baselines, and software updates) to be evaluated for compliance by this configuration baseline. This configuration baseline will be assessed as compliant if all the items specified are compliant. Optional items are evaluated only if the relevant application is present on the client devices.

Configuration data:

Filter...

Name	Type	Purpose	Revision
CABB HiveNightmare	Operating System	Required	Latest

Add

Change Purpose

Change Revision


Remove

OK

Cancel

Apply

Deployed our Hive Nightmare Configuration Baseline to our team's collection. After a refresh, it had already detected one of our machines as now being compliant after remediation.

CABB Hive Nightmare				
Icon	Collection	Compliance %	Deployment Start Time	Action
	Team CABB's User Collection	25.0	9/25/2023 5:37 AM	Remediate

Finally, the compliance report shows the Hive Nightmare compliance state as compliant.

Compliance Report

Report View | Xsl View

COMPUTER NAME: ASU-FRM1-APP065  
EVALUATION TIME: 9/25/2023 6:23:02 AM  
BASELINE NAME: CABB Hive Nightmare  
REVISION: 2  
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
CABB Hive Nightmare	2	Baseline		<span>Compliant</span>	None	0	0	0	0
CABB HiveNightmare	22	Operating System Configuration Item	Required	<span>Compliant</span>	None	0	0	0	0

Details:

NAME: CABB Hive Nightmare  
TYPE: Baseline  
REVISION: 2  
COMPLIANCE STATE: Compliant  
NON-COMPLIANCE SEVERITY: None  
DESCRIPTION:

NAME: CABB HiveNightmare  
TYPE: Operating System Configuration Item  
REVISION: 22  
COMPLIANCE STATE: Compliant  
NON-COMPLIANCE SEVERITY: None  
DESCRIPTION: Echo's Compliant or echo's Vulnerable

Messenger

9:23 AM 9/25/2023

```
# The detection script
$detection = icacis $env:WINDIR\system32\config\sam
```

```
if ($detection.Contains("*BUILTIN\Users:(I)(RX)*")){
    "Not compliant"
}
else{
    "Compliant"
}
```

```
# Our remediation script
icacis %windir%\system32\config\*. * /inheritance:e
```

```
vssadmin delete shadows /all /quiet
```

```
$shadow = get-wmiobject win32_shadowcopy
"HiveNightmare remediated" -f $shadow.count
```

