ForeScout® Extended Module for Advanced Compliance

Configuration Guide

Version 1.1.0
# Table of Contents

**About Advanced Compliance Integration** ......................................................... 4
  Use Cases ............................................................................................................ 4
  Additional Documentation .................................................................................... 6

**About This Module** ......................................................................................... 7
  How It Works ....................................................................................................... 7
  What to Do ......................................................................................................... 8

**Requirements** ................................................................................................. 8
  CounterACT Software Requirements ................................................................ 8
  Endpoint Requirements ...................................................................................... 8
  Networking Requirements .................................................................................. 8
  CounterACT Endpoint Access and Advanced Compliance .............................. 9
  ForeScout Module License Requirements ......................................................... 10
    Requesting a License ..................................................................................... 11
    More License Information ............................................................................. 12
  Third-Party Requirements ................................................................................ 12
    Supported SCAP Content .............................................................................. 12

**Install the Module** .......................................................................................... 13

**Configure the Module** .................................................................................. 13
  Import SCAP Content ......................................................................................... 14
  View SCAP File Details .................................................................................... 15
  View Benchmark Details ............................................................................... 16
  Edit a Short Benchmark Title .......................................................................... 17
  View OVAL Collection Details .................................................................... 18
  Edit an OVAL Collection Name .................................................................... 19
  Test the Endpoints .......................................................................................... 20

**Run Advanced Compliance Policy Templates** ........................................... 21
  SCAP Compliance Score Policy Template ...................................................... 21
    Prerequisites ................................................................................................ 21
    Run the Template ......................................................................................... 21
  How Devices are Detected and Handled ........................................................ 27
    Main Rule ..................................................................................................... 27
    Sub-Rules .................................................................................................... 27

**Create Custom Advanced Compliance Policies** ......................................... 28

**Detecting Compliance – Policy Properties** ............................................... 29
  Profile Score Property .................................................................................... 30
Rule Results Property................................................................. 31

Managing Advanced Compliance Results – Policy Action .................. 33
   Email Compliance Report Action ................................................. 34

Display Advanced Compliance Inventory Information ........................... 34

Generate Advanced Compliance Evaluation Reports ............................ 35
   Create an SCAP ARF Report ....................................................... 35

Additional CounterACT Documentation ............................................. 39
   Documentation Portal ............................................................... 39
   Customer Support Portal .......................................................... 40
   CounterACT Console Online Help Tools ...................................... 40

Appendix A: Executable Files Used by the Module .............................. 40
About Advanced Compliance Integration

The CounterACT Advanced Compliance integration greatly simplifies the effort required to enforce compliance on network endpoints by automating compliance scanning and reporting. SCAP content is downloaded from known public repositories and then uploaded to CounterACT. CounterACT uses the benchmark to assess the compliance status of managed Windows endpoints. Endpoints can be scanned and assessed according to a schedule or based on a specific event, such as an attempt to gain access to the network. CounterACT uses the scan results to identify device compliance based on customizable thresholds. CounterACT policies can be used to isolate non-compliant devices, and to notify the security officer or network administrator so that appropriate actions can be taken.

Use Cases

This section describes important use cases supported by this module. To understand how this module helps you achieve these goals, see About This Module.

Continuous Configuration Management

- Ensure that Windows endpoints are compliant with regulatory requirements such as PCI or government standards such as the Secure Technical Implementation Guide (STIG) before they are granted full network access.
- Confirm that all Windows endpoints remain compliant while they are on the network.

Report and Quarantine Non-Compliant Endpoints

- Create and email a detailed report of any Windows endpoint which fails to meet a defined compliance level for any given SCAP Compliance benchmark.
- Quarantine all endpoints that fall below a minimum compliance level.
Measure the Organizational Compliance Level Against Known Benchmarks

- Obtain an overview of the compliance of all Windows endpoints for a given benchmark.
- Drill down to compliance rules of interest to understand the compliance level among Windows endpoints.
Generate Standard Security Compliance Reports

Information Security Officers can use the CounterACT Reports portal to generate detailed reports in Asset Report Format (ARF). A report template provided by this module generates XML reports of XCCDF profile evaluation results. Each report created with this template reports the scores for a specified benchmark profile for selected Windows endpoints in the network.

- You can use the Reports portal to generate individual reports, or more typically to define a schedule for regular report generation.
- For each report job, you can define a target server on which CounterACT places report files. This supports automated submission/deposit of data to external ARF compatible applications.

Additional Documentation

For more information about SCAP 1.0, refer to:

For more information about SCAP 1.1, refer to:

For more information about SCAP 1.2, refer to:
About This Module

The Advanced Compliance Module provides a mechanism for verifying endpoint configuration using industry standard SCAP content. It can also produce XML formatted results for use by third-party systems.

Use the Advanced Compliance Module to:

- Easily import SCAP data streams, bundles, and OVAL collections for compliance assessment.
- View the ID, title and description of all profiles.
- View the definition ID, class, title, reference ID, description and version number of all OVAL rules.
- Create policies to:
  - Automatically initiate Windows endpoint scans for compliance based on a fixed schedule or a specific event.
  - Create policies for assessing endpoints based on their scan profile scores or the results of specific OVAL checks.
  - Automatically trigger CounterACT actions based on scan results.
- Automatically or manually email detailed scan results to relevant recipients.
- View the profile scores and OVAL results of scans in the Inventory view.
- Generate detailed ARF compliance reports that evaluate a specified benchmark profile for selected Windows endpoints in the network.

To use the module, you should have a basic understanding of SCAP concepts, functionality and terminology, and understand how CounterACT policies and other basic features work.

How It Works

The following describes a typical Advanced Compliance scenario.

1. The user imports required SCAP content files.
2. For each profile in an imported benchmark, CounterACT automatically creates one Profile Score Property and one Rule Results Property.
3. The user creates policies using one or more Advanced Compliance properties.
4. When a policy is run on a Windows endpoint, a compliance scan is initiated, and the Profile Score Property and Rule Results Property are evaluated.
5. (Optional) Depending on the conditions that are matched, optional actions defined in the policy are run. For example, actions such as emailing scan results can be added to the policies.
What to Do
This section lists the steps you should take to set up your system when working with the Advanced Compliance Module:

1. Verify that you have met system requirements. See Requirements.
2. Install the Module
3. Run Advanced Compliance Policy Templates
4. Create Custom Advanced Compliance Policies

Requirements
This section describes system requirements, including:

- CounterACT Software Requirements
- Endpoint Requirements
- Networking Requirements
- CounterACT Endpoint Access and Advanced Compliance
- ForeScout Module License Requirements
- Third-Party Requirements

CounterACT Software Requirements
The module requires the following CounterACT releases and other CounterACT components.

- CounterACT version 7.0.0
- Service Pack 2.3.3 or above
- Operating System Update Pack 1.2.0 or above
- HPS Inspection Engine 10.4.0 or above

Endpoint Requirements
Endpoints to be scanned must be manageable by the HPS Inspection Engine, and must have Windows PowerShell and .NET Framework 2.0 or above installed.

Networking Requirements
The following port must be open on enterprise firewalls to support communication between endpoints to be scanned for compliance and the managing Appliance:

- 10008/TCP
CounterACT Endpoint Access and Advanced Compliance

CounterACT accesses endpoints to learn detailed information such as applications and installed files, registry key information and more. In addition, this access lets CounterACT run scripts on endpoints.

CounterACT uses one of the following methods to access Windows endpoints:

- Remote Inspection uses WMI and other standard domain/host management protocols to query the endpoint, and to run scripts. Remote Inspection is agentless - CounterACT does not install any applications on the endpoint.
- SecureConnector is a small-footprint executable that runs on the endpoint. It reports endpoint information to CounterACT, and runs scripts.

When CounterACT successfully implements one of these access methods on an endpoint, the endpoint is resolved as Manageable by CounterACT. Because the Advanced Compliance module runs scripts on endpoints to implement compliance scans, it requires that endpoints be manageable by CounterACT.

The methods CounterACT uses to access the endpoint and the way they are deployed determine which endpoint user account is used to run the compliance scan, and therefore what permissions are available. This can impact the ability to perform certain queries or tests in the scan.

For example, when Windows endpoints are managed using SecureConnector:

- When SecureConnector is installed as a service, compliance scans are run in the context of the SYSTEM account and have full system access.
- When SecureConnector is installed as an application, compliance scans are run in the context of the logged in user.

Similarly, when Windows endpoints are managed using Remote Inspection:

- When Remote Inspection is configured to run scripts with the ForeScout Remote Inspection Service (fsprocsvc) utility, compliance scans are run in the context of the SYSTEM account, and have full system access.
- When Remote Inspection is configured to run scripts using WMI or Task Scheduler, compliance scans are run in the context of the Administrator user configured under Domain Credentials.

\[ WMI\text{ security features prevent remotely run scripts from establishing connections with other machines on the network. Therefore, when Remote Inspection is configured to run scripts with WMI only, CounterACT evaluation of any OVAL rule which establishes a connection with another endpoint on the network (for example, an Active Directory server) will fail for that rule.}\]

To ensure maximum compatibility with scan tests, the recommended configuration for managed endpoints is as follows:

- If using SecureConnector, install SecureConnector as a Service.
If using Remote Inspection, run scripts using fsprocsvc.

Deployment options for Remote Inspection and SecureConnector are configured in the HPS Inspection Engine Plugin. For more information about Remote Inspection, SecureConnector, and the user credentials with which CounterACT runs scripts on endpoints, refer to the HPS Inspection Engine Plugin Configuration Guide.

**ForeScout Module License Requirements**

This ForeScout Module requires a module license. The installation package for the module is in the form of a CounterACT plugin. When installing the plugin you are provided with a 90-day demo module license.
If you would like to continue exploring the module before purchasing a permanent license, you can request a demo license extension. Consult with your ForeScout representative before requesting the extension. You will receive email notification and alerts at the Console before the demo period expires.

When the demo period expires, you will be required to purchase a permanent module license. In order to continue working with the module, you must purchase the license.

Demo license extension requests and permanent license requests are made from the CounterACT Console.

**Requesting a License**

When requesting a demo license extension or permanent license, you are asked to provide the device **capacity** requirements. This is the number of devices that you want this license to handle. You must define at least the number of devices currently detected by CounterACT. You can request a license that handles more to ensure that you are licensed for support on additional devices as your deployment grows.

Enter this number in the **Devices** pane of the Module License Request wizard, in the CounterACT, Console Modules pane.

To view the number of currently detected devices:

1. Select the **Home** tab.
2. In the Views pane, select the **All Hosts** folder. The number in parentheses displayed next to the **All Hosts** folder is the number of devices currently detected.
More License Information

See the CounterACT Console User Manual for information on requesting a permanent license or a demo license extension. You can also contact your ForeScout representative or license@forescout.com for more information.

Third-Party Requirements

This module requires access to SCAP content. The content may be custom-made or from a public repository, such as:

- https://web.nvd.nist.gov/view/ncp/repository

Supported SCAP Content

The module can import SCAP content in one of the following standard formats:

- SCAP 1.2 compliant source data stream (XML file containing XCCDF benchmarks and related OVAL rules)
- SCAP 1.0 / 1.1 compliant bundle (ZIP archive of XML files)
- OVAL 5.11.1 compliant file containing one or more OVALs

The module ignores OCIL (Open Checklist Interactive Language) content, commonly used for manual SCAP security checks.
Install the Module

This section describes how to install the module.

The installation package for the module is in the form of a CounterACT plugin.

To install the plugin:

1. Navigate to the Customer Support, ForeScout Modules page and download the plugin .fpi file.

2. Save the file to the machine where the CounterACT Console is installed.

3. Log into the CounterACT Console and select Options from the Tools menu.


5. Select Install. The Open dialog box opens.

6. Browse to and select the saved plugin .fpi file.

7. Select Install.

8. If you have not yet purchased a permanent module license, a message appears indicating that the plugin will be installed with a demo module license. Select Yes and then select Install.

9. An installation or upgrade information dialog box and an End User License Agreement will open. Accept the agreement to proceed with the installation.

10. When the installation completes, select Close. The plugin is displayed in the Plugins pane. The Module Status column indicates the status of your license. See ForeScout Module License Requirements or the CounterACT Console User Manual for details on requesting a permanent license or a demo license extension.

11. Select the plugin and select Start. The Select Appliances dialog box opens.

12. Select the CounterACT devices on which to start the plugin.

13. Select OK. The plugin runs on the selected devices.

Configure the Module

Configure the module to import SCAP content so you can assess Windows endpoint compliance. Use the module configuration window to:

- Import SCAP Content
- View SCAP File Details
- View Benchmark Details
- Edit a Short Benchmark Title
- View OVAL Collection Details
- Edit an OVAL Collection Name
- Test the Endpoints
To configure the module:

1. In the CounterACT Console, select Options from the Tools menu. The Options pane opens.
2. Navigate to and select Advanced Compliance. The Advanced Compliance pane opens.

Import SCAP Content

For each profile imported to the CounterACT Advanced Compliance Module, one Profile Score Property and one Rule Results Property are automatically added to the list of available policy conditions. If a freestanding file of OVALs is imported, only the Rule Results Property is created.

CounterACT’s SCAP repository can contain up to 128 files at one time.

To import an SCAP source data stream, bundle, or OVAL collection:

1. In the SCAP Source Data tab, select Import. The Import SCAP File dialog box opens.
2. Browse to and select the SCAP source data stream or bundle to be imported, select **Import**, and select **OK**. XCCDF benchmark and OVAL details are imported into CounterACT.

3. Select **Close**. You are prompted to enter a short title for each benchmark included in the imported data stream or bundle.
   - If you import a benchmark with the same name as a benchmark that was previously imported into CounterACT, you are prompted to enter a different short name, to distinguish the two benchmarks.

4. Enter a short, unique, meaningful title so you can easily identify the benchmark.
   The imported SCAP file is added to the SCAP Source Data tab, and information is displayed in the Benchmarks and OVAL Collections tabs.

5. Select **Apply** and then select **Close** to save the module configuration changes.

### View SCAP File Details

You can view details of an imported SCAP file to ensure that it contains the specifications required.

**To view SCAP file details:**
1. In the SCAP Source Data tab, select the SCAP file name, and select **Details**. The following is displayed:
   - Details of the imported SCAP file
   - Details of the XCCDF benchmark(s), if applicable
   - Details of the OVAL collection

---

### View Benchmark Details

You can view details of the imported XCCDF benchmark profiles used for endpoint compliance scans.

**To view XCCDF benchmark details:**

1. In the Advanced Compliance pane, select the Benchmarks tab.
2. To view more benchmark details and the list of profiles included in the benchmark, select the benchmark of interest, and select **Details**. The following is displayed:
   - Details of the imported SCAP file that included the benchmark
   - Details of the benchmark
   - A list of the profiles included in the benchmark

3. To view more profile details, select the profile, and select **Details**. The following information is displayed:
   - Profile ID
   - Profile Title
   - Profile Description

4. Select **Close** to close the windows.

**Edit a Short Benchmark Title**

You can define a short, unique, meaningful title so you can easily identify the benchmark in CounterACT.

**To edit a short benchmark title:**
1. In the Benchmarks tab, select the benchmark ID, and select **Edit**. The Short Benchmark Title window opens.

2. Enter a short benchmark title, and select **OK**. The title may contain letters, numbers, a colon, a period, and spaces.

3. Select **Apply** and then select **Close** to save the module configuration changes.

**View OVAL Collection Details**

You can view details of the imported OVAL rules.

**To view OVAL collection details:**

1. In the Advanced Compliance pane, select the OVAL Collections tab.

2. To view more collection details and the list of OVAL rules included in the collection, select the collection, and select **Details**. The following is displayed:
   - Details of the imported SCAP file that included the OVAL collection
   - Details of the OVAL collection
   - A list of the rule definitions included in the OVAL collection
3. To view more information for a rule definition, select the definition, and select **Details**. The following OVAL rule information is displayed:

- Definition ID
- Class
- Title
- Reference ID
- Description
- Version

4. Select **Close** to close the windows.

**Edit an OVAL Collection Name**

You can define a short, unique, meaningful name so you can easily identify the OVAL collection in the OVAL Collections tab.

**To edit an OVAL collection name:**

1. In the OVAL Collections tab, select the collection, and select **Edit**. The OVAL Collection Name window opens.
2. Enter an OVAL collection name, and select **OK**.

3. Select **Apply** and then select **Close** to save the module configuration changes.

### Test the Endpoints

The test tab can be used for troubleshooting failed scans of endpoints, or to verify that an endpoint meets all the necessary requirements for a successful SCAP scan (for example, the endpoint is managed by the HPS Inspection Engine, has PowerShell installed, and can establish a TCP/IP connection to the Appliance).

In the Test tab, enter the IP addresses of endpoints you wish to test for Advanced Compliance module functionality. You can add a number of endpoints for testing, and save them in the Test tab list. The test runs on one selected endpoint at a time.

1. In the **Options > Advanced Compliance > Test** tab, select Add. The Edit SCAP Test Endpoint dialog box opens.
2. Enter the following information, and select OK to save the settings.

<table>
<thead>
<tr>
<th>IP Address</th>
<th>Enter the IP address of an endpoint you want to test.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>(Optional) - enter a name for the endpoint for easy reference.</td>
</tr>
</tbody>
</table>

3. In the Test tab, select Test. The test runs on the currently selected endpoint.

Run Advanced Compliance Policy Templates

This module provides the following policy template to detect, manage and remediate endpoints based on Advanced Compliance scan results.

- The Advanced Compliance Score policy template generates a policy that detects and manages endpoints based on the results of a compliance scan using a particular SCAP benchmark profile.

> It is recommended that you have a basic understanding of CounterACT policies before working with the templates. See the CounterACT Templates and Policy Management chapters of the Console User Guide.

SCAP Compliance Score Policy Template

Use this policy to evaluate an XCCDF profile on selected endpoints, and to apply management actions based on the resulting scan score.

Prerequisites

CounterACT runs scripts on endpoints to perform Advanced Compliance scans. Therefore, policies you create with this template are only relevant to endpoints that are managed by CounterACT using Remote Inspection or SecureConnector.

> This release of the module only supports Windows endpoints.

Run the Template

This section describes how to create a policy from the policy template. For details about how the policy works, see How Devices are Detected and Handled.
To run the template:

1. Log in to the CounterACT Console and select the Policy tab.
2. Select Add from the Policy Manager. The Policy Wizard opens.
3. Expand the Compliance folder and select SCAP Compliance Score. The SCAP Compliance Score pane opens.

4. Select Next. The Name page opens.

Name the Policy

The Name pane lets you define a unique policy name and useful policy description. Policy names appear in the Policy Manager, the Views pane, NAC Reports and in other features. Precise names make working with policies and reports more efficient.

1. Define a unique name for the policy you are creating based on this template, and enter a description.
Naming Tips

- Make sure names are accurate and clearly reflect what the policy does. For example, do not use a generic name such as My_Compliance_Policy.
- Use a descriptive name that indicates what your policy is verifying and which actions will be taken.
- Ensure that the name indicates whether the policy criteria must be met or not met.
- Avoid having another policy with a similar name.

2. Select Next. The Groups pane opens.

If you have created a Managed Windows Devices group, the Groups pane is not displayed in the Policy Wizard.

Select a Group

The Groups pane lets you select the group used to filter results. Only managed Windows endpoints should be included in this policy.

1. Select a group that contains your managed Windows endpoints from the list, or select Continue Without the group.

2. Select Next. The Scope pane and IP Address Range dialog box opens.

Define which Hosts will be Inspected - Policy Scope

The Scope pane and IP Address Range dialog box let you define a range of endpoints to be inspected for this policy.
1. Use the IP Address Range dialog box to define which endpoints are inspected. The following options are available for defining a scope:

   - **All IPs**: Include all addresses in the Internal Network. The Internal Network was defined when CounterACT was set up.
   - **Segment**: Select a previously defined segment of the network. To specify multiple segments, select OK to close the IP Address Range dialog box, and select Segments from the Scope page.
   - **IP Range**: Define a range of IP addresses. These addresses must be within the Internal Network.
   - **Unknown IP addresses**: Apply the policy to endpoints whose IP addresses are not known. Endpoint detection is based on the endpoint MAC address. Not applicable for this policy template.

   *Filter the range by including only certain CounterACT groups and/or by excluding certain endpoints or users or groups when using this policy.*

2. Select OK. The added range appears in the Scope pane.

3. Select Next. The SCAP Profile pane opens.

**Select a SCAP Profile to Evaluate on Endpoints - SCAP Profile**

The SCAP Profile page lets you specify the XCCDF profile that is evaluated on endpoints within the policy scope.

Before you use this page to select an XCCDF benchmark or its profiles, you must first import the corresponding XCCDF benchmark into CounterACT. The drop-downs of this page only list benchmarks that were previously imported into CounterACT.
1. In the **Short Benchmark Title** drop-down, select a benchmark. Use the full name of the benchmark in the **Benchmark Title** field to confirm your selection.

2. The **Profile Title** drop-down lists the profiles contained in the selected benchmark file. Select the profile that this policy evaluates on endpoints in its scope.

3. Select **Next**. The Main Rule pane opens.

**Refine Endpoint Scope - Main Rule**

Use this pane to define the Main Rule for the policy. Only endpoints that match the conditions of this rule are evaluated by sub-rules of the policy. Use the Main Rule to:

- **Modify policy scope**: Specify conditions, but no actions, to further narrow the selection of endpoints that are passed to sub-rules.

  For example, you can use Main Rule conditions to select endpoints whose type, configuration, or installed applications qualify them for the Advanced Compliance scan implemented by the policy.

- **Prepare endpoints for evaluation by sub-rules**: Actions you specify here are applied to each endpoint that matches the rule, before it is evaluated by sub-rules of the policy. Use this rule to check for pre-requisites required by endpoint evaluation or remediation actions.

  For example, you can use the Main Rule to detect endpoints with PowerShell and other endpoint requirements, and perform additional preparation steps such as updating the Windows version running on the endpoint.
Select **Next**. The Sub-Rules pane opens.

**Evaluate and Remediate Endpoints - Sub-Rules**

Use this pane to review the default set of sub-rules that manage/remediate endpoints based on the results of the specified compliance scan. For a description of the default rules of the template, see **How Devices are Detected and Handled**.

1. Select **Finish**. The policy is created.
2. Select **Apply** to save the policy in the Policy Manager.
How Devices are Detected and Handled

This section describes the main rule and sub-rules of the policy created by this policy template. Policy rules instruct CounterACT how to detect and handled endpoints included in the policy scope.

Endpoints that match the Main Rule are included in the next stage of policy evaluation, and are inspected by sub-rules of the policy. *Endpoints that do not match the Main Rule are not passed to sub-rules; policy evaluation ends for these endpoints at this point.*

Sub-rules are evaluated in order until a match is found. If the host does not match the conditions of the sub-rule, it is evaluated by the next rule. When an endpoint matches the conditions of a rule, the corresponding action is applied to the host.

Main Rule

By default, the main rule of this policy filters endpoints according to the group Managed Windows Devices, and it specifies recheck behavior for the policy. By default, the policy is evaluated once a week, and is applied to newly discovered endpoints.

Sub-Rules

Sub-rules of the policy detect endpoints based on the **Profile Score Property** corresponding to the profile that is evaluated by the policy. You can use each rule to apply remediation actions relevant to a different range of scores.

For these sub-rule conditions:
- The score is calculated using the Default option of the Scoring Model field.
- The matching score range is expressed as a percentage in the Score Percentage field.

By default, the actions in the template are disabled. These are examples of the type of action that may be appropriate for each range of scores.

1. This rule detects endpoints for which the profile scan scored 90-100 percent.
2. This rule detects endpoints for which the profile scan scored 80-90 percent.
3. This rule detects endpoints for which the profile scan scored 70-80 percent.
   Endpoints that match one of these rules are considered compliant with the profile, and no remedial action is applied to them.
4. This rule detects endpoints for which the profile scan scored below 70 percent.
   An optional Advanced Compliance Send Report action (disabled by default) generates an HTML report containing scan results for the endpoint. The action emails the report file to an administrator.
5. This rule detects endpoints for which the profile scan score could not be resolved. Endpoints matching this rule are rechecked once a day.
   An optional Send Email action (disabled by default) sends an email alert to an administrator.

Create Custom Advanced Compliance Policies

Custom CounterACT policy tools provide you with an extensive range of options for detecting and handling endpoints. Specifically, you can use the policy to instruct CounterACT to apply a policy action to endpoints that do or do not match property values defined in policy conditions.

Properties
CounterACT policy properties let you instruct CounterACT to detect hosts with specific attributes. For example, create a policy that instructs CounterACT to detect hosts running a certain Operating System or having a certain application installed.

Actions
CounterACT policy actions let you instruct CounterACT how to control detected devices. For example, assign a detected device to an isolated VLAN or send the device user or IT team an email.

In addition to the bundled CounterACT properties and actions available for detecting and handling endpoints, you can work with Advanced Compliance related properties and actions to create the custom policies. These items are available when you install and configure the module. For more information about working with policies, select Help from the policy wizard.
To create a custom policy:
1. Log in to the CounterACT Console.
2. On the Console toolbar, select the Policy tab. The Policy Manager opens.
3. Select Add to create a policy. The Policy Wizard opens.
4. In the Templates tree, select Custom.

Detecting Compliance – Policy Properties

For each profile in the benchmark imported to the CounterACT Advanced Compliance Module, one Profile Score Property and one Rule Results Property are added to the list of available conditions. If a freestanding file of OVALs is imported, only the Rule Results Property is created.

When an endpoint is evaluated in a policy rule that uses one of these properties, a compliance scan for that profile is initiated. You can create policies that use the SCAP profile compliance score or OVAL rule results to trigger actions on relevant endpoints.

To access Advanced Compliance properties:
1. Navigate to the Properties tree from the Policy Conditions dialog box.
2. Do one of the following:
   - For a benchmark profile, expand the Compliance folder in the Properties tree that corresponds to the benchmark short name.
   - For a freestanding OVAL collection, expand the Compliance > Independent OVAL Collection folder, and select the Rule Result property corresponding to the collection.
Profile Score Property

This property indicates the latest score of the profile scan. When an endpoint falls within the scope of a policy that uses this property, and its most recent scan results are older than the policy recheck interval, an endpoint scan for the profile is initiated. The name and description of the profile used for the scan is displayed at the top of the window.
Scoring Model | The model used for computing the profile score:
---|---
Absolute: | - 1 indicates that all checked OVAL rules passed.
- 0 indicates that not all checked OVAL rules passed.
Default: | The result is the normalized weighted sum for all checked rules, taking into account rule grouping relationships as per the SCAP standard.
Flat: | The result is the sum of the weights assigned to each OVAL rule that passed, and the maximum score is the sum of the weights of all checked rules.
Flat Unweighted: | Each rule has a weight of 1. The result is the number of OVAL rules that passed, and the maximum score is the number of rules checked.

For more information about these scoring models, see Specification for the Extensible Configuration Checklist Description Format (XCCDF).

Score | The profile scan score computed using the selected scoring model. This value is relative to the Maximum Score calculated for the endpoint.

Maximum Score | The theoretical maximum score if the endpoint passed/satisfied all rules in the profile that are applicable to the endpoint. CounterACT calculates this value as part of profile evaluation on each endpoint, using the selected scoring model.

Select this option if you want to define a condition that matches the Maximum Score calculated for each endpoint.

- OVAL rules with the following results are not factored into the maximum score:
  - Informational
  - Not Applicable
  - Not Checked
  - Not Selected

Score Percentage | Select this option to specify a matching condition that expresses the score for the endpoint as a percentage of the theoretical maximum score for the profile.

Rule Results Property

This property indicates the result of all OVAL rule evaluations for the corresponding profile. When an endpoint falls within the scope of a policy that uses this property, and its most recent scan results are older than the policy recheck interval, an endpoint scan for the profile is initiated. The name and description of the profile used for the scan is displayed at the top of the window.
**Definition ID**
The Definition ID of the OVAL rule(s) evaluated.

**Rule Evaluation Results**
The result of the OVAL rule evaluation:
- **Error:** An error occurred during the rule evaluation. For example, the scan was run with insufficient privileges.
- **Fail:** The rule was not satisfied.
- **Fixed:** The endpoint was remediated to satisfy the rule that had previously failed.
- **Informational:** The rule is not a test for compliance.
- **Not Applicable:** The rule is not applicable to this endpoint. For example, a rule relevant to a Windows 7 platform only is not applicable to a Windows 10 machine.
- **Not Checked:** The rule was not checked. For example, its language is not supported by the checking engine, or it depends on a parent rule that did not pass.
- **Not Selected:** The rule is not selected for evaluation in this profile.
- **Pass:** The rule was satisfied.
- **Unknown:** Unable to determine if the rule was satisfied.

A rule is considered satisfied if the result of the evaluation is either Pass or Fixed.

When you use this property to define a policy condition, use the following procedure to select the OVAL rule definitions you want to evaluate.

**To create a policy condition that evaluates OVAL rules:**

1. In the Properties tree, select the **Rule Results** property corresponding to the collection of OVAL rules you want to use.
2. Select the **Definition ID** checkbox.
3. Initially, the table in the Definition ID area is empty. Select Add. A dialog box lists OVAL rules in the collection.

4. Select the rule(s) you want to evaluate. Then select OK. The selected rule(s) appear in the Definition ID table.

5. Specify the values that you want to match in the Rule Evaluation Results field.

6. Select OK to save the condition.

When you create a condition that evaluates more than one rule:

- Use the For one or more property values option to return a positive match if any of the selected OVAL rules evaluates to any of the specified Rule Evaluation Results values.
- Use the For all property values option to return a positive match if all of the OVAL rules in the profile have been selected and they all match any of the specified Rule Evaluation Results values.

Managing Advanced Compliance Results – Policy Action

This section describes the action that is made available when the Advanced Compliance Module is installed.

To access the SCAP action:

1. Navigate to the Actions tree from the Policy Actions dialog box.

2. Expand the SCAP folder in the Actions tree.
3. The following action is available:
   - Email Compliance Report Action

**Email Compliance Report Action**

Use the *Email Compliance Report* action in CounterACT policies to email a report of Advanced Compliance results in either HTML or XML format.

<table>
<thead>
<tr>
<th><strong>Email</strong></th>
<th>The email address to which the Advanced Compliance results are sent. If no address is provided, the mail is sent to the CounterACT administrator address.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Attachment Type</strong></td>
<td>The format of the attachment:</td>
</tr>
<tr>
<td></td>
<td>- HTML: Results are written in an easy-to-read report.</td>
</tr>
<tr>
<td></td>
<td>- XML: Results are written as an ARF-compatible XCCDF data stream.</td>
</tr>
<tr>
<td><strong>Compress Attachment (.ZIP)</strong></td>
<td>The attachment is compressed and sent as a .ZIP file.</td>
</tr>
<tr>
<td><strong>Short Benchmark Title</strong></td>
<td>The user-defined title of the benchmark used for the scan.</td>
</tr>
<tr>
<td><strong>Benchmark Title</strong></td>
<td>The title of the benchmark used for the scan.</td>
</tr>
<tr>
<td><strong>Profile Title</strong></td>
<td>The title of the benchmark profile used for the scan.</td>
</tr>
</tbody>
</table>

**Display Advanced Compliance Inventory Information**

Use the CounterACT Inventory to view a real-time display of benchmark scores and OVAL checks.

**To access the inventory:**

1. Select the **Inventory** icon from the Console toolbar.
2. Navigate to the Advanced Compliance benchmark entries, expand the appropriate benchmark title, and select the **Rule Results** or **Profile Score** property for the appropriate profile title.

![CounterACT Console User Interface](image)

Refer to *Working at the Console > Working with Inventory Detections* in the *CounterACT Console User Manual* or the Console online help for information about how to work with the CounterACT Inventory. For a description of the inventory fields, see:

- **Profile Score Property**
- **Rule Results Property**

### Generate Advanced Compliance Evaluation Reports

The **SCAP ARF Report** template, which is available in the CounterACT Reports Portal, allows you to create reports that list the most recent results of a specific SCAP profile evaluation on selected endpoints.

The structure and content of these reports follow the Asset Reporting Format (ARF) data model, a standard for compiling IT asset information which is a component of SCAP. The information compiled using the ARF standard can be easily shared with third-party systems.

The reports are XML formatted, and are delivered in a ZIP archive to a remote server specified by the user (via FTP, SFTP, or SCP). The Reports portal allows you run reports on demand, or configure periodic generation of reports.

### Create an SCAP ARF Report

Many of the configuration choices in the report template correspond to choices in the **SCAP Compliance Score Policy Template** provided by the module. For example, you define the scope of endpoints included in the report and specify the SCAP benchmark and profile for which evaluation results are reported.
The email sent by the Reports portal does not contain report output files, it only contains the pathname of the report on the server upon which report files are placed.

To create an ARF Report:

1. In the CounterACT Console toolbar, select the Reports Portal icon.


4. In the Header section:
− In the **Name** field, enter a report name (*required*). Maximum length is 60 characters. The following characters cannot be used in this field:
  & # : / ' ` "
− In the **Description** field, enter descriptive text (*optional*).
− In the **Generated by** field, enter the name of the CounterACT user generating or associated with the report (*optional*). Maximum length is 60 characters.

When an ARF report is generated, the information defined in the **Header** section is not included in the report, as it is not part of the ARF data model standard. The sole purpose of the information in these fields is to support the user of the ARF Report template.

5. In the **Scope** section, select either all IPs, a host IP range or the network IP segments for which to create the report.

![Scope Section](image)

6. In the **Include > Benchmark Selection** section, select the Short Benchmark Title and Profile Title used for this report.

![Include Section](image)

7. In the **File Transfer Parameters** section, provide the following details that are used to transfer the generated ARF report to a remote server:
Protocol to Transfer File: Select the protocol used to transfer the file containing the generated ARF report.

Destination Server: Enter the server to which the file will be transferred. Enter a server IP address, server FQDN, or server name.

Port: Enter the port number to connect to on the remote server. The default port of the selected transfer protocol automatically appears in this field.

Username: Enter the username for logging in to the remote server.

Password: Enter the password for logging in to the remote server.

Verify Password: Verify the specified password by re-entering it.

Directory to Receive File: Specify the directory to receive the transferred file.

When transferred by the SCP protocol, any spaces in the saved file name are converted to underscore characters.

8. In the File Transfer Parameters section, select Test File Transfer to execute a file transfer test based on the information you defined.

9. In the Schedule section, define a report generation schedule (optional).

Define a schedule to generate either a daily recurring report (Daily At <time of day>) or a day of week recurring report (Every <day of week> At <time of day>).
− In the **Send Report to** field, enter an email address to send a notification of the generated report to. You may enter multiple email addresses, separating them with commas.

**10.** Perform either of the following:
− Select **Run** to generate a report using the defined report template.
− Select **Save** to save the defined report template for later use.

The defined report template is saved and appears in the **My Reports** table on the **Reports Portal** home page.

---

### Additional CounterACT Documentation

For more detailed information about the CounterACT features described here or additional CounterACT features and modules, refer to the following resources:

- [Documentation Portal](#)
- [Customer Support Portal](#)
- [CounterACT Console Online Help Tools](#)

### Documentation Portal

The ForeScout Documentation Portal is a Web-based library containing information about CounterACT tools, features and functionality and integrations.

![ForeScout Documentation Portal](image)

**To access the Documentation Portal:**
2. Use your customer support credentials to log in.
3. Select the CounterACT version you want to discover.

Customer Support Portal

The Customer Support Portal provides links to CounterACT version releases, service packs, plugins and modules as well as related documentation. The portal also provides a variety of How-to Guides, Installation Guides and more.

To access the Customer Support Portal:
2. Select the CounterACT version you want to discover.

CounterACT Console Online Help Tools

Access information directly from the CounterACT Console.

Console Help Buttons
Use context sensitive Help buttons to quickly access information about the tasks and topics you are working with.

Console User Manual
Select CounterACT Help from the Help menu.

Plugin Help files
1. After the plugin is installed, select Options from the Tools menu and then select Plugins.
2. Select the plugin and then select Help.

Documentation Portal
Select Documentation Portal from the Help menu.

Appendix A: Executable Files Used by the Module

The following executable file is run on endpoints during Advanced Compliance scans. Refer to the Advanced Compliance Module Release Notes for information regarding changes made to these files.

<table>
<thead>
<tr>
<th>EXE files</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>processproxy.exe</td>
<td>Client process that performs SCAP content OVAL checks on the endpoint and reports the results over port 10008 using a</td>
</tr>
</tbody>
</table>
secured TCP connection to the managing CounterACT Appliance.
Legal Notice

Copyright © ForeScout Technologies, Inc. 2000-2017. All rights reserved. The copyright and proprietary rights in this document belong to ForeScout Technologies, Inc. ("ForeScout"). It is strictly forbidden to copy, duplicate, sell, lend or otherwise use this document in any way, shape or form without the prior written consent of ForeScout. All other trademarks used in this document are the property of their respective owners.

These products are based on software developed by ForeScout. The products described in this document may be protected by one or more of the following U.S. patents: #6,363,489, #8,254,286, #8,590,004, #8,639,800 and #9,027,079 and may be protected by other U.S. patents and foreign patents.

Redistribution and use in source and binary forms are permitted, provided that the above copyright notice and this paragraph are duplicated in all such forms and that any documentation, advertising materials and other materials related to such distribution and use acknowledge that the software was developed by ForeScout.

Unless there is a valid written agreement signed by you and ForeScout that governs the below ForeScout products and services:

- If you have purchased any ForeScout products, your use of such products is subject to your acceptance of the terms set forth at http://www.forescout.com/eula/;
- If you have purchased any ForeScout support service ("ActiveCare"), your use of ActiveCare is subject to your acceptance of the terms set forth at http://www.forescout.com/activecare-maintenance-and-support-policy/;
- If you have purchased any ForeScout Professional Services, the provision of such services is subject to your acceptance of the terms set forth at http://www.forescout.com/professional-services-agreement/;
- If you are evaluating ForeScout’s products, your evaluation is subject to your acceptance of the applicable terms set forth below:
  - If you have requested a General Availability Product, the terms applicable to your use of such product are set forth at: http://www.forescout.com/evaluation-license/.
  - If you have requested a Beta Product, the terms applicable to your use of such product are set forth at: http://www.forescout.com/beta-test-agreement/.
  - If you have purchased any ForeScout Not For Resale licenses, such license is subject to your acceptance of the terms set forth at http://www.forescout.com/nfr-license/.

Send comments and questions about this document to: documentation@forescout.com

2017-03-08 17:45