



ForeScout

eyeExtend for Advanced Compliance

Configuration Guide

Versions 1.3.1 and 1.3.2



Contact Information

Forescout Technologies, Inc.

190 West Tasman Drive

San Jose, CA 95134 USA

<https://www.Forescout.com/support/>

Toll-Free (US): 1.866.377.8771

Tel (Intl): 1.408.213.3191

Support: 1.708.237.6591

About the Documentation

- Refer to the Technical Documentation page on the Forescout website for additional documentation: <https://www.Forescout.com/company/technical-documentation/>
- Have feedback or questions? Write to us at documentation@forescout.com

Legal Notice

© 2020 Forescout Technologies, Inc. All rights reserved. Forescout Technologies, Inc. is a Delaware corporation. A list of our trademarks and patents can be found at <https://www.Forescout.com/company/legal/intellectual-property-patents-trademarks>. Other brands, products, or service names may be trademarks or service marks of their respective owners.

2020-08-27 14:48

Table of Contents

About Advanced Compliance Integration	4
About eyeExtend for Advanced Compliance Module	6
How to Work with eyeExtend for Advanced Compliance.....	8
Install eyeExtend for Advanced Compliance Module	14
Configure eyeExtend for Advanced Compliance Module	15
Import SCAP Content.....	15
View SCAP File Details	17
View Benchmark Details	18
Edit a Short Benchmark Title	19
View OVAL Collection Details.....	19
Edit an OVAL Collection Name	21
Test Advanced Compliance Endpoints.....	22
Edit IP Address of an Endpoint	23
Run Advanced Compliance Policy Templates	24
SCAP Compliance Score Policy Template.....	24
Create Custom Advanced Compliance Policies	30
Detect Compliance – Policy Properties	31
Manage Advanced Compliance Results – Policy Action	36
Display Advanced Compliance Inventory Information.....	37
Generate Advanced Compliance Evaluation Reports.....	37
Appendix A: Executable Files Used by the Module	43

About Advanced Compliance Integration

The Forescout eyeExtend for Advanced Compliance integration greatly simplifies the effort required to enforce compliance on network endpoints by automating compliance scanning and reporting. Security Content Automation Protocol (SCAP) content is downloaded from known public repositories and then uploaded to the Forescout platform. The Forescout platform 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. The Forescout platform uses the scan results to identify device compliance based on customizable thresholds. Forescout platform 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.

Supported Forescout Platform Version

The following table lists the Forescout platform version that works with each version covered by this guide.

Version	Forescout Platform Version
1.3.1	8.1 and 8.2
1.3.2	8.1 and 8.2

About Certification Compliance Mode

Forescout eyeExtend for Advanced Compliance supports Certification Compliance mode. For information about this mode, refer to [Certification Compliance](#) in the *Forescout Installation Guide*.

Use Cases

This section describes important use cases supported by Forescout eyeExtend for Advanced Compliance. To understand how this module helps you achieve these goals, see [About eyeExtend for Advanced Compliance 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 that fails to meet a defined compliance level for any given SCAP Compliance benchmark.
- Quarantine all endpoints that fall below a minimum compliance level.


XCCDF Scan Results

Scan Date	Started 20 Mar 2016 at 23:01:35 and completed 20 Mar 2016 at 23:18:30
Benchmark	USGCB: Guidance for Securing Microsoft Windows 7 Systems version v1.2.3.1 xccdf_gov.nist_benchmark_USGCB-Windows-7
Profile	United States Government Configuration Baseline 1.2.3.1 xccdf_gov.nist_profile_united_states_government_configuration_baseline_version_1.2.3.1
Target	192.168.1.100 - 192.168.1.101 - 192.168.1.102 - 192.168.1.103 - 192.168.1.104 - 192.168.1.105 - 192.168.1.106 - 192.168.1.107 - 192.168.1.108 - 192.168.1.109 - 192.168.1.110
Identity	192.168.1.100 - 192.168.1.101 - 192.168.1.102 - 192.168.1.103 - 192.168.1.104 - 192.168.1.105 - 192.168.1.106 - 192.168.1.107 - 192.168.1.108 - 192.168.1.109 - 192.168.1.110 authenticated, privileged
System	CounterACT SCAP Plugin 1.1.0

Scoring

Method	Score	Max	%
Default Scoring	10.90	100.00	10.90%
Flat Scoring	770.00	2,500.00	30.80%
Flat Unweighted Scoring	77.00	250.00	30.80%
Absolute Scoring	0.00	1.00	0.00%

Rule Results Summary



Method	Score	Max	%
Default Scoring	10.90	100.00	10.90%
Flat Scoring	770.00	2,500.00	30.80%
Flat Unweighted Scoring	77.00	250.00	30.80%
Absolute Scoring	0.00	1.00	0.00%

Rule Results

Rule	Reference(s)	Result
USGCB Security Settings » Account Policies Group » Account Lockout Policy Settings		
Account Lockout Duration	CCE-9308-8	PASS
Account Lockout Threshold	CCE-9136-3	FAIL
Reset Account Lockout Counter After	CCE-9400-3	PASS
USGCB Security Settings » Account Policies Group » Password Policy Settings		
Enforce Password History	CCE-8912-8	FAIL

Enforce Password History Result Diagnostics

This setting determines how many old passwords the system will remember for each account. Users will be prevented from reusing any of the old passwords. For example, if this is set to 24, then the system will not allow users to reuse any of their last 24 passwords. Old passwords may have been compromised, or an attacker may have taken a long time to crack encrypted passwords. Reusing an old password could inadvertently give attackers access to the system.

Result Component Logic

ALL OF

ALL OF Extend Definition: Windows 7 is installed

OVAL TEST: The installed operating system is part of the Microsoft Windows family

OVAL TEST: Windows 7 is installed

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.

Scoring Model	Score	Maximum Score	Lists	No. of Hosts	Last Update	Last Host
Default	0.0	100.0		1	8/11/17 2:07:19 AM	10.43.3.89
Compliance: USGCB: Guidance for Securing Microsoft	10.895139092217	100.0		3	8/13/17 3:17:47 PM	10.44.2.116
Default	11.443384706252	100.0		2	8/13/17 1:44:08 PM	10.41.1.238

Host	Host IP	Segment	MAC Addr...	Comment	Display N...	Switch IP ...	Switch Po...	Switch Po...	Function	Actions
WORKGRO...	10.44.2.116	PM Network	34363b5f92...						Protocol ban	

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 Forescout eyeExtend for Advanced Compliance 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 the Forescout platform 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:

<http://csrc.nist.gov/publications/nistpubs/800-126/sp800-126.pdf>

For more information about SCAP 1.1, refer to:

<http://csrc.nist.gov/publications/nistpubs/800-126-rev1/SP800-126r1.pdf>

For more information about SCAP 1.2, refer to:

<http://csrc.nist.gov/publications/nistpubs/800-126-rev2/SP800-126r2.pdf>

About eyeExtend for Advanced Compliance Module

Forescout eyeExtend for Advanced Compliance 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 Forescout eyeExtend for Advanced Compliance 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 Forescout platform 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 Asset Inventory.
- 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 Forescout platform 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, the Forescout platform 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.

How to Work with eyeExtend for Advanced Compliance

This topic describes how to work with the module and module requirements.

What to Do

This section lists the steps you should take to set up your system when working with Forescout eyeExtend for Advanced Compliance:

1. Verify that you have met system requirements. See [Requirements](#).
2. [Install eyeExtend for Advanced Compliance Module](#).
3. [Run Advanced Compliance Policy Templates](#).
4. [Create Custom Advanced Compliance Policies](#).

Requirements

This section describes system requirements, including:

- [Forescout Requirements](#)
- [Endpoint Requirements](#)
- [Networking Requirements](#)
- [Endpoint Access and Advanced Compliance](#)
- [Third-Party Requirements](#)
- [Supported SCAP Content](#)
- [Forescout eyeExtend \(Extended Module\) Licensing Requirements](#)

Forescout Requirements

The module requires the following Forescout releases and other components.

- Endpoint Module with the HPS Inspection Engine running.
- A module license for the Endpoint Module. See [Forescout eyeExtend \(Extended Module\) Licensing Requirements](#) for details.

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

Endpoint Access and Advanced Compliance

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

The Forescout platform 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. The Forescout platform does not install any applications on the endpoint.
- SecureConnector is a small-footprint executable that runs on the endpoint. It reports endpoint information to the Forescout platform and runs scripts.

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


The methods used by the Forescout platform 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.

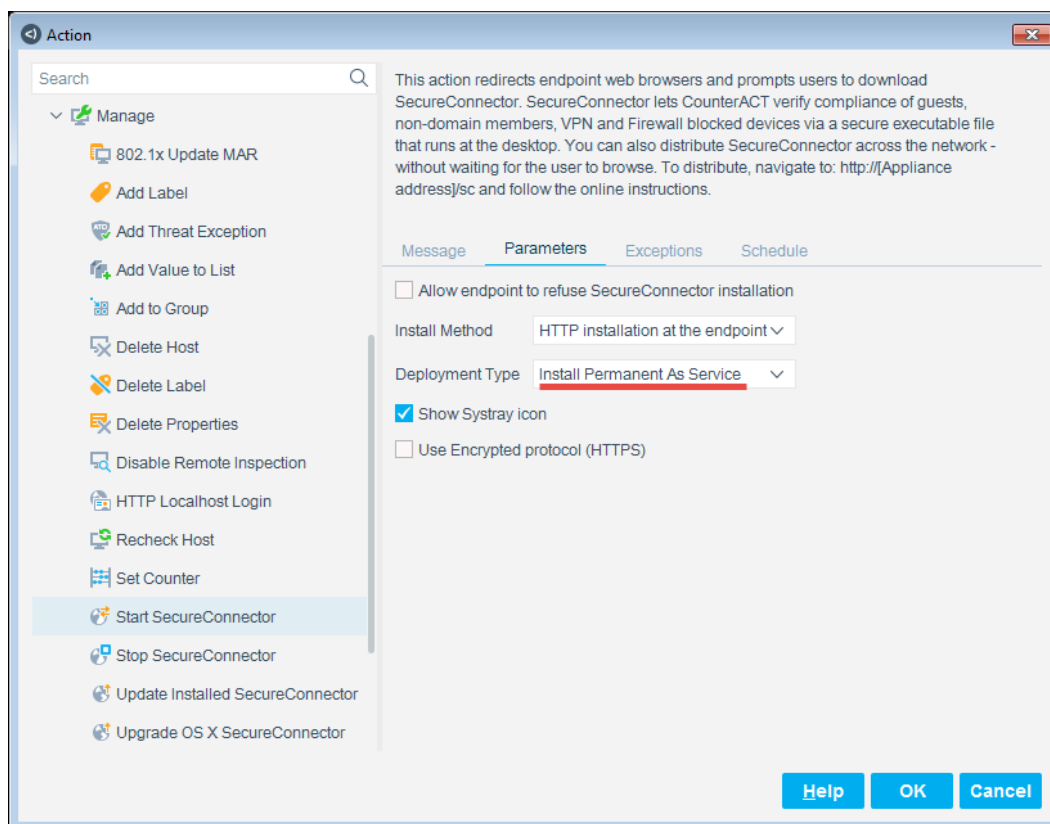
Similarly, when Windows endpoints are managed using Remote Inspection:

- 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.

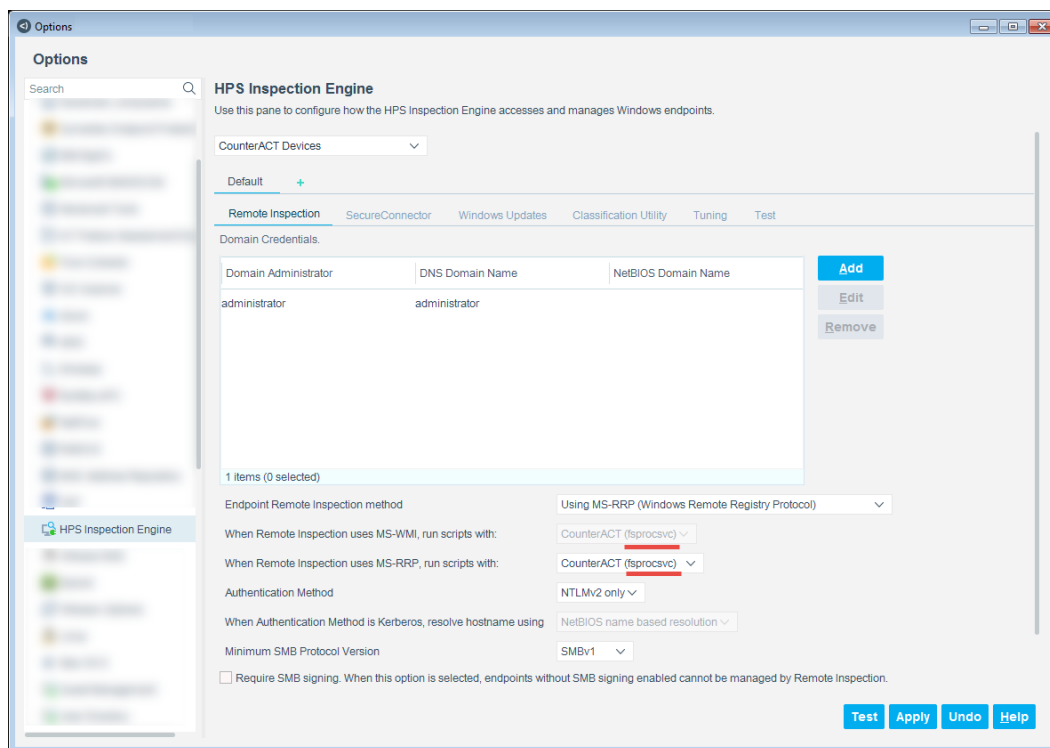
 *WMI security features prevent remotely run scripts from establishing connections with other machines on the network. Therefore, when Remote Inspection is configured to run scripts with WMI only, the Forescout platform evaluation of any OVAL rule that establishes a connection with another endpoint on 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. For more information about Remote Inspection, SecureConnector, and the user credentials with which the Forescout platform runs scripts on endpoints, refer to the [Forescout Endpoint Module: HPS Inspection Engine Configuration Guide](#).

Third-Party Requirements

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

- http://usgcb.nist.gov/usgcb/microsoft_content.html
- <http://iase.disa.mil/stigs/scap/Pages/index.aspx>
- <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 Open Checklist Interactive Language (OCIL) content, commonly used for manual SCAP security checks.*

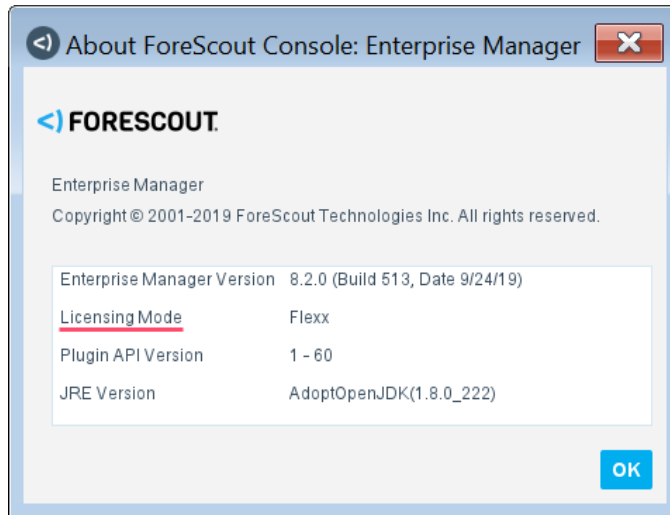
Forescout eyeExtend (Extended Module) Licensing Requirements

This Forescout eyeExtend module requires a valid license. Licensing requirements differ based on which licensing mode your deployment is operating in:

- [Per-Appliance Licensing Mode](#)
- [Flexx Licensing Mode](#)

To identify your licensing mode:

- From the Console, select **Help > About Forescout**.




Per-Appliance Licensing Mode

When installing the module, you are provided with a 90-day demo 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.

To continue working with the module after the demo period expires, you must purchase a permanent module license.

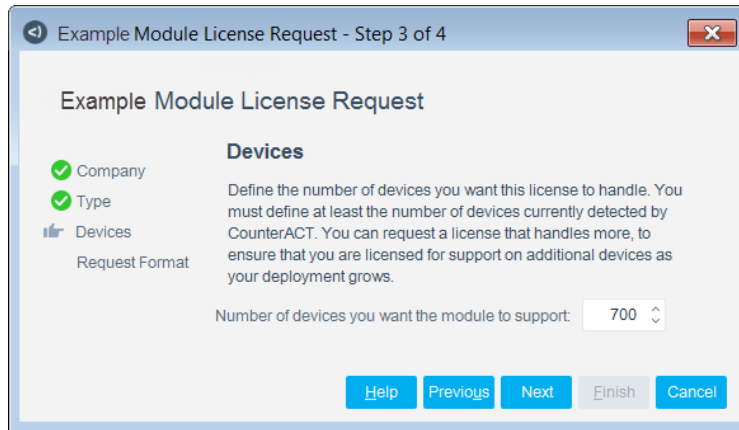
Demo license extension requests and permanent license requests are made from the Console.

 *This module may have been previously packaged as a component of an Integration Module which contained additional modules. If you already installed this module as a component of an Integration Module, you can continue to use it as such. Refer to the section about module packaging in the Forescout Administration Guide for more information.*

Requesting a License

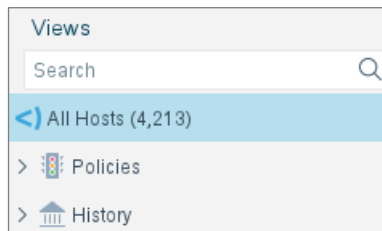
When requesting a demo license extension or permanent license, you are asked to provide the device *capacity* requirements. This is the number of devices that you want this license to handle. You must define at least the number of devices currently detected by the Forescout platform. You can request 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 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.




Flexx Licensing Mode

When you set up your Forescout deployment, you must activate a license file containing valid licenses for each feature you want to work with in your deployment, including eyeExtend modules. After the initial license file has been activated, you can update the file to add additional eyeExtend licenses or change endpoint capacity for existing eyeExtend modules. For more information on obtaining eyeExtend licenses, contact your Forescout sales representative.

 *No demo license is automatically installed during system installation.*

License entitlements are managed in the [Forescout Customer Portal](#). After an entitlement has been allocated to a deployment, you can activate or update the relevant licenses for the deployment in the Console.

Each eyeExtend license has an associated capacity, indicating the number of endpoints the license can handle. The capacity of each eyeExtend license varies by module but does not exceed the capacity of the Forescout eyeSight license.

 *Integration Modules, which package together groups of related licensed modules, are not supported when operating in Flexx Licensing Mode. Only eyeExtend modules, packaging individual licensed modules are supported. The eyeExtend Connect Module is an eyeExtend module even though it packages more than one module.*

More License Information

For more information on eyeExtend (Extended Module) licenses:

- **Per-Appliance Licensing.** Refer to the *Forescout Administration Guide*.
- **Flexx Licensing.** Refer to the *Flexx Licensing How-to Guide*.

You can also contact your Forescout sales representative for more information.

Install eyeExtend for Advanced Compliance Module


This topic describes how to download and install the module.


To install the module:

1. Navigate to one of the following Forescout download portals, depending on the licensing mode your deployment is using:
 - [Product Updates Portal](#) - **Per-Appliance Licensing Mode**
 - [Customer Portal, Downloads Page](#) - **Flexx Licensing Mode**

To identify your licensing mode, select **Help > About ForeScout** from the Console.

2. Download the module `.fpi` file.
3. Save the file to the machine where the Console is installed.
4. Log into the Console and select **Options** from the **Tools** menu.
5. Select **Modules**. The Modules pane opens.
6. Select **Install**. The Open dialog box opens.
7. Browse to and select the saved module `.fpi` file.
8. Select **Install**. The Installation screen opens.
9. Select **I agree to the License Agreement** to confirm that you have read and agree to the terms of the License Agreement and select **Install**. The installation cannot proceed unless you agree to the license agreement.

 *The installation begins immediately after selecting Install and cannot be interrupted or canceled.*

 *In modules that contain more than one component, the installation proceeds automatically one component at a time.*

10. When the installation completes, select **Close** to close the window. The installed module is displayed in the Modules pane.

 *Some components are not automatically started following installation.*

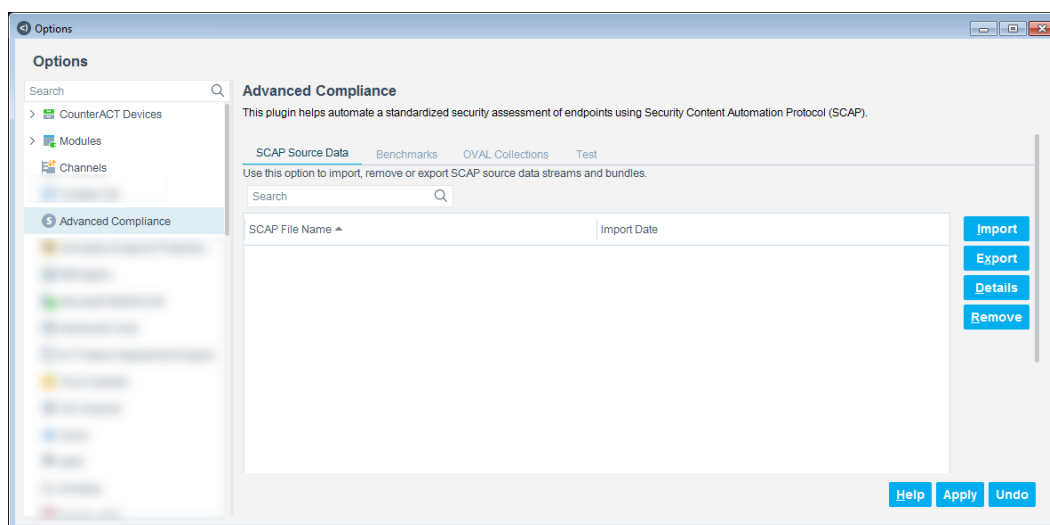
Configure eyeExtend for Advanced Compliance Module

Configure the module to import SCAP content so you can assess Windows endpoint compliance. Use module configuration 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 Advanced Compliance Endpoints](#)
- [Edit IP Address of an Endpoint](#)


To configure the module:

1. In the Console, select **Options** from the **Tools** menu. The Options pane opens.
2. Select **Advanced Compliance**.



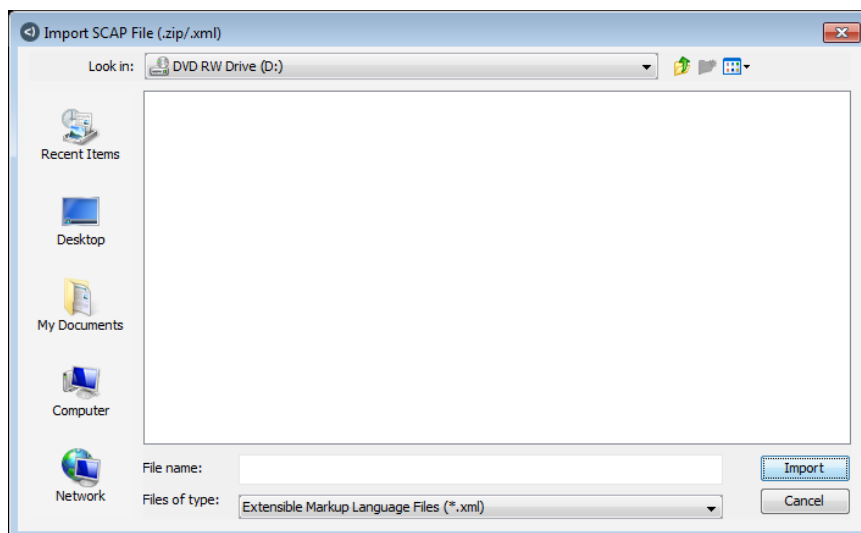
Import SCAP Content

For each profile imported to Forescout eyeExtend for Advanced Compliance, 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.

 *The Forescout platform's SCAP repository can contain up to 128 files at one time.*

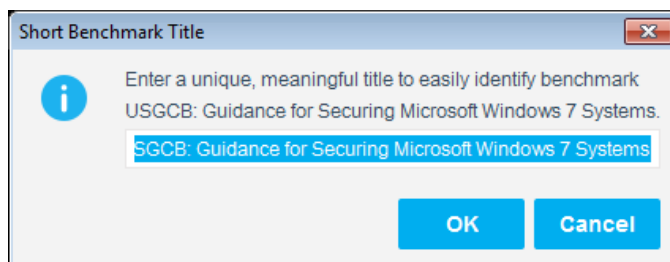
To import an SCAP source data stream, bundle, or OVAL collection:

1. In the SCAP Source Data tab, select **Import**.



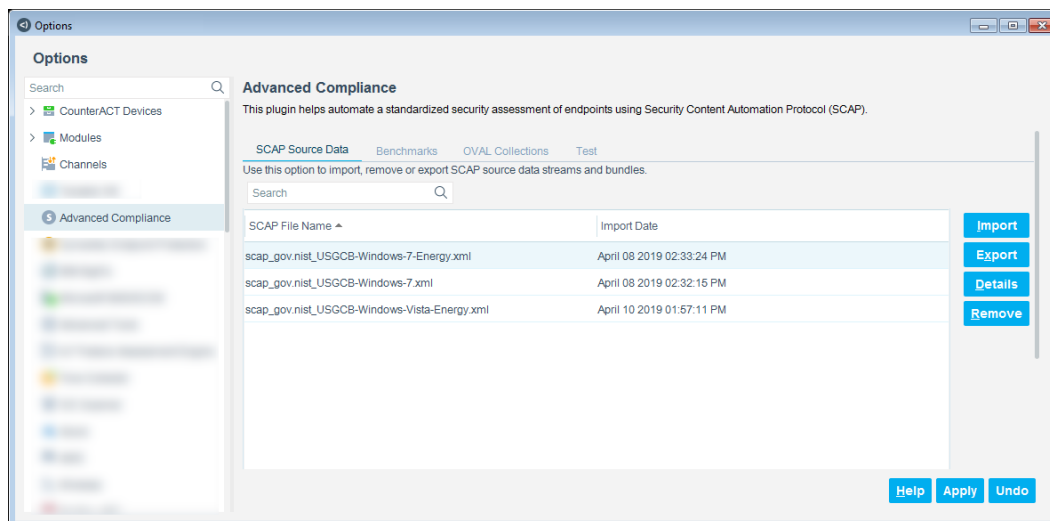
2. Browse to and select the SCAP source data stream or bundle to be imported. From the Files of type menu, select either .xml or .zip. Then select **Import**, and select **OK**. XCCDF benchmark and OVAL details are imported into the Forescout platform.
3. Select **Close**. You are prompted to enter a 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 the Forescout platform, 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.



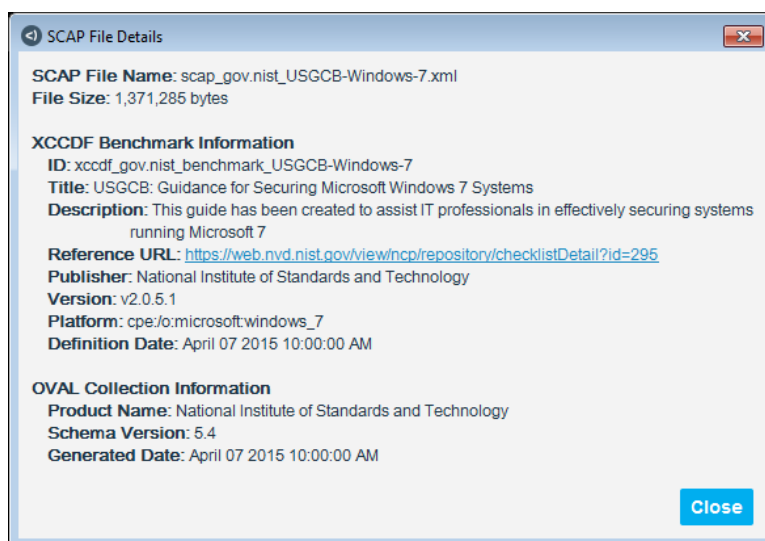
5. Select **Apply** and then select **Close** to save the module configuration.

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



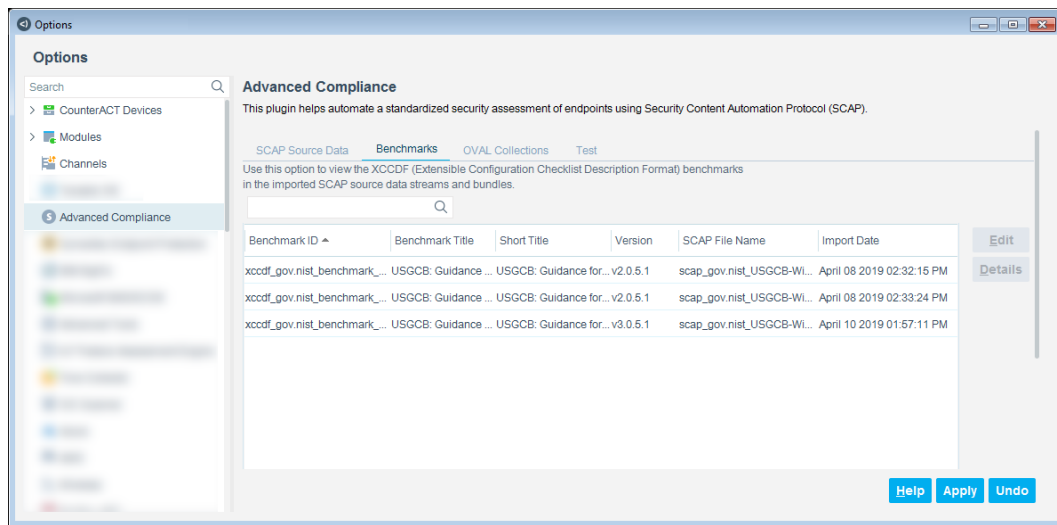
2. Select **Close**.

View Benchmark Details

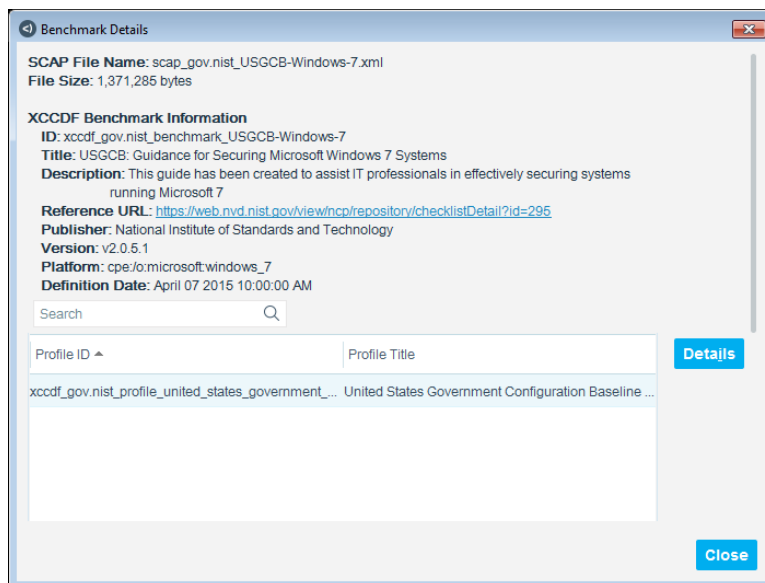
You can view details of the imported XCCDF benchmark profiles used for endpoint compliance scans.

To view XCCDF benchmark details:

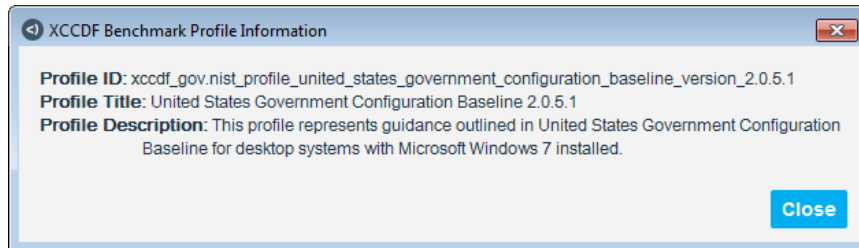
1. In the Advanced Compliance pane, select the Benchmarks tab.



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



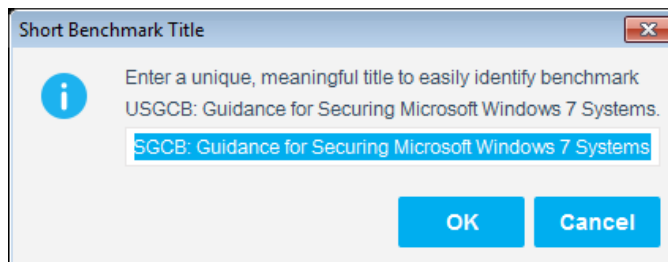
4. Select **Close** to close the dialog boxes.

Edit a Short Benchmark Title

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

To edit a short benchmark title:

1. In the Benchmarks tab, select the benchmark ID, and select **Edit**.



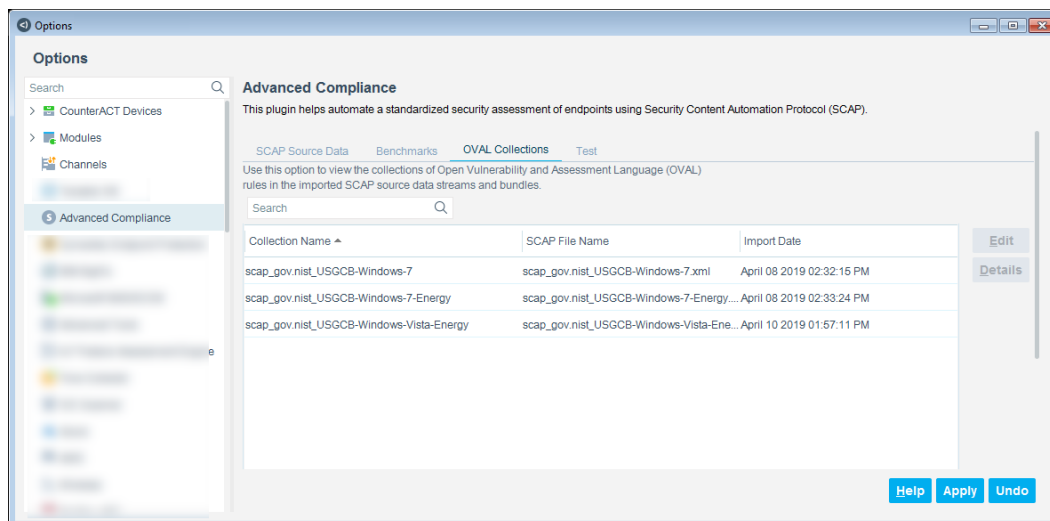
2. Enter a short benchmark title, and select **OK**. The title may contain letters, numbers, a colon, a period, and spaces.
3. Select **Apply** and then select **Close** to save the module configuration.

View OVAL Collection Details

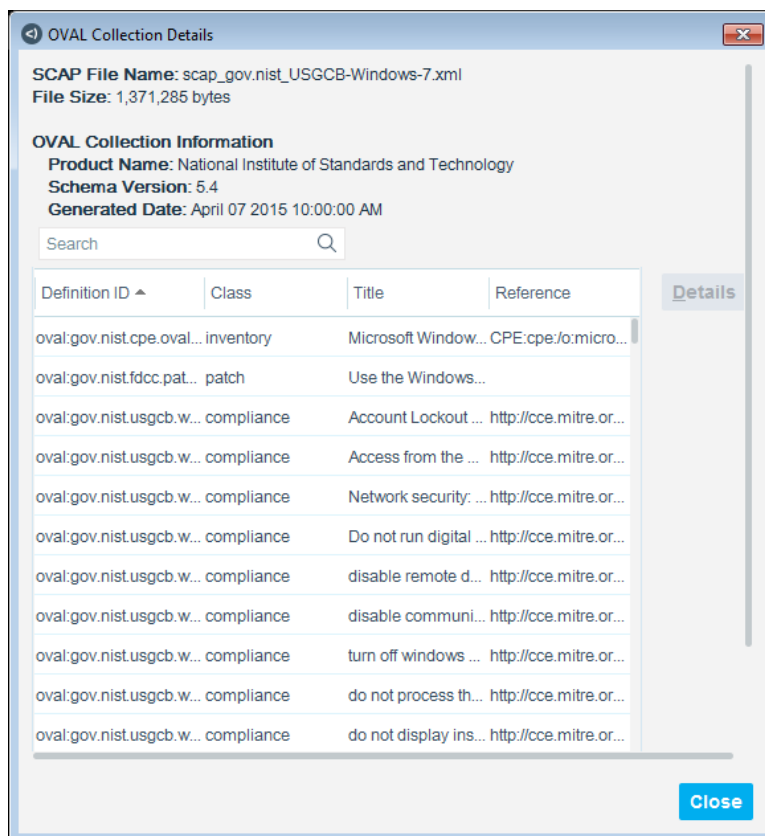
You can view details of the imported OVAL rules.

To view OVAL collection details:

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

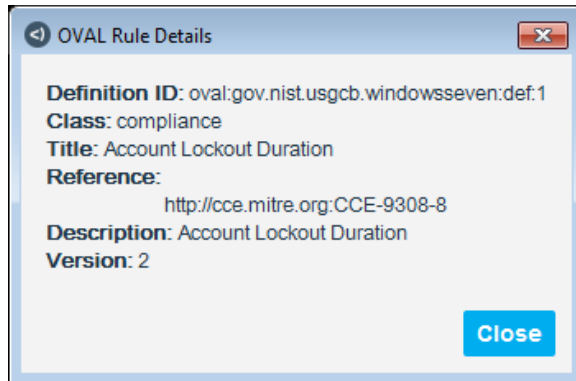


2. To view more collection details and the list of OVAL rules included in the collection, select the collection, and select **Details**. The following is displayed:
 - Details of the imported SCAP file that included the OVAL collection
 - Details of the OVAL collection
 - A list of the rule definitions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



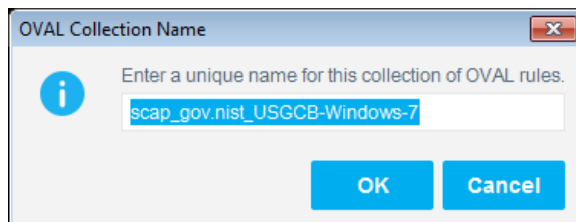
4. Select **Close** to close the dialog boxes.

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**.



2. Enter an OVAL collection name, and select **OK**.
3. Select **Apply** and then select **Close** to save the module configuration.

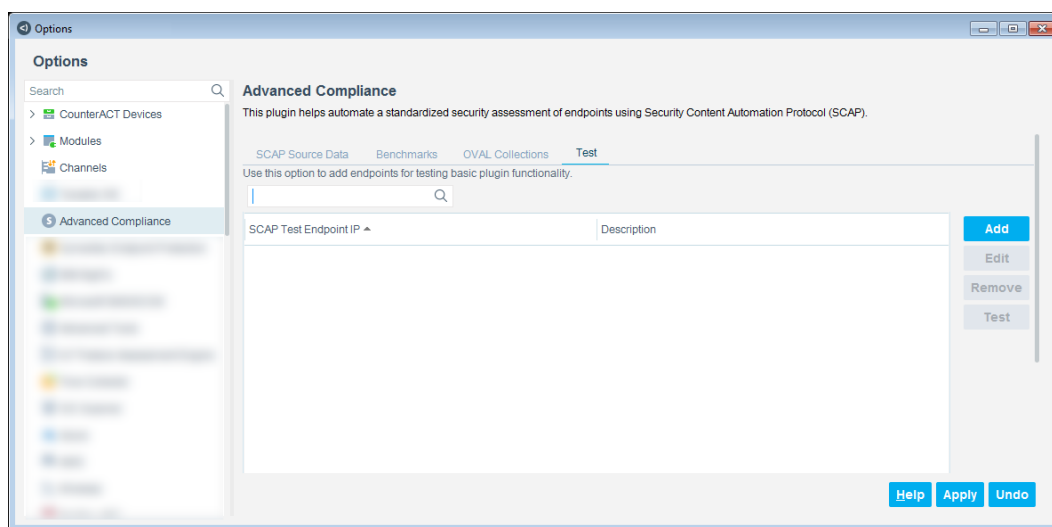
Test Advanced Compliance Endpoints

Use the Test tab 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).

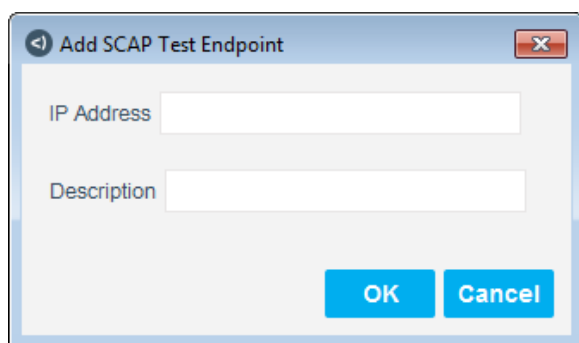
In the Test tab, enter the IP addresses of endpoints you wish to test for Advanced Compliance functionality. You can add a number of endpoints for testing and save them in the Test tab list. The test runs on one selected endpoint at a time.

To test an endpoint:

1. Select **Options > Advanced Compliance** and then select the Test tab.



2. Select **Add**.

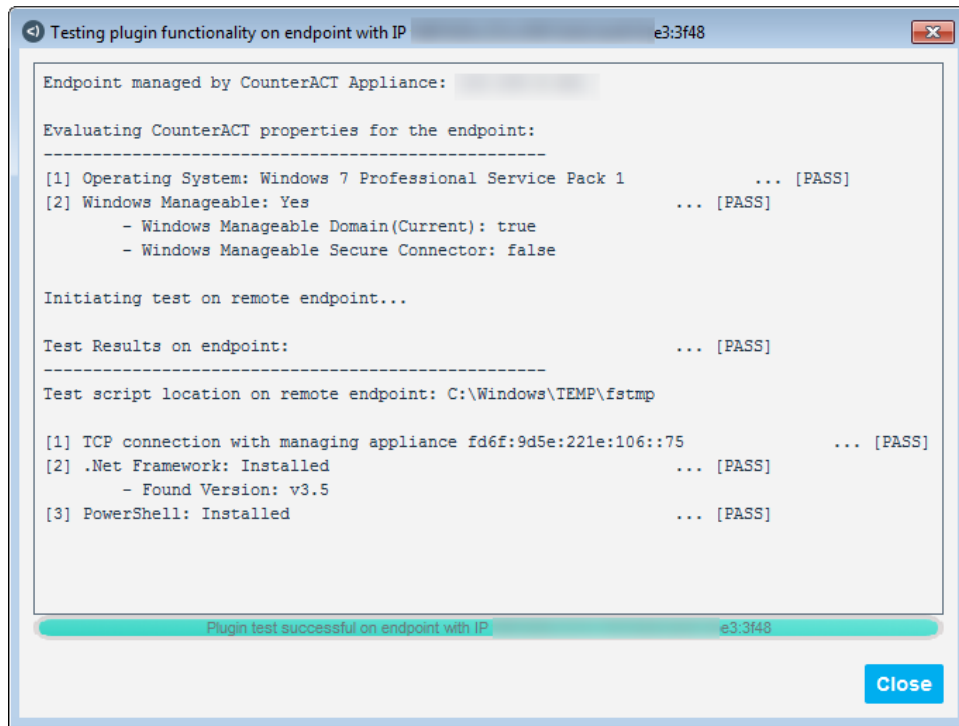


3. Define the SCAP test endpoint parameters:

IP Address	Enter the IPv4 or IPv6 address of an endpoint you want to test. Endpoints can have IPv4-only, IPv6-only, or IPv4 and IPv6 addresses.
Description	(Optional) Enter a short description for the endpoint.

4. Select **OK** to save the settings.

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



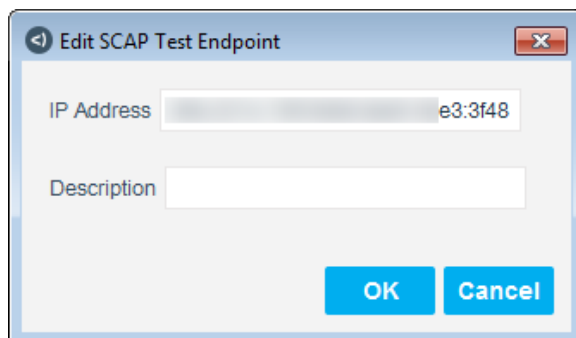
6. Select **Close**.

Edit IP Address of an Endpoint

You can edit the IP address of an endpoint.

To edit the IP address of an endpoint:

1. Select **Options > Advanced Compliance** and then select the Test tab.
2. Select an existing endpoint and then select **Edit**.



3. Edit the IP address of the endpoint and then select **OK**.


Run Advanced Compliance Policy Templates

Forescout eyeExtend for Advanced Compliance provides a policy template to detect, manage, and remediate endpoints based on Advanced Compliance scan results.

The SCAP 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.

See the following:

- [SCAP Compliance Score Policy Template](#)
- [Create Custom Advanced Compliance Policies](#)


 *It is recommended that you have a basic understanding of Forescout platform policies before working with the templates. Refer to [Policy Templates](#) and [Policy Management](#) in the Forescout Administration 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

The Forescout platform 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 the Forescout platform using Remote Inspection or SecureConnector.

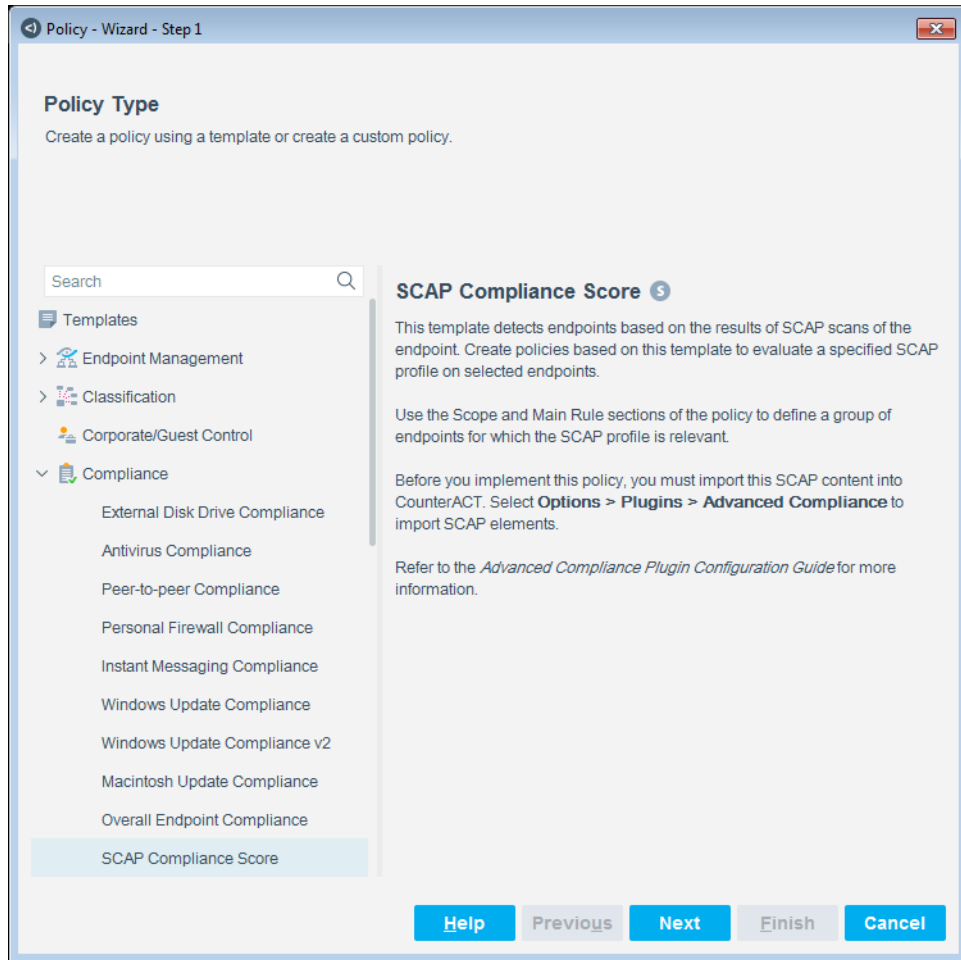
 *This release of Forescout eyeExtend for Advanced Compliance only supports Windows endpoints.*

Create the Policy

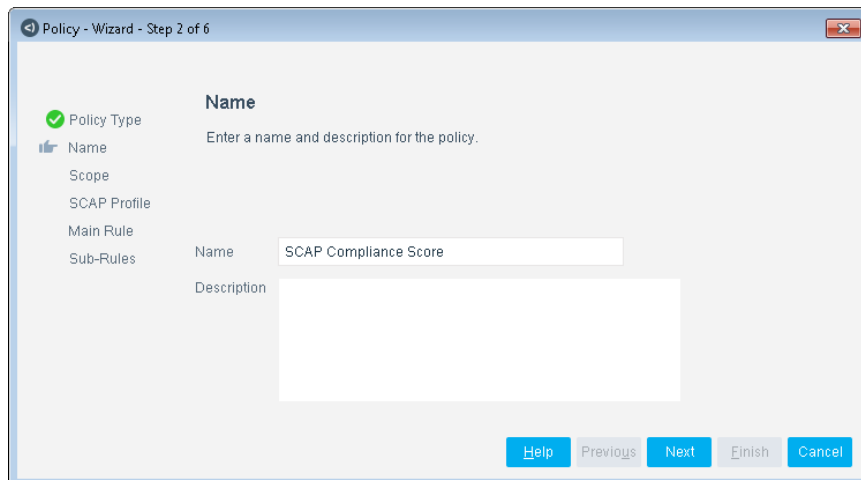
This section describes how to create a policy from the policy template.

To create the policy:

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




4. Select **Next**.




5. Enter a name for the policy. Optionally, enter a description.

- 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`.

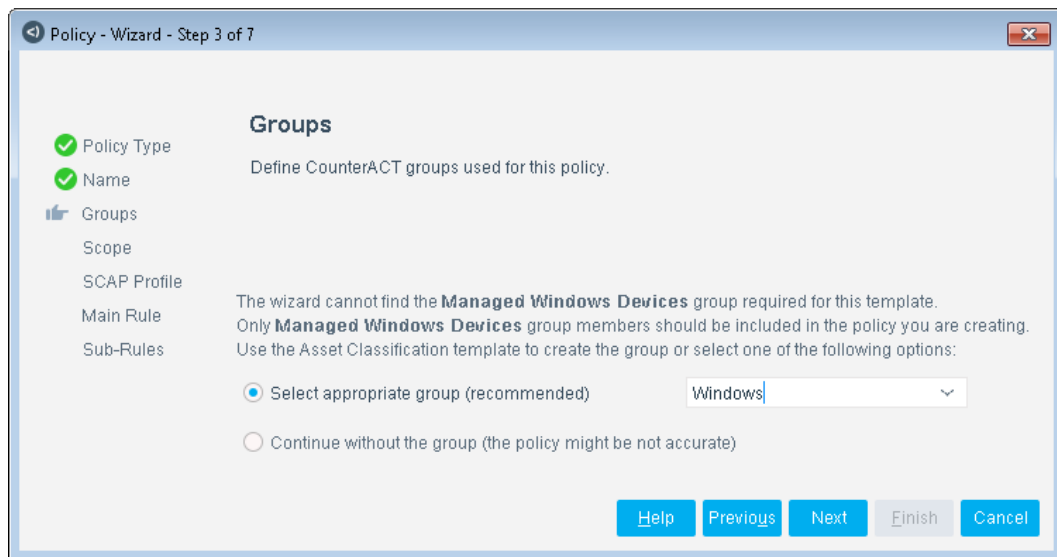
- Use a descriptive name that indicates what your policy is verifying and the actions that will be taken.
- Ensure that the name indicates whether the policy criteria must be met or not met.
- Avoid having another policy with a similar name.

 *Policy names are displayed in the Policy Manager, the Views pane, NAC Reports and in other features. Precise names make working with policies and reports more efficient.*

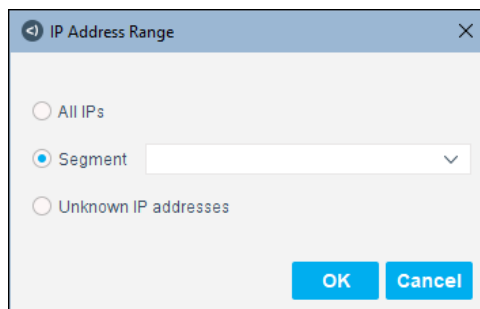
6. Select **Next**. The Groups pane opens, which lets you select the group used to filter results. Only managed Windows endpoints should be included in this policy.

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

7. Select a group that contains your managed Windows endpoints from the list, or select **Continue without the group**.




8. Select **Next**. Both the IP Address Range dialog box and the Scope pane open.
9. Use the IP Address Range dialog box to define which endpoints are inspected.



The following options are available:

- **All IPs:** Include all IP addresses in the Internal Network.
- **Segment:** Select a previously defined segment of the network. To specify multiple segments, select **OK** or **Cancel** to close this dialog box, and select **Segments** from the Scope pane.
- **Unknown IP addresses:** Apply the policy to endpoints whose IP addresses are not known. Endpoint detection is based on the endpoint MAC address.

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

10. Select **OK**. The added range is displayed in the Scope pane.

11. Select **Next**. The SCAP Profile pane opens, which lets you specify the XCCDF profile that is evaluated on endpoints within the policy scope.

Before you use this pane to select an XCCDF benchmark or its profiles, you must first import the corresponding XCCDF benchmark into the Forescout platform. The drop-down menus of this pane only list benchmarks that were previously imported into the Forescout platform.



12. In the **Short Benchmark Title** drop-down menu, select a benchmark. Use the full name of the benchmark in the **Benchmark Title** field to confirm your selection.

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

14. Select **Next**. The Main Rule pane opens, which lets you 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.

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

Policy - Wizard - Step 6 of 7

Main Rule

Use this screen 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 conditions without an action to filter/select endpoints for evaluation by sub-rules. Actions you specify here are applied to each matching endpoint before it is evaluated by sub-rules of the policy.

Condition

A host matches this rule if it meets the following condition:

All criteria are True

Criteria
OS CPE Format - Contains microsoft:windows_7

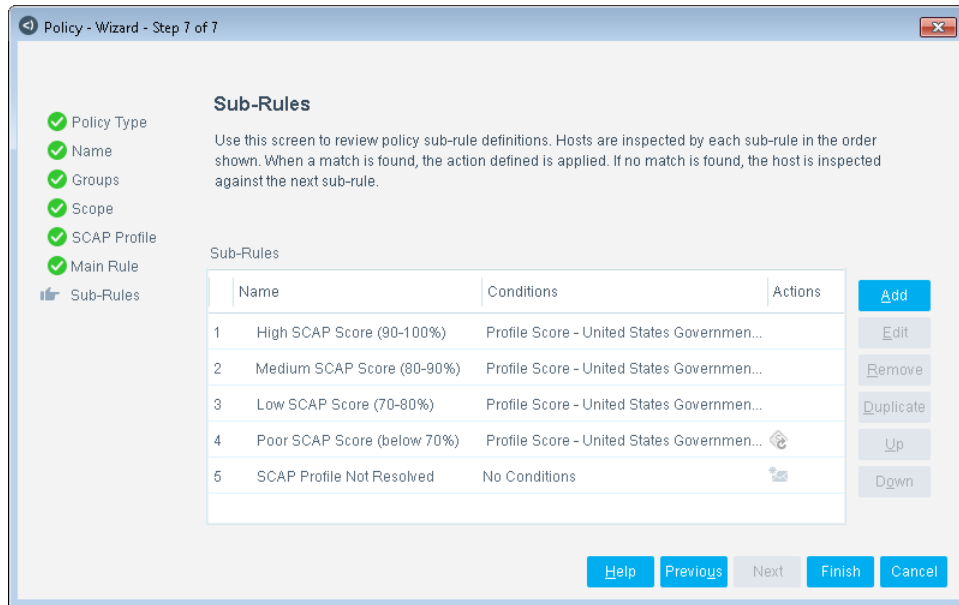
Actions

Actions are applied to hosts matching the above condition.

Enable	Action	Details
No items to display		

Help Previous Next Finish Cancel

- 15. Select *Next*.** The Sub-Rules pane opens, which lets you review the default set of sub-rules that manage/remediate endpoints based on the results of the specified compliance scan.



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. Examples of the type of action that may be appropriate for each range of scores are as follows.

- 1 High SCAP Score (90-100%): This rule detects endpoints for which the profile scan scored 90-100 percent.
 - 2 Medium SCAP Score (80-90%): This rule detects endpoints for which the profile scan scored 80-90 percent.
 - 3 Low SCAP Score (70-80%): This rule detects endpoints for which the profile scan scored 70-80 percent.
- Endpoints that match one of these three rules are considered compliant with the profile, and no remedial action is applied to them.
- 4 Poor SCAP Score (below 70%): 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 SCAP Profile Not Resolved: This rule detects endpoints for which the profile scan score could not be resolved. Endpoints matching this rule are rechecked once a day.

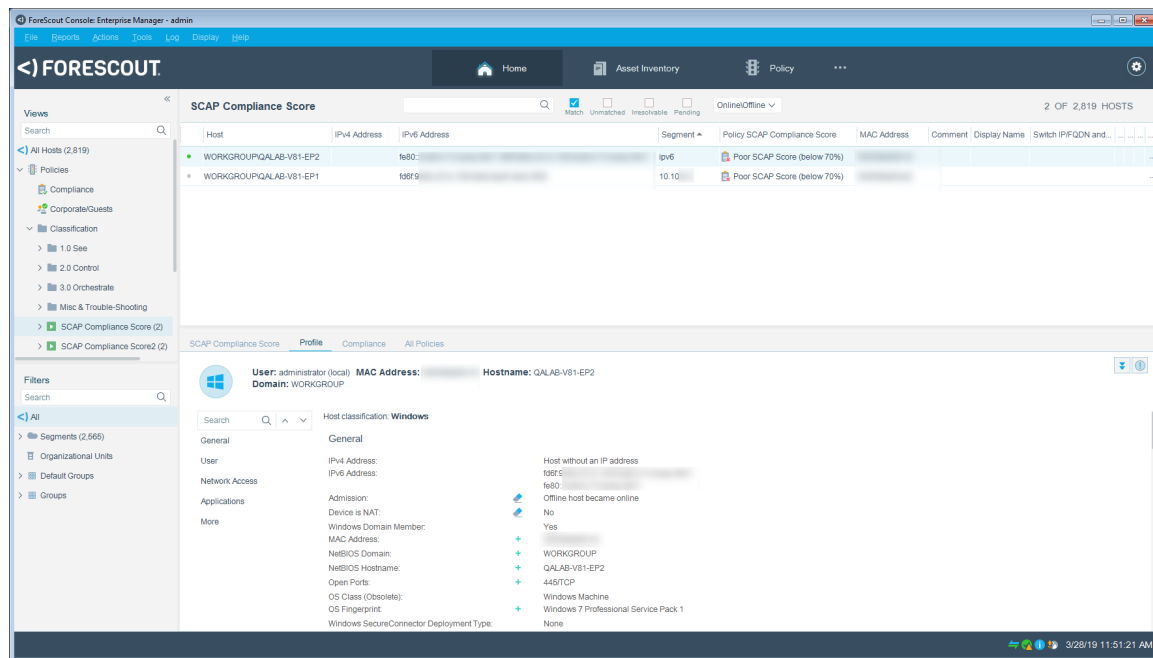
An optional **Send Email** action (disabled by default) sends an email alert to an administrator.

16.Select **Finish**. The policy is created.

17.Select **Apply** to save the policy in the Policy Manager.

Display IPv6 Addresses

After adding the SCAP Compliance Score policy, you can go to the All Hosts pane and select the policy to display the policy results, including the configured IPv4 and IPv6 addresses.



Create Custom Advanced Compliance Policies

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

Properties

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

Actions

Policy actions let you instruct the Forescout platform 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 Forescout platform 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 Console and select **Policy**. The Policy Manager opens.
2. Select **Add** to create a policy. The Policy Wizard opens.
3. In the Templates tree, select **Custom**.

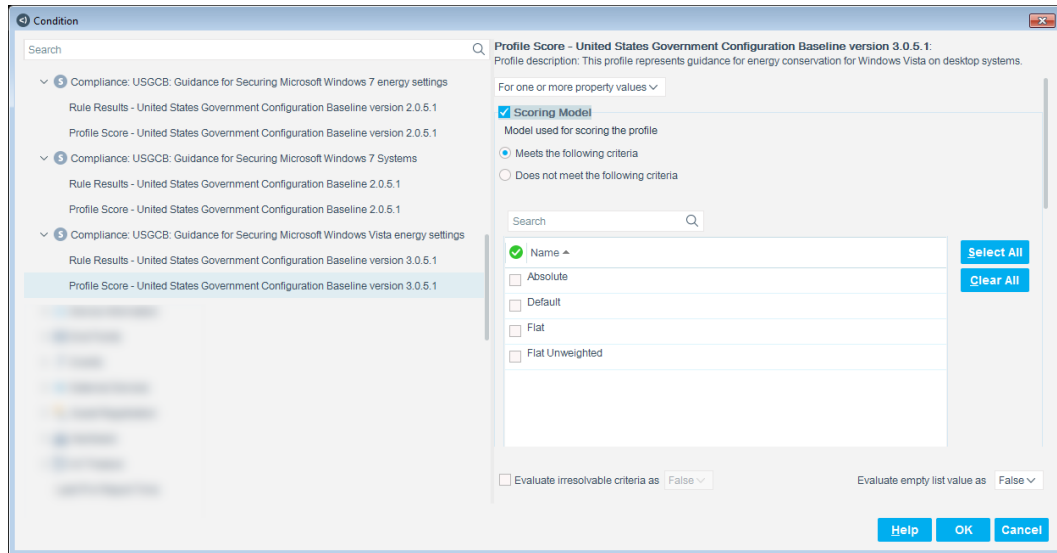
Detect Compliance – Policy Properties

For each profile in the benchmark imported to Forescout eyeExtend for Advanced Compliance, 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.

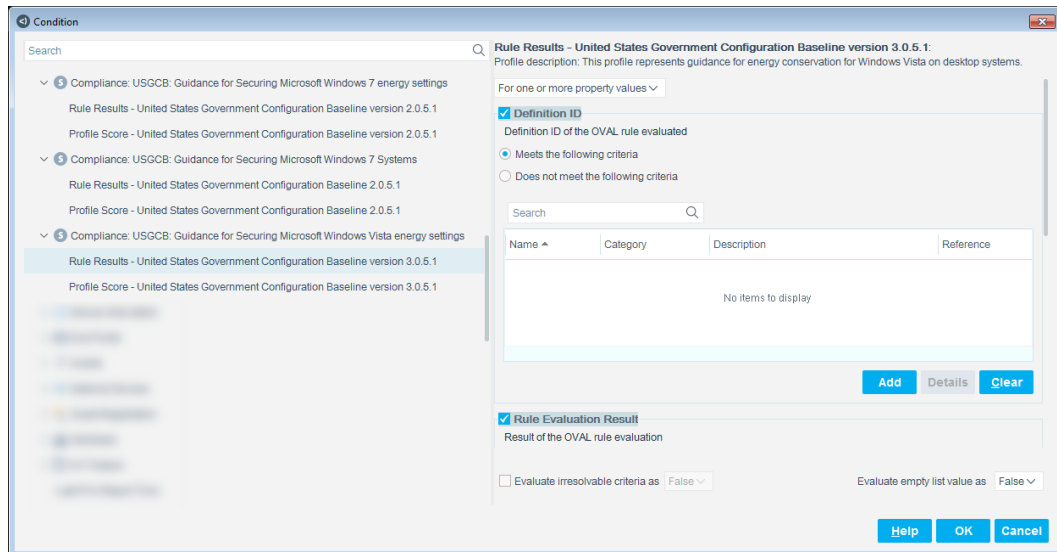
When an endpoint is evaluated in a policy rule that uses one of these properties, a compliance scan for that profile is initiated. You can create policies that use the SCAP profile compliance score or OVAL rule results to trigger actions on relevant endpoints.

To access Advanced Compliance properties:

1. Go 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.

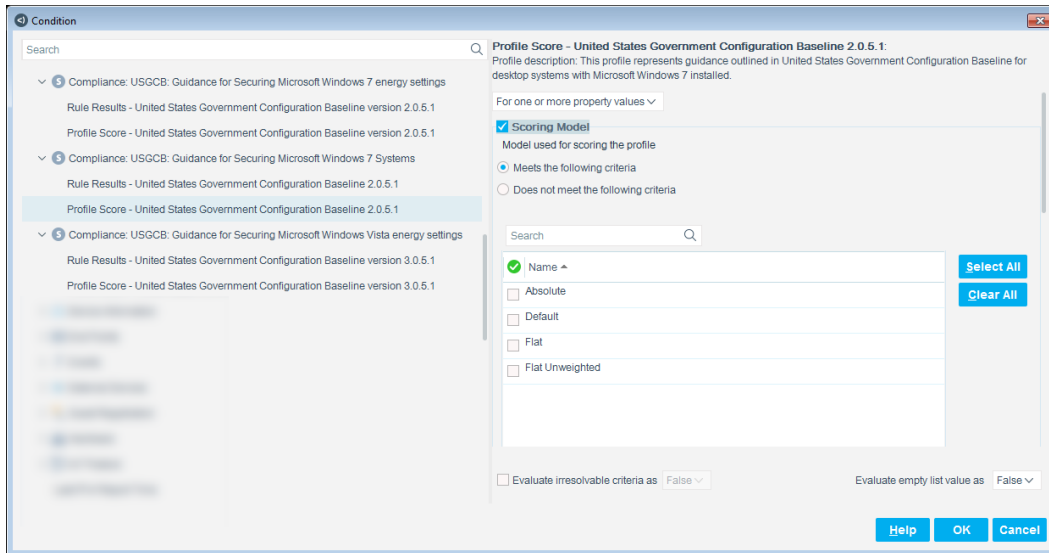


- For a freestanding OVAL collection, expand the Compliance > Independent OVAL Collection folder, and select the **Rule Result** property corresponding to the collection.



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 pane.



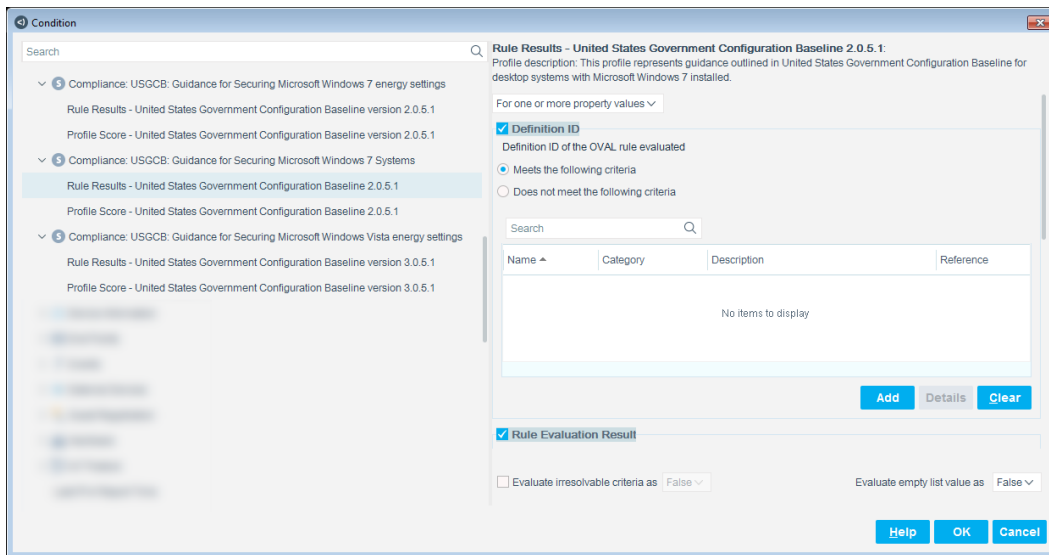
The following parameters are available:

Scoring Model	<p>The model used for computing the profile score:</p> <ul style="list-style-type: none"> ▪ Absolute: <ul style="list-style-type: none"> - 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. The maximum score is the number of rules checked. <p>For more information about these scoring models, refer to Specification for the Extensible Configuration Checklist Description Format (XCCDF).</p>
Score	<p>The profile scan score computed using the selected scoring model. This value is relative to the Maximum Score calculated for the endpoint.</p>
Maximum Score	<p>The theoretical maximum score if the endpoint passes/satisfies all rules in the profile applicable to the endpoint. The Forescout platform calculates this value as part of profile evaluation on each endpoint, using the selected scoring model.</p> <p>Select this option if you want to define a condition that matches the Maximum Score calculated for each endpoint.</p> <p>OVAL rules with the following results are not factored into the maximum score:</p> <ul style="list-style-type: none"> - <i>Informational</i> - <i>Not Applicable</i> - <i>Not Checked</i> - <i>Not Selected</i>

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 pane.



The following parameters are available:

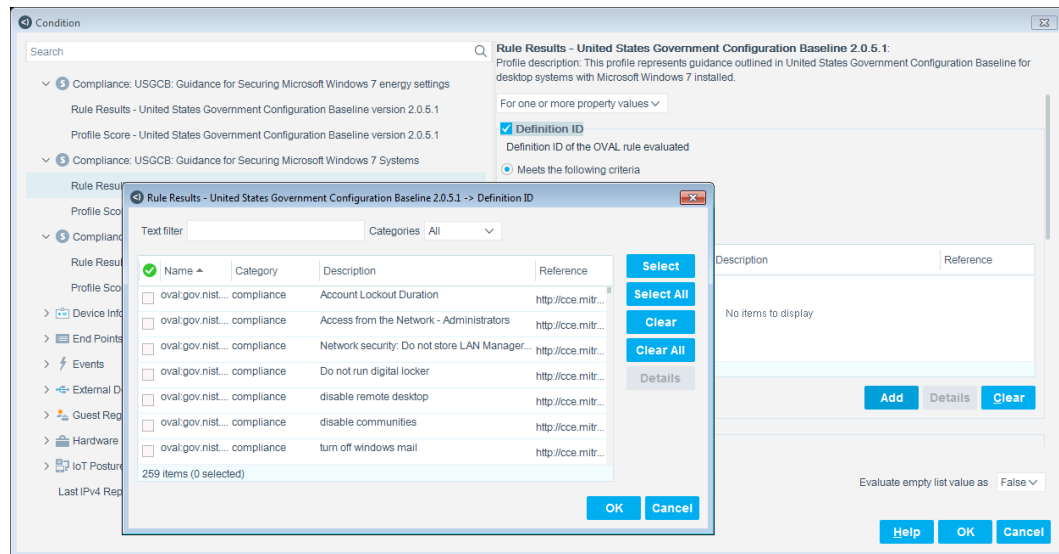
Definition ID	The Definition ID of the OVAL rule(s) evaluated.
Rule Evaluation Result	<p>The result of the OVAL rule evaluation:</p> <ul style="list-style-type: none"> ▪ Error: An error occurred during the rule evaluation. For example, the scan was run with insufficient privileges. ▪ Fail: The rule was 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. <p>A rule is considered satisfied if the result of the evaluation is either Pass or Fixed.</p>

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** option.
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 and then select **OK**.
The selected rule(s) are displayed 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.

Manage Advanced Compliance Results – Policy Action

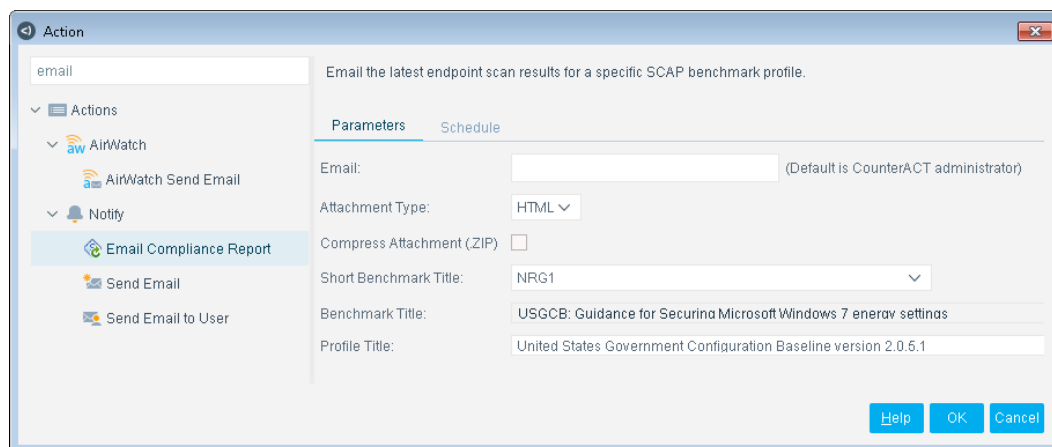
This topic describes the action that is made available when Forescout eyeExtend for Advanced Compliance is installed.

To access the SCAP action:

1. Go to the Actions tree from the Policy Actions dialog box.
2. Expand the Notify 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 Forescout platform policies to email a report of Advanced Compliance results in either HTML or XML format.



The following parameters are available:

Email	The email address to which the Advanced Compliance results are sent. If no address is provided, the mail is sent to the Forescout administrator address.
Attachment Type	The format of the attachment: <ul style="list-style-type: none"> ▪ HTML: Results are written in an easy-to-read report. ▪ XML: Results are written as an ARF-compatible XCCDF data stream.
Compress Attachment (.ZIP)	The attachment is compressed and sent as a .ZIP file.
Short Benchmark Title	The user-defined title of the benchmark used for the scan.
Benchmark Title	The title of the benchmark used for the scan.
Profile Title	The title of the benchmark profile used for the scan.

Display Advanced Compliance Inventory Information

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

To access the Asset Inventory:

1. Select **Asset Inventory** from the Console toolbar.
2. Go 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.



Refer to [Working with Asset Inventory Detections](#) in the *Forescout Administration Guide* or the Console online help for information about how to work with the Asset 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, lets you 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 lets you run reports on demand or configure periodic generation of reports.

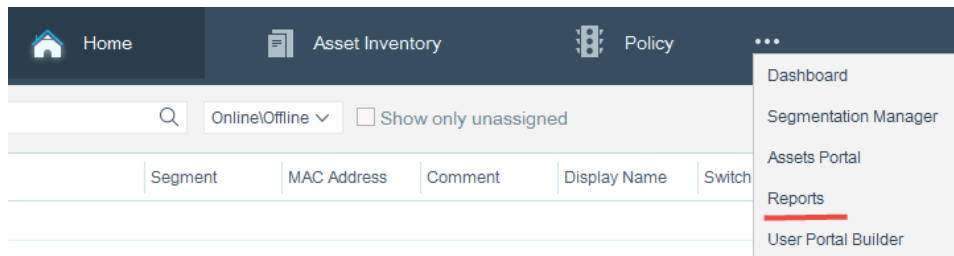
Create an SCAP ARF Report

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 the evaluation results that are reported.

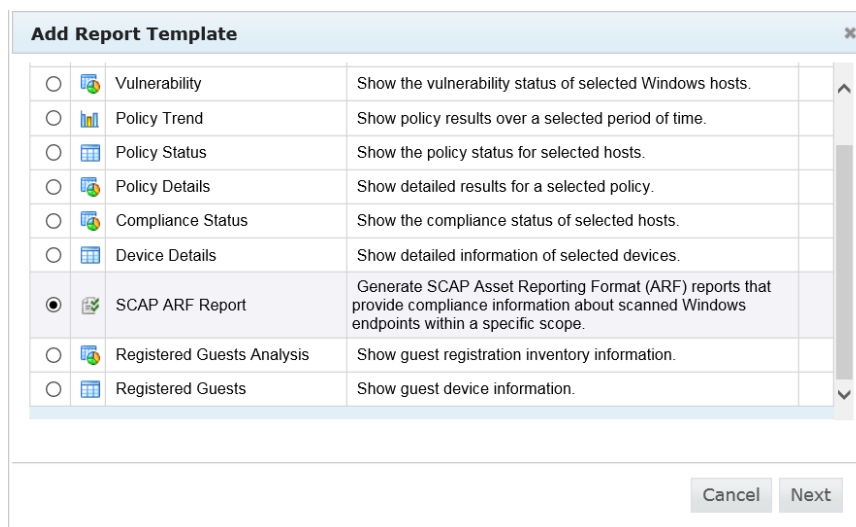
 *The email sent by the Reports portal does not contain report output files. It only contains the pathname of the report on the server on which report files are placed.*

To create an ARF Report:

1. Select the **Ellipsis**  from the Console **Toolbar**.



2. Select **Reports** from the drop-down menu.
3. In the **Reports** home page, select **Add**.



4. Select **SCAP ARF Report** and select **Next**. The report template parameters page opens. The **Header** section is the first section.

The screenshot shows the '1. Header' section of a configuration form. It has a yellow header bar with the text '1. Header'. Below it, there are three light blue sections: 'Name:', 'Description:', and 'Generated by:'. The 'Name:' section contains a text input field with 'SCAP ARF Report' and a close button 'x'. The 'Description:' section contains a text area with the text 'Generate SCAP Asset Reporting Format (ARF) reports that provide compliance information about scanned Windows endpoints within a specific scope.' and a scroll bar. The 'Generated by:' section contains a text input field with 'admin'.

5. In the **Header** section:

- In the **Name** field, enter a report name. The maximum length of the field is 60 characters. The following characters cannot be used in the name:
& # : / ' ` "
- (Optional) In the **Description** field, enter descriptive text.
- (Optional) In the **Generated by** field, enter the name of the Forescout platform user generating or associated with the report. The maximum length of the field 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.

6. In the **Scope** section, select either **All IP's** or **Segment**, for the network IP segments for which to create the report.

The screenshot shows the '2. Scope' section of a configuration form. It has a yellow header bar with the text '2. Scope'. Below it, there is a light blue section titled 'IP ranges:'. Inside this section, there are two radio buttons: 'All IP's' (which is selected) and 'Segment'. To the right of the 'Segment' radio button is an 'Edit >>' button and a document icon.

7. (Optional) If you select **Segment**, select a segment in the left pane, select **Add** to move it to the right pane, and then select **OK**. Segments can include IPv4 or IPv6 addresses.


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

9. In the **File Transfer Parameters** section, provide the details that are used to transfer the generated ARF report to a remote server.

Enter the following parameters:

- **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.

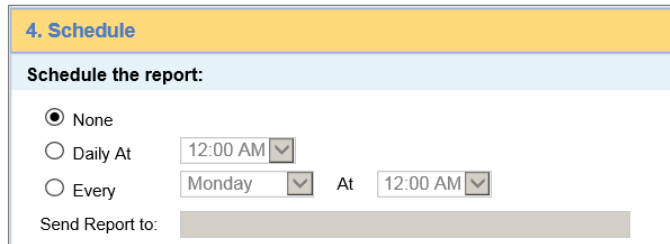
- **Port:** Enter the port number to which to connect on the remote server. The default port of the selected transfer protocol is displayed automatically in this field.
- **Username:** Enter the username for logging in to the remote server.
- **Password:** Enter the password for logging in to the remote server.
- **Verify Password:** Re-enter the specified password to verify 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.*

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

If the file transfer test is successful, **Test successful** is displayed.

11. (Optional) In the **Schedule** section, define a schedule for report generation.



4. Schedule

Schedule the report:

☒ None

☐ Daily At

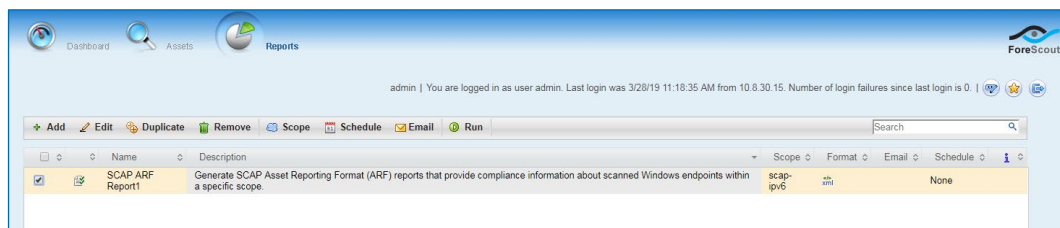
☐ Every At

Send Report to:

- Define a schedule to generate:
 - > a daily recurring report (**Daily At** <time of day>)
 - > 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 which to send a notification of the generated report. You can enter multiple email addresses, separating them with commas.

12. Perform either of the following:

- Select **Save** to save the defined report template for later use. The saved report template is displayed in the table on the **Reports** home page.



- Select **Run** to generate a report using the defined report template. The SCAP Summary Report opens and displays the filename of the SCAP report and the IP addresses or hostnames associated with the file.

SCAP Summary Report

SCAP Report File Name	IP Addresses associated with file
reports/SCAP ARF Report_Forescout_report_Fri_Jan_25_10_23_34_PST_2019-84-p1.xml	CA-S10-W7-1, HMANDADI-W81, QALAB-V81-EP2

View the SCAP ARF Report

The SCAP ARF Report is located in the **Directory to Receive File**, specified in the File Transfer Parameters. It will have a name similar to the following:

SCAP ARF Report_Forescout_report_Thu_Feb_14_10_34_21_PST_2019-summary.html

Double-click the HTML file to view the report. In addition to the Benchmark and the Results Summary, you can display the Results by Rule or the Results by Target.

In Results by Rule, select NOT CHECKED. Hostnames are displayed.

Results by Rule						
Rule	References	Pass	Fail	Unknown	Not Applicable	
▼ Specify the System Hibernate\Sleep Timeout (On Battery)	CCE-18938-1 CCE-79401-6	0	0	3	0	
<p>Specify the System Hibernate\Sleep Timeout (On Battery) xccdf_gov.nist_rule_Specify_the_System_Hibernate_or_Sleep_Timeout_On_Battery</p> <p>Specifies the period of inactivity before Windows transitions the system to hibernate or sleep.</p> <p>References</p> <ul style="list-style-type: none"> • CCE-18938-1 • CCE-79401-6 <p>Target Results</p> <p>NOT CHECKED (3)</p> <p>Targets: CA-S10-W7-1, HMANDADI-W81, QALAB-V81-EP2</p>						

In Results by Target for each hostname, the IPv4 and IPv6 addresses are displayed for Endpoint IP(s) from Segments and for Additional IP(s) Belonging to Endpoint.

Results by Target						
Target	Pass	Fail	Unknown	Not Applicable		
▼ CA-S10-W7-1	0	0	4	0		
<p>Endpoint IP(s) from Segments</p> <ul style="list-style-type: none"> • 10.100.2.135 • fd6f:9d5e:221e:102:0:0:0:135 <p>Additional IP(s) Belonging to Endpoint</p> <ul style="list-style-type: none"> • fe80:0:0:0:8083:a437:f78a:b040 • fd6f:9d5e:221e:102:3cc2:7af5:2864:6804 • fd6f:9d5e:221e:102:8083:a437:f78a:b040 <p>Rule Results</p> <p>NOT CHECKED (4)</p>						

Appendix A: Executable Files Used by the Module

The following executable file is run on endpoints during Advanced Compliance scans.

EXE File Name	Description
processproxy.exe	Client process that performs SCAP content OVAL checks on the endpoint and reports the results over port 10008 using a secured TCP connection to the managing CounterACT® Appliance.