ForeScout CounterACT®

Core Extensions Module: IoT Posture Assessment Engine

Configuration Guide

Version 1.0

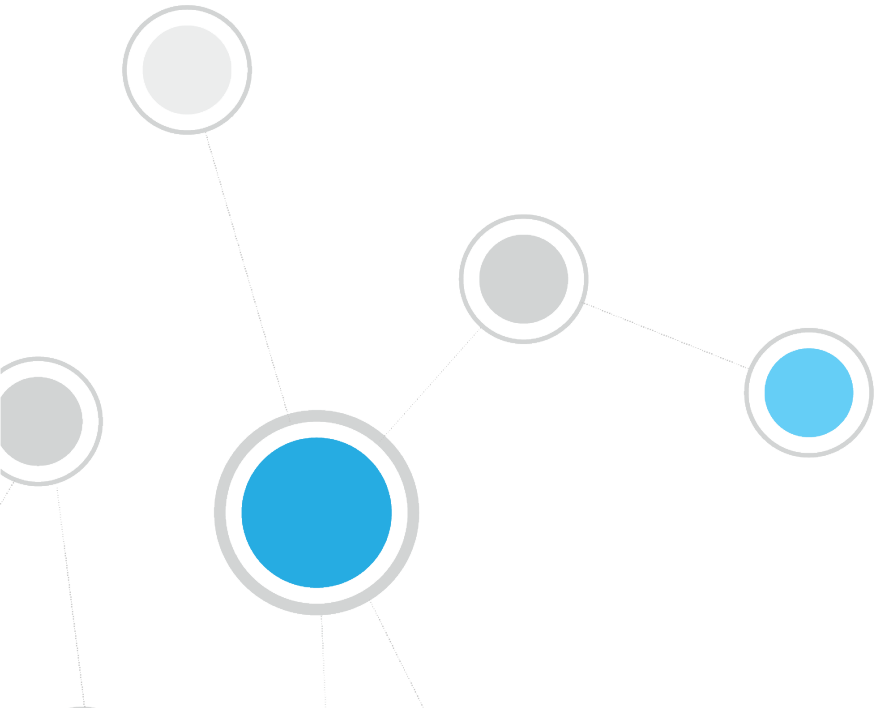


Table of Contents

About the IoT Posture Assessment Engine

The IoT Posture Assessment Engine is a component of the ForeScout CounterACT® Core Extensions Module. See Core Extensions Module Information for details about the module.

The IoT Posture Assessment Engine assesses the security risk associated with IoT devices based on their use of weak login credentials.

The key benefits of the IoT Posture Assessment Engine are:

- Helps you determine which devices in your network are vulnerable to attack due to their use of weak credentials. See View All Endpoints Having a Security Risk.
- Helps you determine which devices and servers in your network are configured to use credentials that are common within the company and should be considered insecure.
- Provides extensible IoT Posture Assessment policy templates for SNMP, SSH, and Telnet credential vulnerabilities.

View All Endpoints Having a Security Risk

The IoT Posture Assessment Engine assesses the IoT devices connected to your network based on their use of weak credentials. Use the *Credential Vulnerability* property to identify endpoints that are at high risk due to:

- Poor Telnet and SSH password hygiene
- Poor SNMP community string hygiene

See Policy Overview.

Assess Corporate Credential Compliance

Use this feature to confirm that the devices connected to your network do not share over-used corporate passwords. Add commonly-used credentials to your Custom Credentials list, and then run a policy to confirm that the devices do not match the sub-rule of Custom Credentials.

How It Works

The IoT Posture Assessment Engine provides a *Credential Vulnerability* property that triggers CounterACT to attempt to log in to each device within the policy scope using a specified protocol and one of the following:

- known factory default credentials
- a set of commonly used credentials
- a custom list of credentials provided by you

When authentication succeeds, the device matches the condition.

What to Do

Perform the following to work with the IoT Posture Assessment Engine:

1. Do one of the following to resolve the *Credential Vulnerability* property on your endpoints:
   - Create and run policies based on the IoT Posture Assessment policy templates.
   - Use the *Credential Vulnerability* property in other policies.
2. Install the content module containing the IoT Posture Assessment Library whenever a new version is available so that the most current credential vulnerabilities are assessed. Refer to the *CounterACT IoT Posture Assessment Library Configuration Guide*. See Additional CounterACT Documentation for information about how to access this guide.

CounterACT Software Requirements

The IoT Posture Assessment Engine requires the following CounterACT releases and other CounterACT components:

- CounterACT version 8.0.
- IoT Posture Assessment Library version 18.0.4 or above. The IoT Posture Assessment Library is a Content Module that delivers a library of pre-defined login credentials that are used by the IoT Posture Assessment Engine to aid in determining the security risk of devices. The IoT Posture Assessment Library is updated periodically to to increase the breadth of the devices for which factory default credentials are known and to update the list of commonly used credentials. Install the latest version of the IoT Posture Assessment Library to take advantage of the most current updates.
- An active Maintenance Contract for CounterACT devices.

Configure the IoT Posture Assessment Engine

For endpoints to be grouped by their credential vulnerability, the Credential Vulnerability Property must be used in a policy, such as a policy created by IoT Posture Assessment policy templates.

See About the IoT Posture Assessment Policy Templates and About Custom Policies.

You can use the IoT Posture Assessment Engine without any configuration. The plugin uses credential lists provided by the IoT Posture Assessment Library to assess if a device uses weak credentials. The credentials in these lists are obtained from various sources on the Internet and are known to be used by hackers. See Commonly Used Credentials.

You can optionally configure custom user credentials to provide additional credentials for checking. See Custom Credentials. You can also test the plugin using a sample endpoint. See Test the Plugin.

Verify That the Plugin Is Running

After installation, verify that the plugin is running.

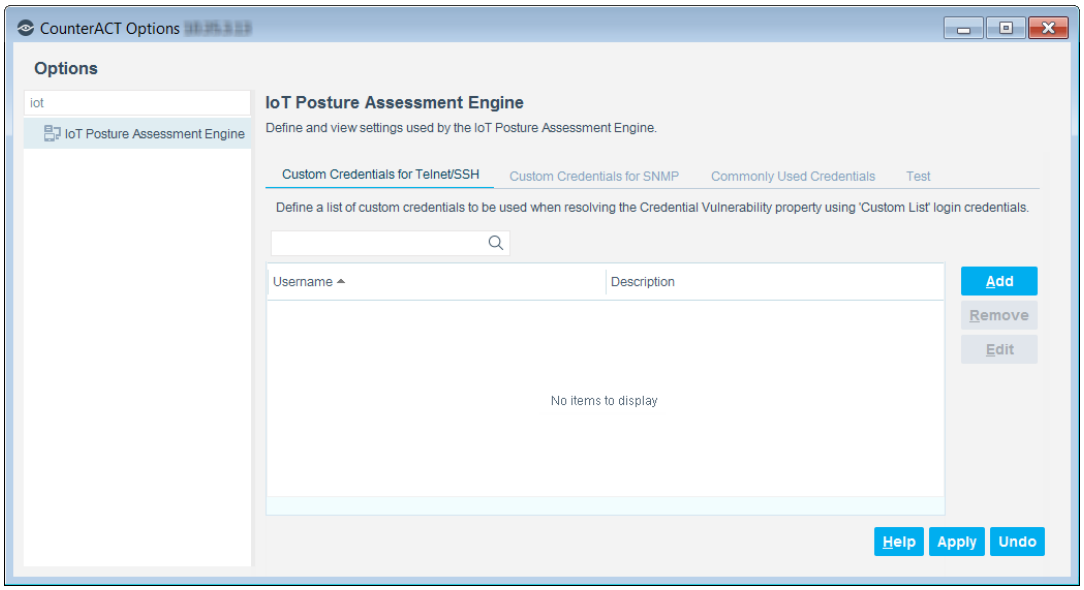
To verify:

1. Select **Tools**>**Options** and then select **Modules**.
2. Navigate to the plugin and select **Start** if the plugin is not running.

Custom Credentials

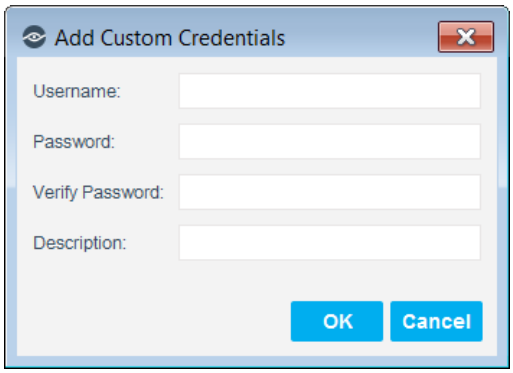
To define custom credentials checked by the Credential Vulnerability property:

1. Select **Options** from the CounterACT Console **Tools** menu, and select **IoT Posture Assessment Engine**.

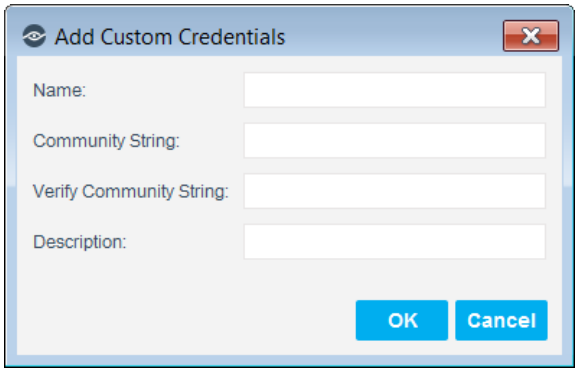


2. You can define a list of custom credentials for devices based on their communication protocol.
   - Select the **Custom Credentials for Telnet/SSH** tab to view and add custom Username / Password pairs for authenticating devices over Telnet and SSH.
   - Select the **Custom Credentials for SNMP** tab to view and add custom Community Strings for communicating with devices over SNMP.
3. To add credentials to the list, select **Add**. The Add Custom Credentials dialog box opens.

– For Custom Credentials for Telnet/SSH, enter the username and password with which CounterACT will attempt to authenticate, and verify the password. Add a description for these credentials (optional).



– For Custom Credentials for SNMP, enter the community string with which CounterACT will attempt to authenticate, and verify the string. Add a name and a description for these credentials (optional).



Commonly Used Credentials

The IoT Posture Assessment Library includes:

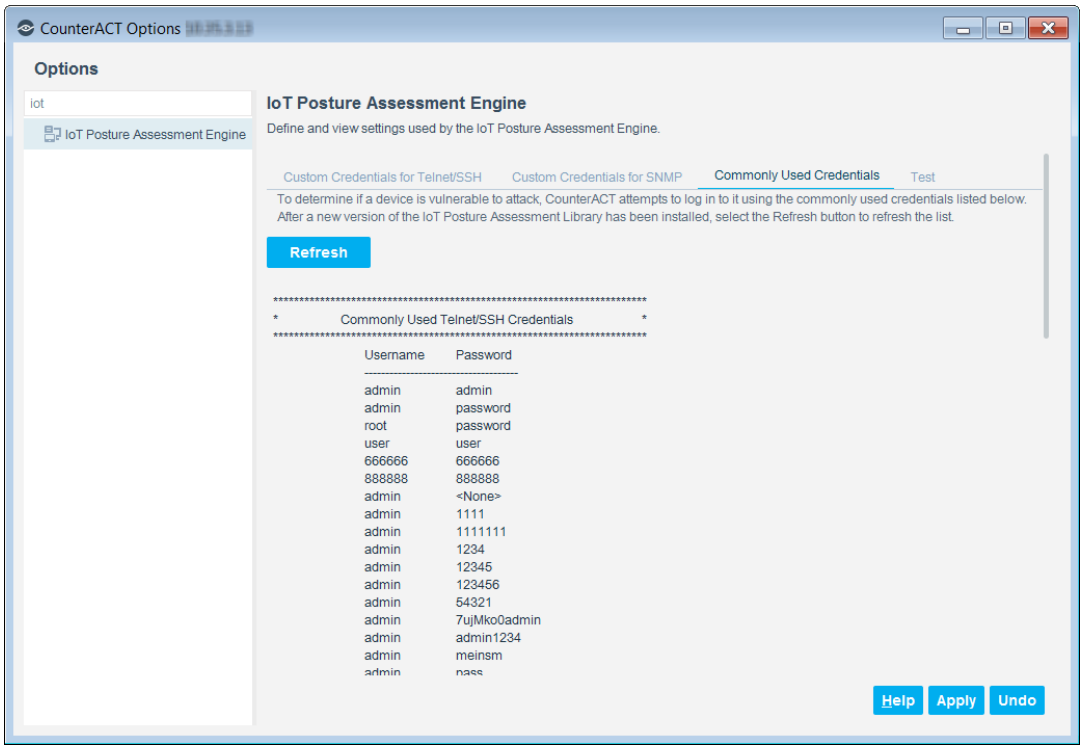
- Factory default credentials for various devices
- Commonly used credentials

For more information about the IoT Posture Assessment Library, refer to the *CounterACT IoT Posture Assessment Library Configuration Guide*. See Additional CounterACT Documentation for information about how to access this guide.

To view the list of commonly used credentials checked by the Credential Vulnerability property:

1. Select **Options** from the CounterACT Console **Tools** menu, and select **IoT Posture Assessment Engine**.
2. Select the **Commonly Used Credentials** tab. A list of common credentials is displayed for:
   – Telnet/SSH Credentials: Username and Password

– SNMP Credentials: Community String



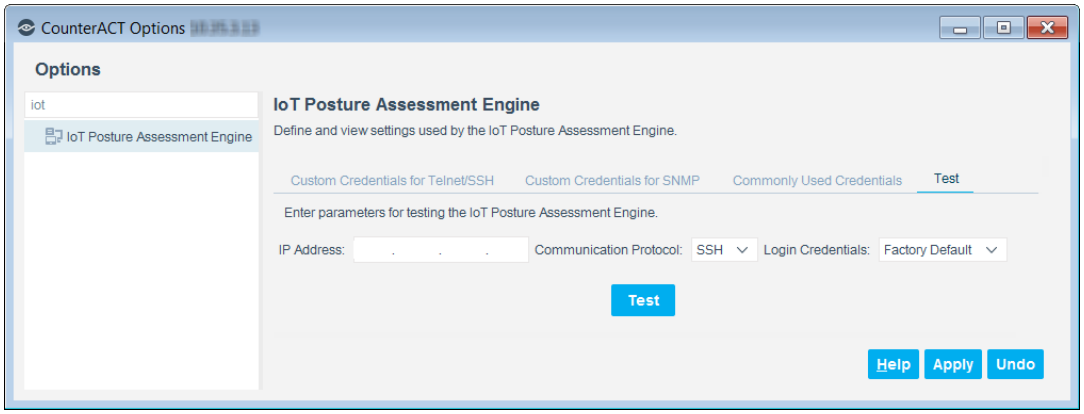
3. To refresh the display after a new version of the IoT Posture Assessment Library was installed, select the **Refresh** button. The updated list is displayed.

Test the Plugin

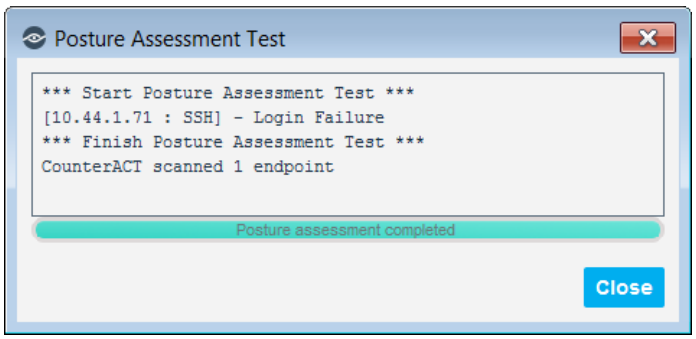
You can test ability of the plugin to assess the risk of a device based on whether or not it has weak credentials.

To test the plugin:

1. Select **Options** from the CounterACT Console **Tools** menu, and select **IoT Posture Assessment Engine**.
2. Select the **Test** tab.



3. Enter the IP address to be tested, the communication protocol, and the type of credentials to be tested.
4. Select **Test**. The test runs and the results are displayed.



5. If the test results in a *Login Failure*, no credential vulnerability was detected.

Credential Vulnerability Property

The IoT Posture Assessment Engine can resolve the security risk of devices based on whether or not they have the following credential vulnerabilities:

- Factory default credentials for various devices, from the list provided by the IoT Posture Assessment Library. The appropriate factory default credentials are selected based on the device classification resolved by the CounterACT Device Classification Engine.
- Commonly used credentials, from the list provided by the IoT Posture Assessment Library.
- Custom credentials, from a list provided by the CounterACT operator in the IoT Posture Assessment Engine options.

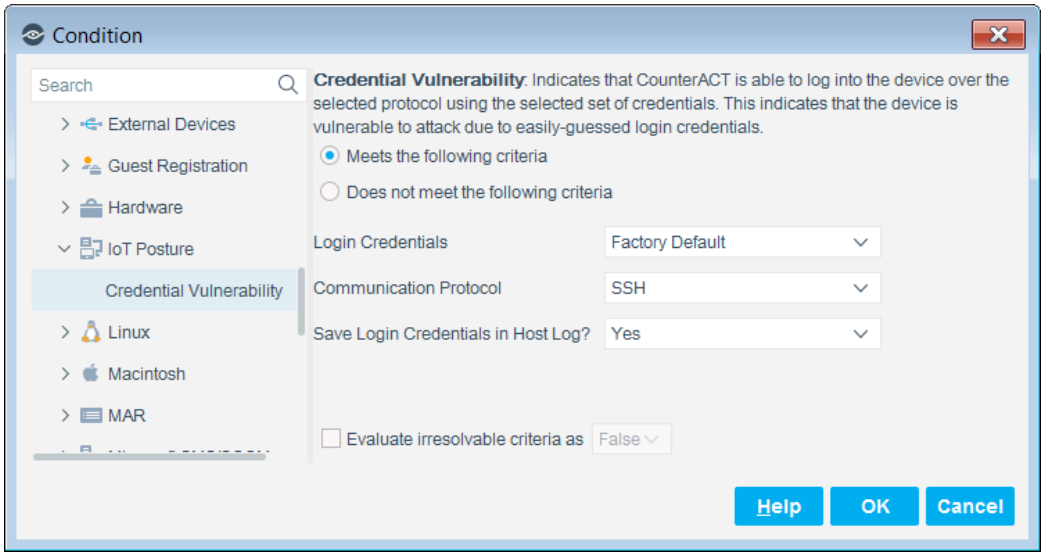
For more information about the IoT Posture Assessment Library, refer to the *CounterACT IoT Posture Assessment Library Configuration Guide*. See Additional CounterACT Documentation for information about how to access this guide.

CounterACT attempts to log in to the device using one of the following communication protocols:

- SSH, on the standard SSH port: TCP/22
- SNMP, on the standard SNMP port: UDP/161
  - Only SNMPv2 is checked
  - The 'read only' community is checked
- Telnet, on the standard Telnet port: TCP/23

To access the Credential Vulnerability property:

1. Navigate to the Properties tree from the Policy Conditions dialog box.
2. The Credential Vulnerability property is available in the IoT Posture node.



3. From the Login Credentials dropdown, select one of the following types of credentials to be used for attempts to log in to the device:
   - Factory Default
   - Commonly Used
   - Custom List
4. From the Communication Protocol dropdown, select one of the following:
   - SSH
   - Telnet
   - SNMP
5. To save the login credentials used for successful login so that they can be viewed in the Host Log, select **Yes**.

About the IoT Posture Assessment Policy Templates

The IoT Posture Assessment Engine provides policy templates for checking credential vulnerability using three different communication protocols:

- SNMP
- SSH
- Telnet

You can use the policy templates to create policies that resolve the Credential Vulnerability Property.

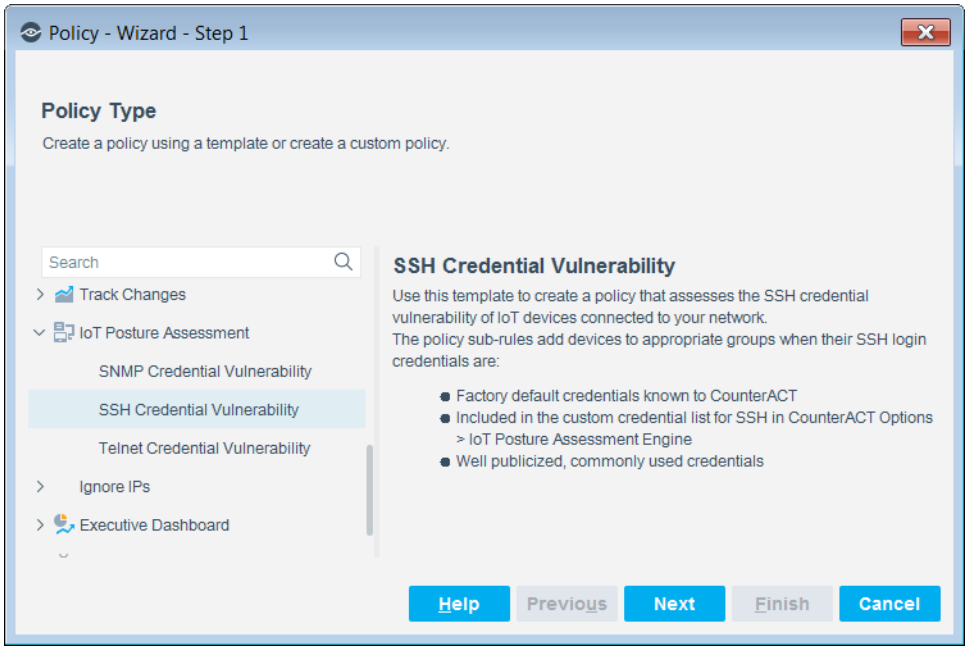
Sub-rules provided by the templates detect endpoints determined to be vulnerable to botnet and other attacks based on the use of weak login credentials. Policy actions add the vulnerable devices to one of the following groups:

- Factory Default Credentials (for SSH and Telnet only)
- Custom Credentials
- Commonly Used Credentials

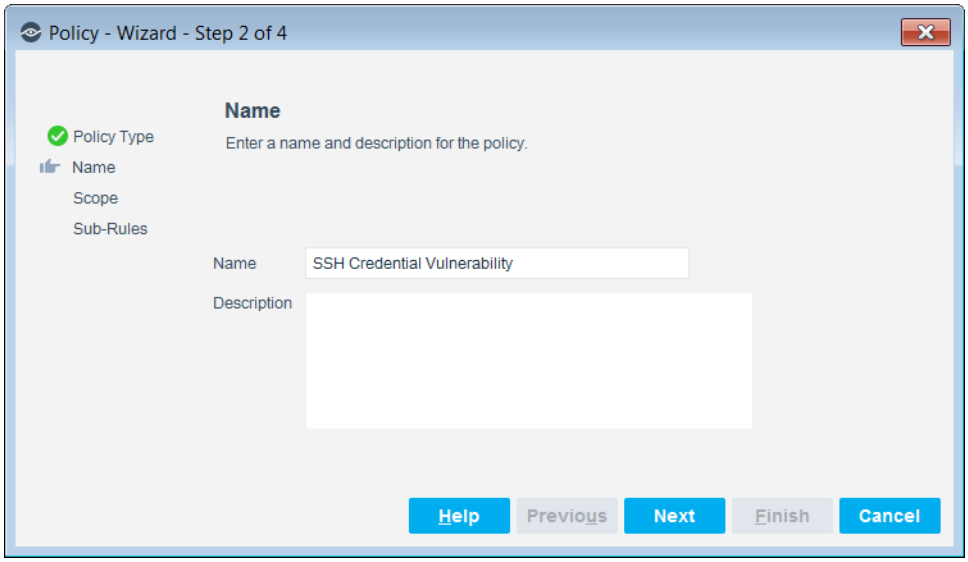
After a policy is run, you can see the endpoints that the policy detected.

To use the IoT Posture Assessment policy templates:

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 IoT Posture Assessment folder and select the appropriate communication protocol:
   - SNMP
   - SSH
   - Telnet



4. Select **Next.** The policy wizard opens to the **Name** pane.



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.

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

   Naming Tips

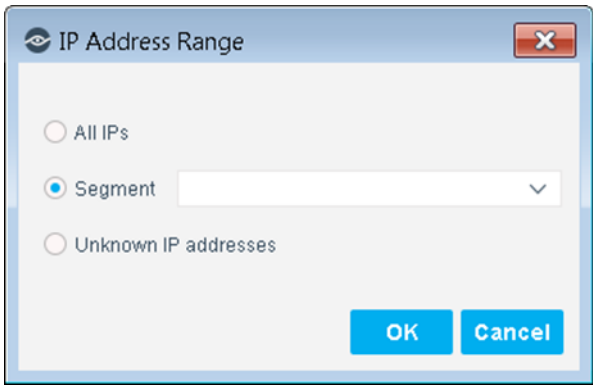
   – Make sure names are accurate and clearly reflect what the policy does. For example, do not use a generic name such as My_Compliance_Policy.

- The name should indicate what the policy verifies and what actions are taken.
- The name should indicate whether policy criteria must be met or not met.
- Avoid having another policy with a similar name.

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

Define Which Hosts Will Be Inspected - Policy Scope

7. Use the IP Address Range dialog box to define which endpoints are inspected.



Define Policy Scope

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** to close this dialog box, and select **Segments** from the Scope page.
- **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.

8. Select **OK**. The added range displays in the Scope pane.
9. (Optional) To review and modify default policy logic before you create the policy, select **Next**. The Main Rule pane displays.

How Devices are Detected and Handled

Policy rules instruct CounterACT how to detect and handle endpoints defined in the policy scope.

Endpoints that match the Main Rule pass to sub-rules of the policy for further evaluation. *Endpoints that do not match the Main Rule are not passed to sub-rules of the policy*. Sub-rules let you automatically follow up initial detection and handling with additional detection and remediation actions, in one automated sequence.

For each endpoint that matches the Main Rule, the condition of each sub-rule is evaluated in order until a condition is matched. If an endpoint does not match the condition of a sub-rule, evaluation moves to the next rule.

When a match is found, the corresponding actions are applied to the endpoint. No further sub-rules are evaluated for this endpoint.

Main Rule

The main rule of this policy detects devices that are classified as one of the following:

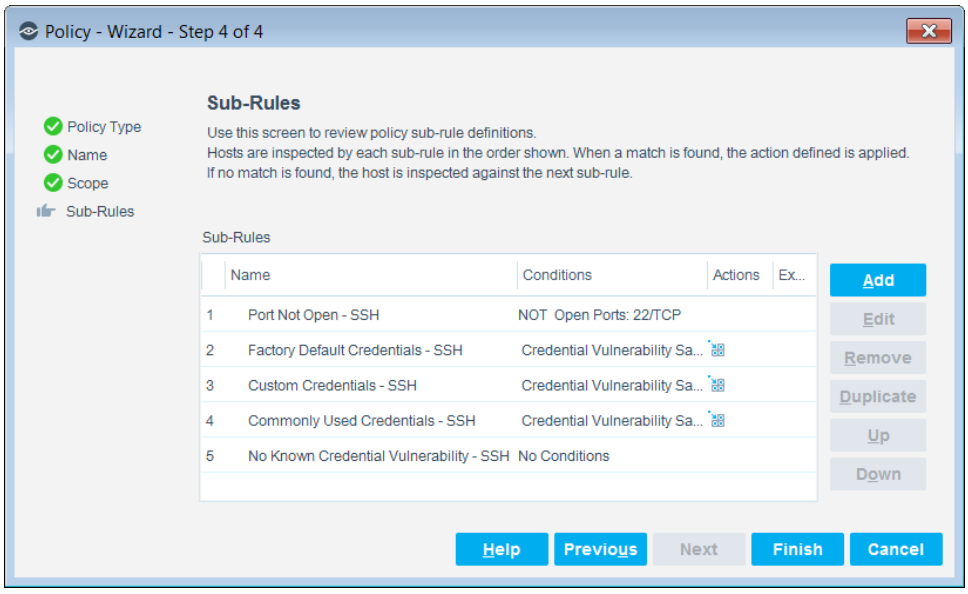
- IP Camera
- Router or Switch
- Printer

The Main Rule pane is available when you edit an existing policy.

10. Select **Next**. The Sub-Rules pane displays.

Sub-Rules

The sub-rules of the policy resolve the Credential Vulnerability Property of the device.



You can **Add** conditions and actions. A list of these items can be found in the *CounterACT Administration Guide*. See Additional CounterACT Documentation for information about how to access this guide.

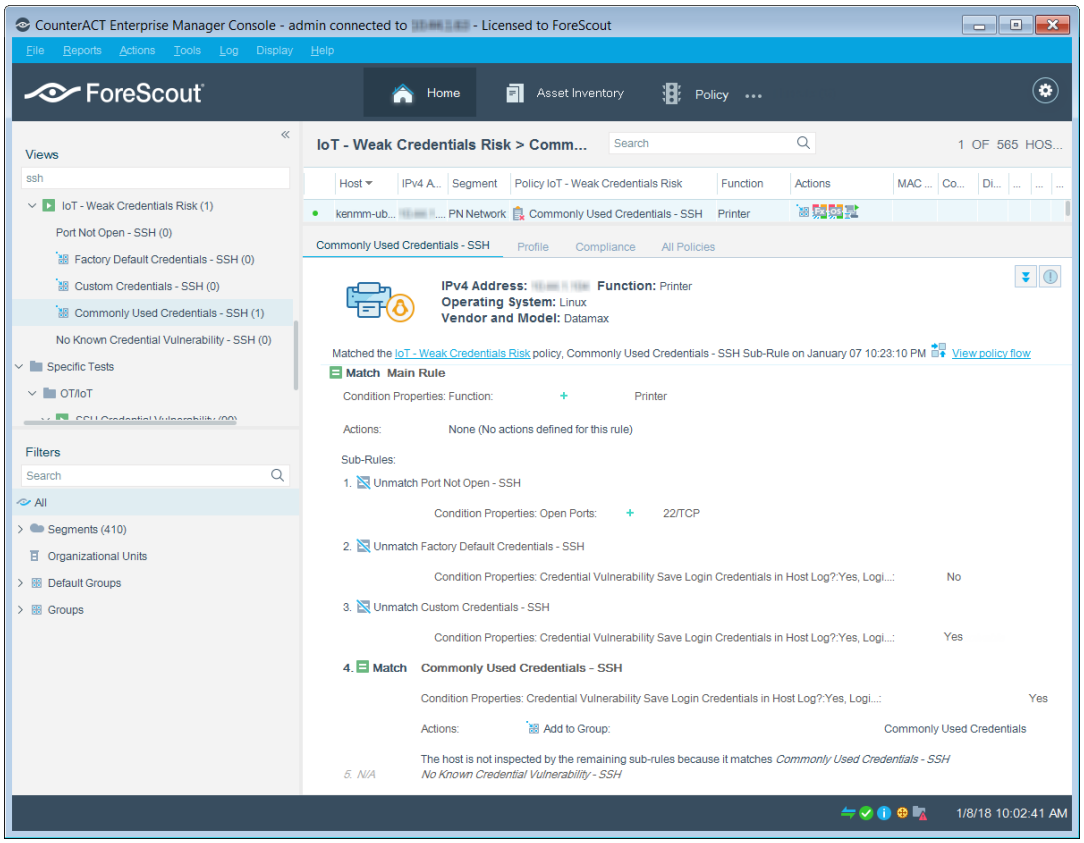
11. Select **Finish**.

12. On the CounterACT Console, select **Apply** to save the policy.

Policy Overview

To see an overview of your policies:

1. In the Console Home tab, Views pane, expand the Policies folder.
2. Expand the folder of the IoT Posture Assessment policy that you created. Each policy sub-rule name is displayed, followed by the number of endpoints that matched it.
3. Select a sub-rule. The endpoints that matched the rule are displayed in the Detections pane.



About Custom Policies

CounterACT policy tools provide you with an extensive range of options for detecting and handling endpoints. You can use a policy to instruct CounterACT to apply actions to endpoints that match conditions based on the Credential Vulnerability Property.

Core Extensions Module Information

The IoT Posture Assessment Engine is installed with the CounterACT Core Extensions Module.

The Core Extensions Module provides an extensive range of capabilities that enhance the core CounterACT solution. These capabilities enhance detection, classification, reporting, troubleshooting and more, and include the following components:

- Advanced Tools Plugin
- CEF Plugin
- DHCP Classifier Plugin
- DNS Client Plugin
- DNS Enforce Plugin
- DNS Query Extension Plugin
- Device Classification Engine
- External Classifier Plugin
- Flow Analyzer Plugin
- IOC Scanner Plugin
- IoT Posture Assessment Engine
- NBT Scanner Plugin
- NetFlow Plugin
- Reports Plugin
- Syslog Plugin
- Technical Support Plugin
- Web GUI Plugin

The Core Extensions Module is a ForeScout Base Module. Base Modules are delivered with each CounterACT release.

Components listed above are released and rolled back with the Core Extensions Module.

Refer to the *CounterACT Core Extensions Module Guide* for more module information, for example module requirements, upgrade and rollback instructions. See *Additional CounterACT Documentation* for information about how to access the module guide.

Additional CounterACT Documentation

For information about other CounterACT features and modules, refer to the following resources:

- Documentation Downloads
- Documentation Portal

- CounterACT Help Tools

Documentation Downloads

Documentation downloads can be accessed from one of two ForeScout portals, depending on which licensing mode your deployment is using.

- ***Per-Appliance Licensing Mode*** - Product Updates Portal
- ***Centralized Licensing Mode*** - Customer Portal

Software downloads are also available from these portals.

To learn which licensing mode your deployment is using, see Identifying Your Licensing Mode in the Console.

Product Updates Portal

The Product Updates Portal provides links to CounterACT version releases, Base and Content Modules, and Extended Modules, as well as related documentation. The portal also provides a variety of additional documentation.

To access the Product Updates Portal:

1. Go to https://updates.forescout.com/support/index.php?url=counteract.
2. Select the CounterACT version you want to discover.

Customer Portal

The Downloads page on the ForeScout Customer Portal provides links to purchased CounterACT version releases, Base and Content Modules, and Extended Modules, as well as related documentation. Software and related documentation will only appear on the Downloads page if you have a license entitlement for the software. The Documentation page on the portal provides a variety of additional documentation.

To access documentation on the ForeScout Customer Portal:

1. Go to https://forescout.force.com/support/.
2. Select **Downloads** or **Documentation**.

Documentation Portal

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

If your deployment is using Centralized Licensing Mode, you may not have credentials to access this portal.

To access the Documentation Portal:

1. Go to www.forescout.com/docportal.
2. Use your customer support credentials to log in.
3. Select the CounterACT version you want to discover.

CounterACT 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.

CounterACT Administration Guide

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 **Modules**.
2. Select the plugin and then select **Help**.

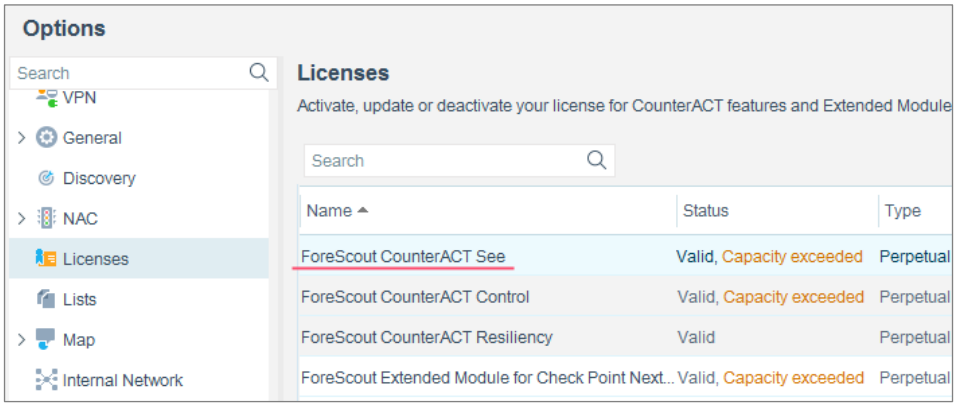
Documentation Portal

Select **Documentation Portal** from the **Help** menu.

Identifying Your Licensing Mode in the Console

If your Enterprise Manager has a *ForeScout CounterACT See* license listed in the Console, your deployment is operating in Centralized Licensing Mode. If not, your deployment is operating in Per-Appliance Licensing Mode.

Select **Options > Licenses** to see whether you have a *ForeScout CounterACT See* license listed in the table.



Contact your ForeScout representative if you have any questions about identifying your licensing mode.

Legal Notice

2018-04-10 09:21