Evaluate-STIG

Deploying Evaluate-STIG with Microsoft Configuration Manager

v1.6

NAVSEA
WARFARE CENTERS

Table of Contents

Introduction

Microsoft Configuration Manager (ConfigMgr) is a popular tool for managing clients in a networked environment and "helps IT manage PCs and servers, keeping software up-to-date, setting configuration and security policies, and monitoring system status".

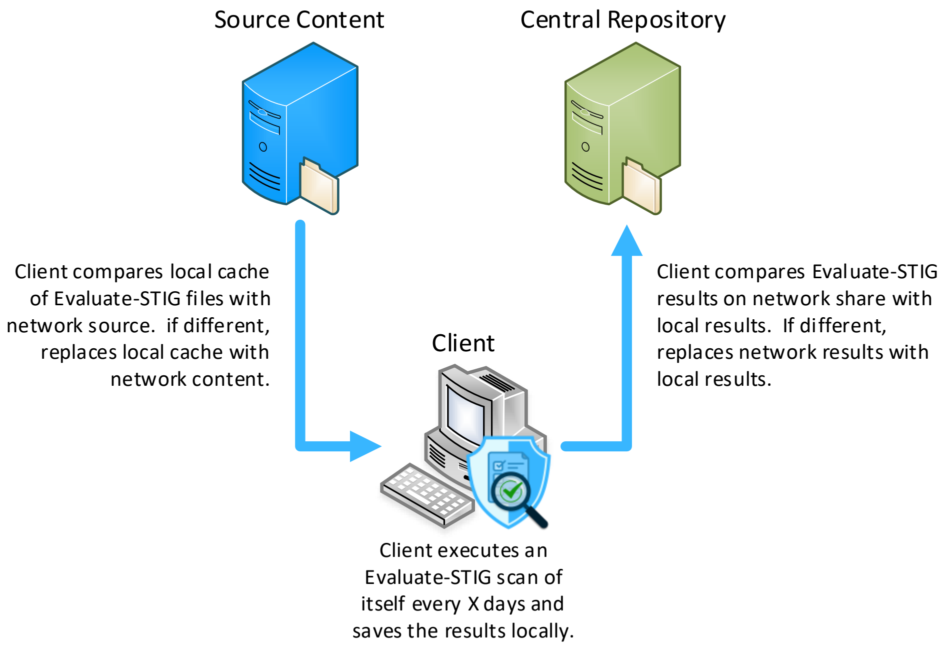
Configuration Baselines (CB) and Configuration Items (CI) have proven to be an effective method of deploying Evaluate-STIG to entire networks and can play an important role in continuous monitoring processes. This guide will describe the steps of importing, configuring, and deploying the **`Evaluate-STIG as CI`** sample CB/CI available for Evaluate-STIG.

`Evaluate-STIG as CI` is designed to ensure clients are scanning with the same Evaluate-STIG version on a configured interval. During each evaluation of the CB, the client will:

1. Compare their local copy of the Evaluate-STIG files with those in the source network share. If any differences are found, the local copy will be refreshed with the network share content.

2. Compare the current date with Evaluate-STIG's tattoo (the **`LastRun`** registry value under **`HKLM:\SOFTWARE\Evaluate-STIG`**). If greater than the specified days, will start an Evaluate-STIG scan and save the results locally on the client. This is to ensure scans complete even when not connected to the network (e.g. remote users not currently connected via VPN).

3. Compare the local scan results with the client's results on a central repository network share. If any differences are found, the central repository's results for the client will be refreshed with the client's local results.



Client compares local cache of Evaluate-STIG files with network source. if different, replaces local cache with network content.

Client compares Evaluate-STIG results on network share with local results. If different, replaces network results with local results.

Client executes an Evaluate-STIG scan of itself every X days and saves the results locally.

Prerequisites

- Default Active Directory security groups:
  - **`Domain Computers`** (if deploying the CB to workstations/member servers)
  - **`Domain Controllers`** (if deploying the CB to domain controllers)

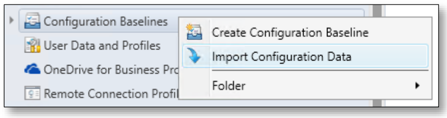
- A network share containing the extracted Evaluate-STIG files. This will be used as the **`$SourceContentPath`** variable below.
  - Minimum NTFS and SHARE permission: **`Read`** for the appropriate group(s) above.

- A network share for Evaluate-STIG results to be sent. This will be used as the **`$CentralRepoPath`** variable below.
  - Minimum NTFS and SHARE permission: **`Modify`** for the appropriate group(s) above.

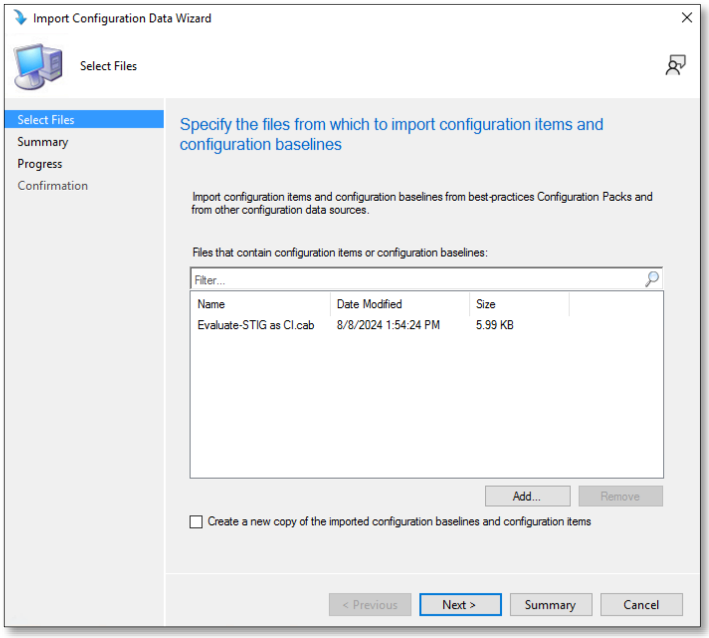
Importing the CB/CI

1. In the Configuration Manager console, navigate to **`Assets and Compliance > Overview > Compliance Settings > Configuration Baselines`**

2. Right-click and select **`Import Configuration Data`**:


Configuration Baselines
User Data and Profiles
OneDrive for Business Pro
Remote Connection Profil
Create Configuration Baseline
Import Configuration Data
Folder

3. Click **Add** and select the **`Evaluate-STIG as CI.cab`** file:



Specify the files from which to import configuration items and configuration baselines

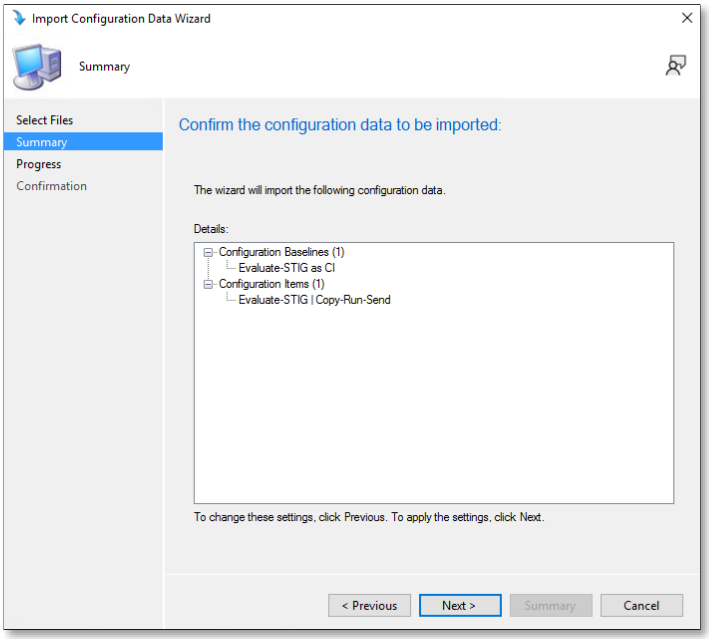
Import configuration items and configuration baselines from best-practices Configuration Packs and from other configuration data sources.

Files that contain configuration items or configuration baselines:

Name	Date Modified	Size
Evaluate-STIG as CI.cab	8/8/2024 1:54:24 PM	5.99 KB

□ Create a new copy of the imported configuration baselines and configuration items

4. Click **Next** and you will be shown the Configuration Baseline and Configuration Item that will be imported:



Confirm the configuration data to be imported:

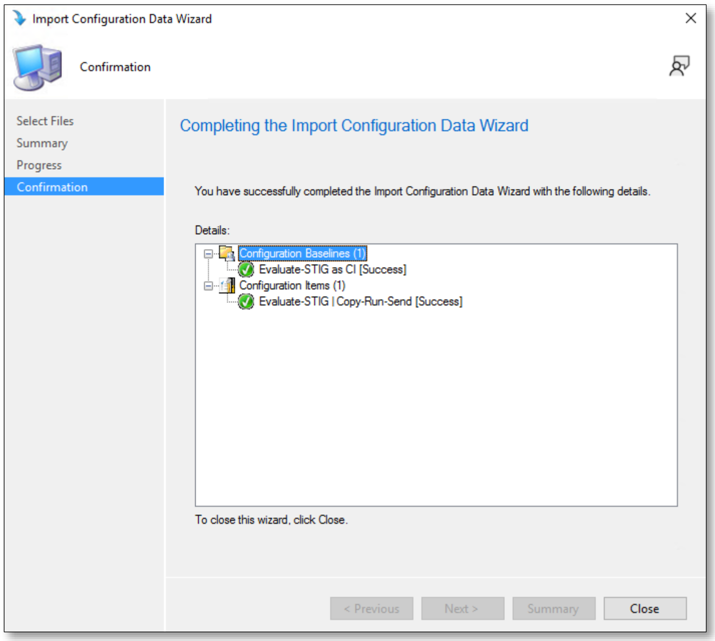
The wizard will import the following configuration data.

Details:

```
⊟ Configuration Baselines (1)
  └ Evaluate-STIG as CI
⊟ Configuration Items (1)
  └ Evaluate-STIG | Copy-Run-Send
```

To change these settings, click Previous. To apply the settings, click Next.

5. Click **Next** and the import will begin. If successful, the next screen will reflect that. Click **Close** to complete.



Completing the Import Configuration Data Wizard

You have successfully completed the Import Configuration Data Wizard with the following details.

Details:

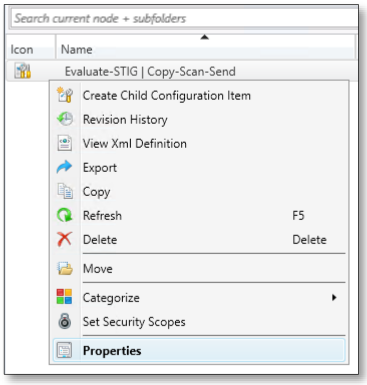
```
⊟ Configuration Baselines (1)
  └ Evaluate-STIG as CI [Success]
⊟ Configuration Items (1)
  └ Evaluate-STIG | Copy-Run-Send [Success]
```

To close this wizard, click Close.

Configuring the CI

1. In the Configuration Manager console, navigate to **Assets and Compliance > Overview > Compliance Settings > Configuration Items**

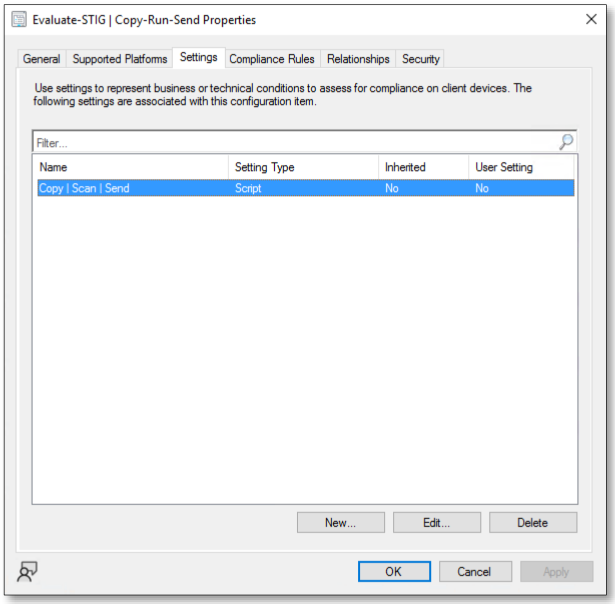
2. Right-click on the **Evaluate-STIG | Copy-Scan-Send** configuration item and select **Properties**:



Icon Name

Evaluate-STIG | Copy-Scan-Send

3. Navigate to the **Settings** tab, select **Copy | Scan | Send** and click **Edit…**

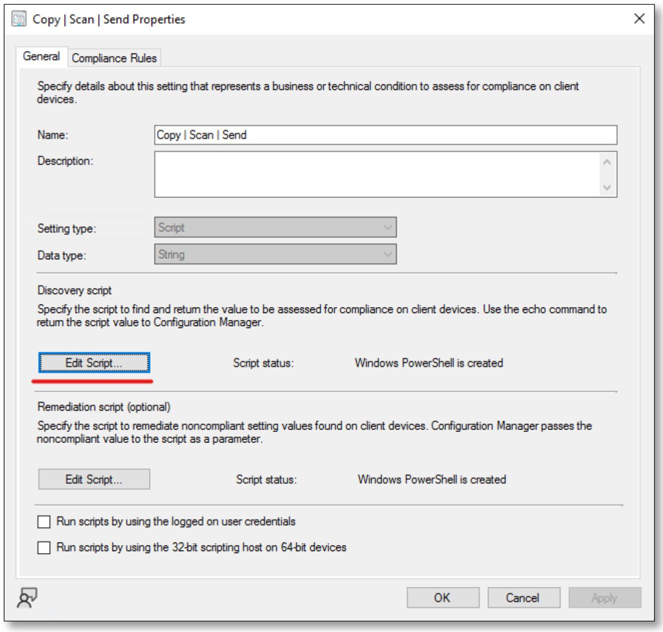


Evaluate-STIG | Copy-Run-Send Properties

Use settings to represent business or technical conditions to assess for compliance on client devices. The following settings are associated with this configuration item.

<table>
<tr><th>Name</th><th>Setting Type</th><th>Inherited</th><th>User Setting</th></tr>
<tr><td>Copy | Scan | Send</td><td>Script</td><td>No</td><td>No</td></tr>
</table>

4. Click the **`Edit Script`** button in the **`Discovery script`** section:



Copy | Scan | Send Properties

General | Compliance Rules

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

Name: Copy | Scan | Send

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.

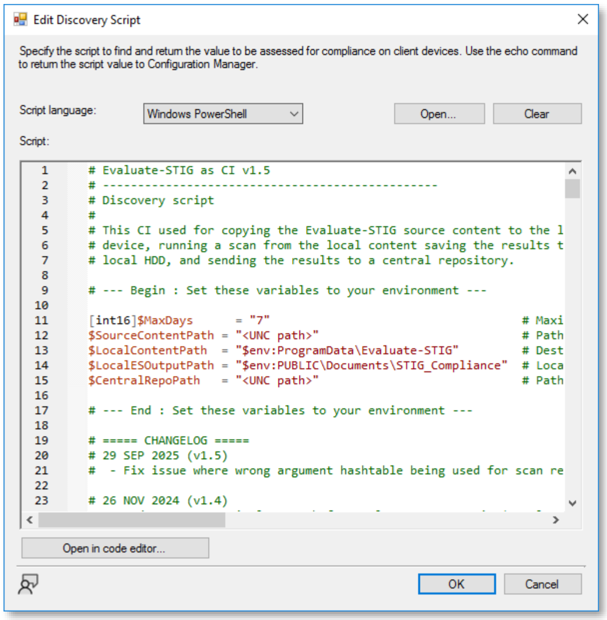
Edit Script... Script status: Windows PowerShell is created

☐ Run scripts by using the logged on user credentials

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

5. Update the variables for your environment and then click **OK** to save the changes:

   a. **`[int16]$MaxDays`**: The number of days to wait before running a new Evaluate-STIG scan.
   b. **`$SourceContentPath`**: Path to where your source Evaluate-STIG files are located. These will be copied locally to each client.
   c. **`$LocalContentPath`**: Path on the client that you want the source Evaluate-STIG files copied to. Scans will be initiated from this location.
   d. **`$LocalESOutputPath`**: Path on the client that Evaluate-STIG results will be saved. These will be copied to a central location later. *Do NOT include the client's hostname in this path.*
   e. **`$CentralRepoPath`**: Central repository to send client results. This should be a network share. *Do NOT include the client's hostname in this path.*



Edit Discovery Script

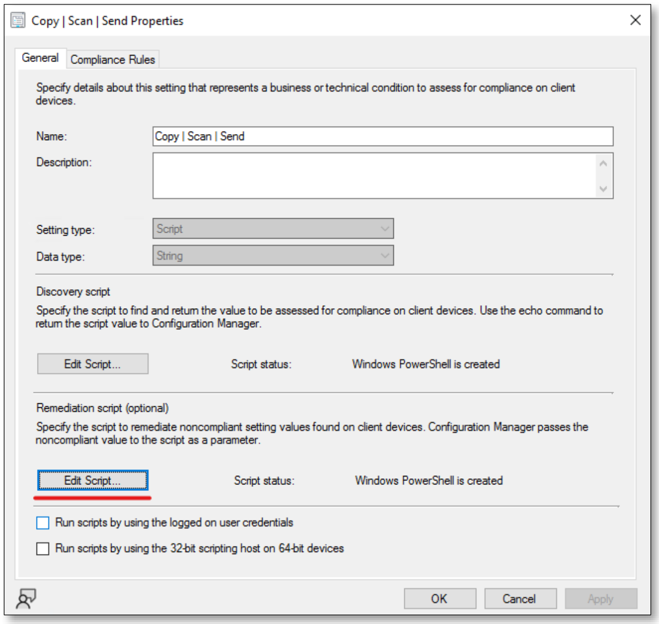
Specify the script to find and return the value to be assessed for compliance on client devices. Use the echo command to return the script value to Configuration Manager.

Script language: Windows PowerShell

Script:

```
# Evaluate-STIG as CI v1.5
# ---------------------------------------------
# Discovery script
#
# This CI used for copying the Evaluate-STIG source content to the l
# device, running a scan from the local content saving the results t
# local HDD, and sending the results to a central repository.

# --- Begin : Set these variables to your environment ---

[int16]$MaxDays      = "7"                                    # Maxi
$SourceContentPath = "<UNC path>"                             # Path
$LocalContentPath  = "$env:ProgramData\Evaluate-STIG"         # Dest
$LocalESOutputPath = "$env:PUBLIC\Documents\STIG_Compliance"  # Loca
$CentralRepoPath   = "<UNC path>"                             # Path

# --- End : Set these variables to your environment ---

# ===== CHANGELOG =====
# 29 SEP 2025 (v1.5)
#  - Fix issue where wrong argument hashtable being used for scan re

# 26 NOV 2024 (v1.4)
```

6. Click the **`Edit Script`** button in the **`Remediation script`** section:



Copy | Scan | Send Properties

General | Compliance Rules

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

Name: Copy | Scan | Send

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)

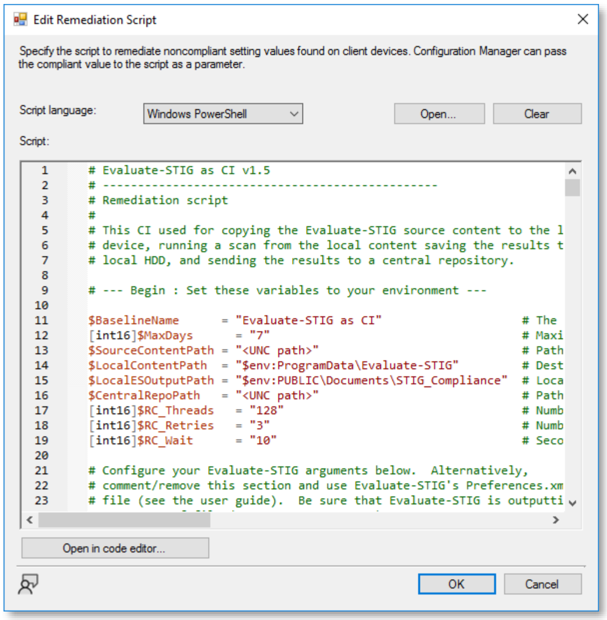
Specify the script to remediate noncompliant setting values found on client devices. Configuration Manager passes the noncompliant value to the script as a parameter.

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

7. Update the variables for your environment and then click **OK** to save the changes:



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

Script:

```
# Evaluate-STIG as CI v1.5
# -----------------------------------------------
# Remediation script
#
# This CI used for copying the Evaluate-STIG source content to the l
# device, running a scan from the local content saving the results t
# local HDD, and sending the results to a central repository.

# --- Begin : Set these variables to your environment ---

$BaselineName      = "Evaluate-STIG as CI"                        # The
[int16]$MaxDays     = "7"                                        # Maxi
$SourceContentPath = "<UNC path>"                                # Path
$LocalContentPath  = "$env:ProgramData\Evaluate-STIG"            # Dest
$LocalESOutputPath = "$env:PUBLIC\Documents\STIG_Compliance"     # Loca
$CentralRepoPath   = "<UNC path>"                                # Path
[int16]$RC_Threads  = "128"                                      # Numb
[int16]$RC_Retries  = "3"                                        # Numb
[int16]$RC_Wait     = "10"                                       # Seco

# Configure your Evaluate-STIG arguments below.  Alternatively,
# comment/remove this section and use Evaluate-STIG's Preferences.xm
# file (see the user guide).  Be sure that Evaluate-STIG is outputti
```

a. **`$BaselineName`**: Display name of the Configuration Baseline as it shows in the console. If a new Evaluate-STIG scan is run, the CI will re-evaluate the CB to clean up any potential time out errors.

b. **`[int16]$MaxDays`**: The number of days to wait before running a new Evaluate-STIG scan.

c. **`$SourceContentPath`**: Path to where your source Evaluate-STIG files are located. These will be copied locally to each client.

d. **`$LocalContentPath`**: Path on the client that you want the source Evaluate-STIG files copied to. Scans will be initiated from this location.

e. **`$LocalESOutputPath`**: Path on the client that Evaluate-STIG results will be saved. These will be copied to a central location later. *Do NOT include the client's hostname in this path.*

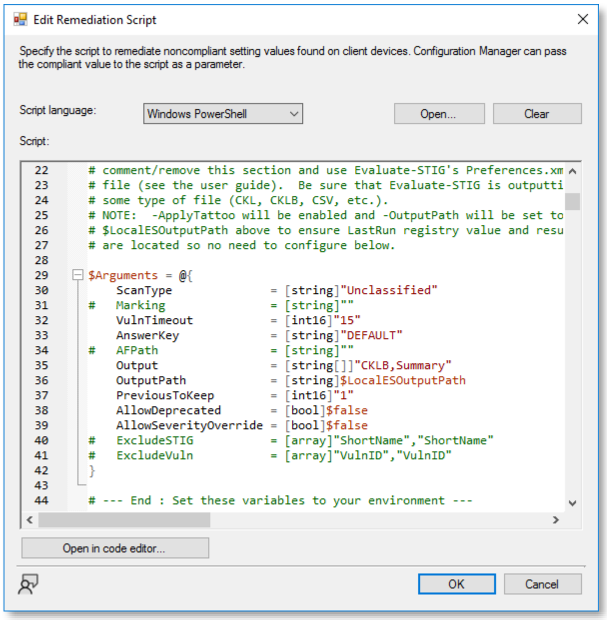
f. **`$CentralRepoPath`**: Central repository to send client results. This should be a network share. *Do NOT include the client's hostname in this path.*

g. **`[int16]$RC_Threads`**: Maximum threads for `robocopy.exe`. Must be at least `1` and no more than `128`.

h. **`[int16]$RC_Retries`**: Maximum retries for `robocopy.exe`.

i. **`[int16]$RC_Wait`**: Time in seconds to wait between retries for `robocopy.exe`.

j. Configure the Evaluate-STIG scan parameters to your requirements or remove this section and use **`Preferences.xml`** (reference Evaluate-STIG's User Guide for more).



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

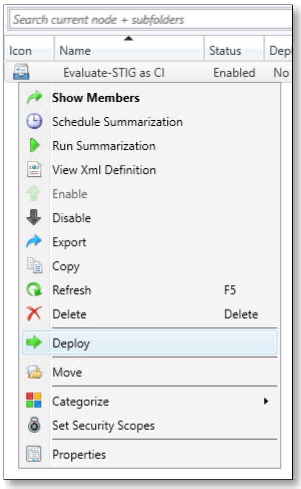
Script:

```
# comment/remove this section and use Evaluate-STIG's Preferences.xm
# file (see the user guide).  Be sure that Evaluate-STIG is outputti
# some type of file (CKL, CKLB, CSV, etc.).
# NOTE:  -ApplyTattoo will be enabled and -OutputPath will be set to
# $LocalESOutputPath above to ensure LastRun registry value and resu
# are located so no need to configure below.

$Arguments = @{
    ScanType              = [string]"Unclassified"
#   Marking               = [string]""
    VulnTimeout           = [int16]"15"
    AnswerKey             = [string]"DEFAULT"
#   AFPath                = [string]""
    Output                = [string[]]"CKLB,Summary"
    OutputPath            = [string]$LocalESOutputPath
    PreviousToKeep        = [int16]"1"
    AllowDeprecated       = [bool]$false
    AllowSeverityOverride = [bool]$false
#   ExcludeSTIG           = [array]"ShortName","ShortName"
#   ExcludeVuln           = [array]"VulnID","VulnID"
}

# --- End : Set these variables to your environment ---
```

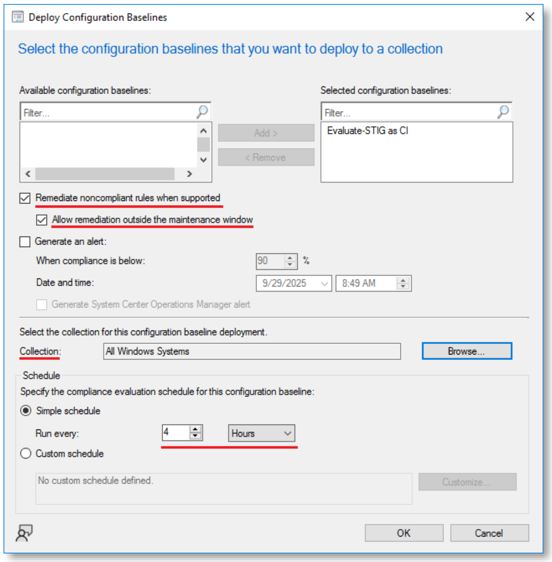
Deploying the CB

1. In the Configuration Manager console, navigate to **`Assets and Compliance > Overview > Compliance Settings > Configuration Baselines`**

2. Right-click on the **`Evaluate-STIG as CI`** configuration baseline and select **Deploy**:



3. Configure the deployment options and click **OK**. Some notes on the underlined options:



Deploy Configuration Baselines

Select the configuration baselines that you want to deploy to a collection

Available configuration baselines:

Selected configuration baselines: Evaluate-STIG as CI

☑ Remediate noncompliant rules when supported

☑ Allow remediation outside the maintenance window

☐ Generate an alert:

When compliance is below: 90 %

Date and time: 9/29/2025 8:49 AM

☐ Generate System Center Operations Manager alert

Select the collection for this configuration baseline deployment.

Collection: All Windows Systems

Schedule

Specify the compliance evaluation schedule for this configuration baseline:

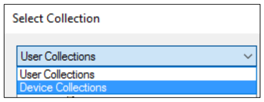
● Simple schedule

Run every: 4 Hours

○ Custom schedule

No custom schedule defined.

   a. **`Remediate noncompliant rules when supported`**: This is required in order correct non-compliant steps (source content, last scan, central repo content).
   b. **`Allow remediation outside the maintenance window`**: This is recommended in order to help ensure continuous monitoring as well as catch remote machines that may not be connected to the network after hours.
   c. **`Collection`**: This must be a ***`Device`*** collection to ensure permissions for Evaluate-STIG scans and network access.



Select Collection

User Collections

User Collections
Device Collections

   d. **`Schedule`**: Recommend every 4 hours. This does not mean an Evaluate-STIG scan will occur every four hours but rather the compliance checks - local content is current, last Evaluate-STIG scan is within the configured threshold, and central repository results are updated.

Troubleshooting

Discovery and Remediation activity detail is logged under **`$env:windir\Temp\Evaluate-STIG_as_CI.log`**. Refer to this log to assist in troubleshooting efforts. Once the log size grows to greater than 1MB, a new log will be created and the current log rotated to **`Evaluate-STIG_as_CI-<date>-<time>.log`**.

For Robocopy, activity is logged to **`$env:windir\Temp\Evaluate-STIG_as_CI_Robocopy.log`**.

Change Log

14 OCT 2025 (v1.6)

- Fix issue where deleting HKLM:\SOFTWARE\Evaluate-STIG fails when it doesn't exist.

29 SEP 2025 (v1.5)

- Fix issue where wrong argument hashtable being used for scan resulting in `-ApplyTattoo` not being set.

26 NOV 2024 (v1.4)

- Update to recursively search for `Evaluate-STIG.ps1` in `$LocalContentPath` and select the most recently modified to use for scan.
- Update to enclose `$EvalSTIG_PS1` in quotes in the event whitespace exists in the path to Evaluate-STIG.ps1
- Fix for `ApplyTattoo` parameter.
- Fix for failed scan if path `$LocalESOutputPath` does not exist.
- Fix issue where switch parameters were being added to command line even when `$false`.
- Fix issue where remediation script would fail if `$LocalESOutputPath` is empty.

26 SEP 2024 (v1.3)

- Fix remediation loop issue due to returning difference object to console.
- Change copy process to use `Robocopy.exe` instead of `Copy-Item` for performance.
- Add configurable `Robocopy.exe` parameters.

24 SEP 2024 (v1.2):

- Add `Write-CILog` function. Log located at **$env:windir\Temp\Evaluate-STIG_as_CI.log** and will be rotated when greater than 1MB.

04 SEP 2024 (v1.1 - internal release):

- Add `Get-CIErrorInformation` function to improve error logging

12 AUG 2024 (V1.0):

- Initial release