FORESCOUT

Forescout

Core Extensions Module: IoT Posture Assessment Engine

Configuration Guide

Version 1.1.1

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

Legal Notice

2019-02-12 13:32

Table of Contents

About the IoT Posture Assessment Engine

The IoT Posture Assessment Engine is a component of the Forescout® 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 the Forescout platform 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 for various devices
- a set of commonly used credentials
- a custom list of credentials provided by you

When authentication succeeds, the device matches the condition.

Considerations

- The SSH Credential Vulnerability condition for Factory Default Credentials may be resolved incorrectly for a CounterACT® Appliance that is managed by itself.
- For Linux and OS X endpoints managed by the Linux and OS X Plugins using Remote Inspection, the Credential Vulnerability property always matches the condition for Commonly Used Credentials, and the Host Log would indicate that the Forescout platform logged in using username='root' and password='password'. This occurs even when no credentials are configured.

What to Do

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

1. Verify that you have met system requirements. See Forescout Requirements.
2. Before resolving a Credential Vulnerability condition for Factory Default Credentials, ensure that the device *Vendor and Model* classification property has been resolved by the Forescout Device Classification Engine. Refer to the *Forescout Device Classification Engine Configuration Guide*. See Additional Forescout Documentation for information about how to access this guide.
3. 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.
4. Install the IoT Posture Assessment Library whenever a new version is available. Refer to the *Forescout IoT Posture Assessment Library Configuration Guide*. See Additional Forescout Documentation for information about how to access this guide.

To help Forescout provide better classification and posture assessment services, opt in to the Forescout Research and Intelligent Analytics Program. This voluntary program uploads anonymous host information from your environment to be used by Forescout researchers to improve the product. Refer to The Forescout Research and Intelligent Analytics Program *section in the* Forescout Administration Guide *for more information about this program. See Additional Forescout Documentation for information on how to access the guide.*

Forescout Requirements

The IoT Posture Assessment Engine Plugin requires the following:

- Forescout version 8.1.

- IoT Posture Assessment Library. This 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 upgraded periodically 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.

About Support for Dual Stack Environments

Forescout version 8.1 detects endpoints and interacts with network devices based on both IPv4 and IPv6 addresses. However, ***IPv6 addresses are not yet supported by this module.*** The functionality described in this document is based only on IPv4 addresses. IPv6-only endpoints are typically ignored or not detected by the properties, actions, and policies provided by this module.

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.

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.

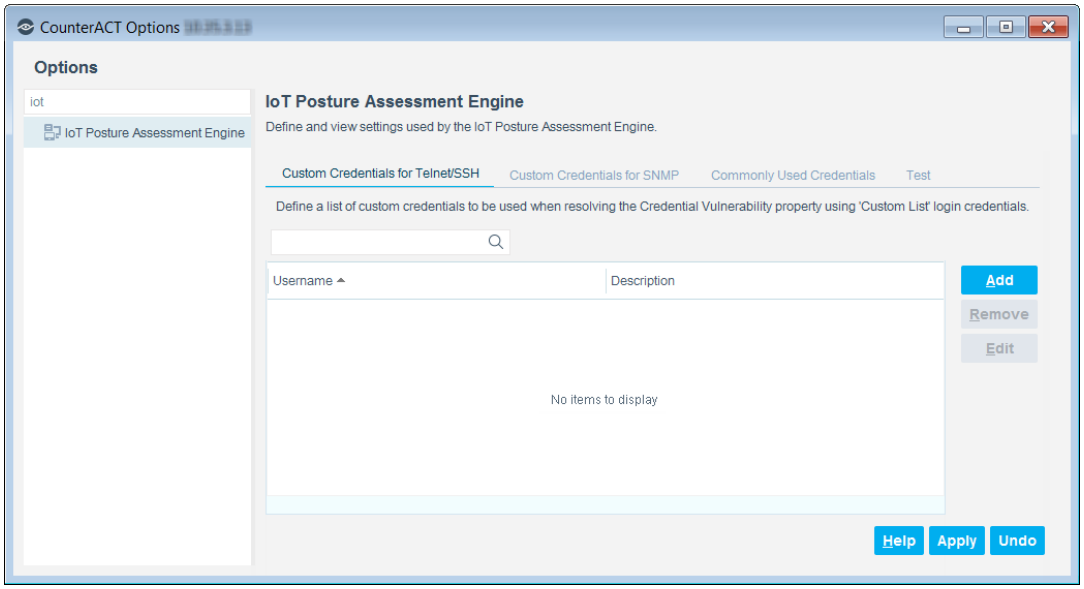
To verify:

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

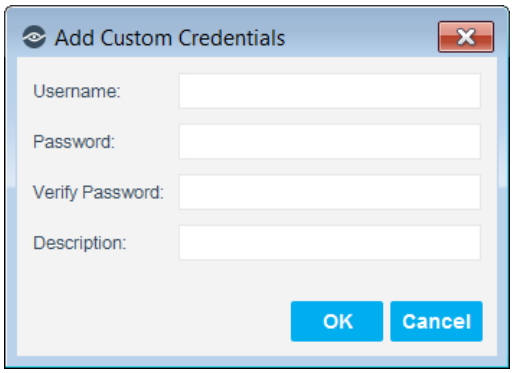
Custom Credentials

To define custom credentials checked by the Credential Vulnerability property:

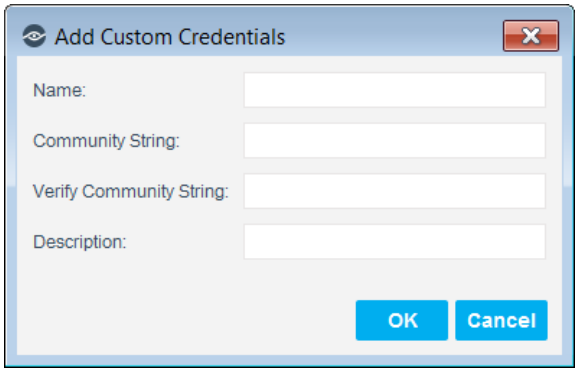
1. Select **Options** from the Console **Tools** menu, and select **IoT Posture Assessment Engine**.



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**.



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



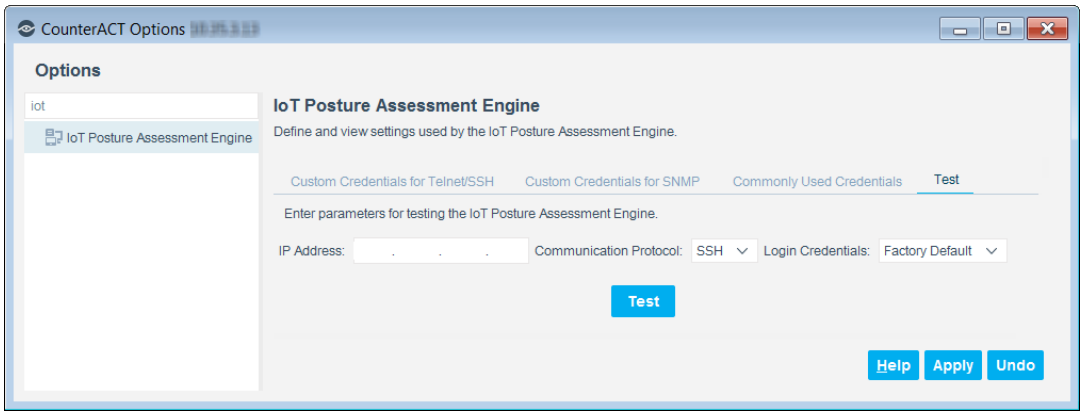
Test the Plugin

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

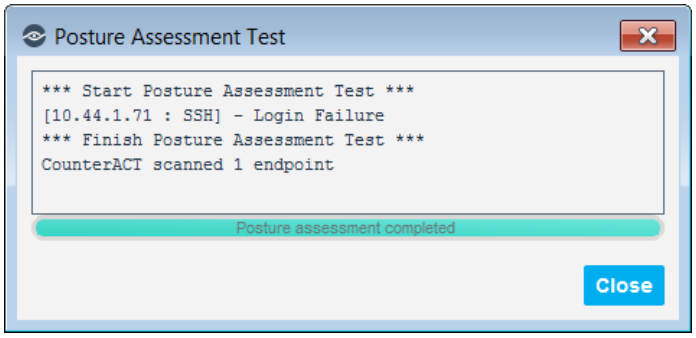
Plugin test results for Factory Default Credentials are unreliable in an environment with more than one CounterACT Appliance.

To test the plugin:

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



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.

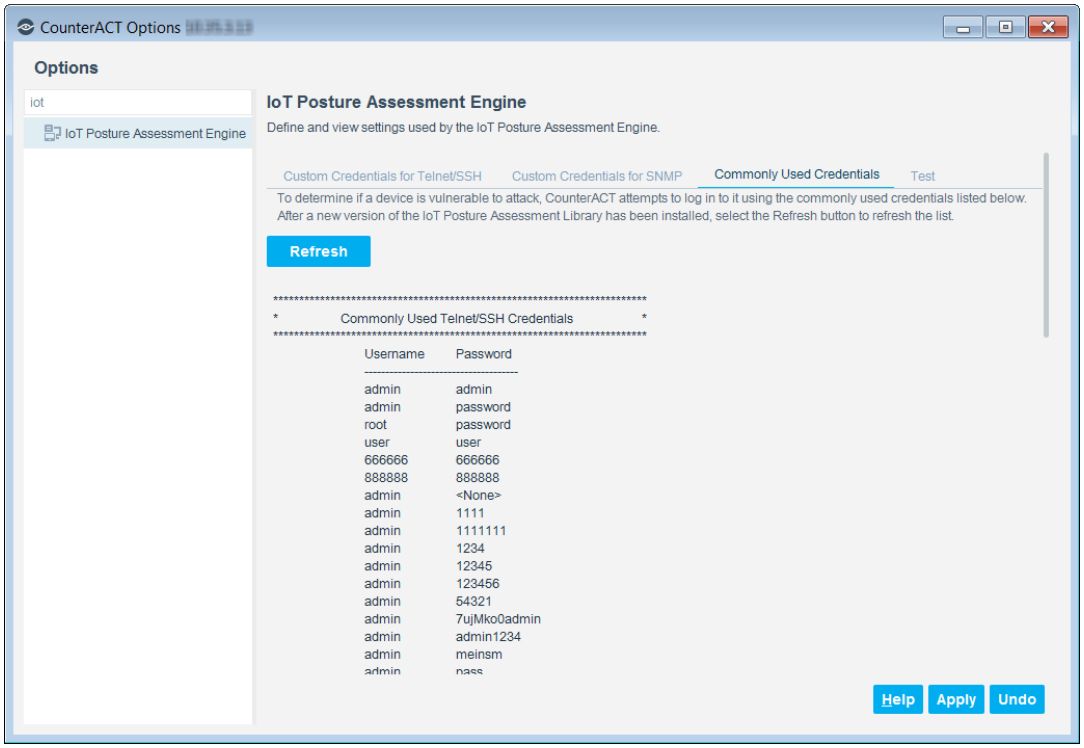
View the List of Commonly Used Credentials

You can view the list of commonly used credentials checked by the Credential Vulnerability property. These credentials, provided by the IoT Posture Assessment Library, were obtained from various sources on the Internet and are known to be used by hackers and malware.

Some credentials that have been used in known attacks may contain offensive terms.

To view the list of commonly used credentials:

1. Select **Options** from the 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.

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 *Vendor and Model* classification property.

  Ensure that the Vendor and Model *classification property has been resolved for the device.*

  For a CounterACT Appliance that is managed by itself, the SSH Credential Vulnerability condition for Factory Default Credentials may be unreliable.

- Commonly used credentials, from the list provided by the IoT Posture Assessment Library. To view these credentials, see View the List of Commonly Used Credentials.

  For Linux and OS X endpoints managed by the Linux and OS X Plugins using Remote Inspection, the Credential Vulnerability property always matches the condition for Commonly Used Credentials, even when no credentials are configured.

- Custom credentials, from a list provided by the Forescout platform operator in the IoT Posture Assessment Engine options.

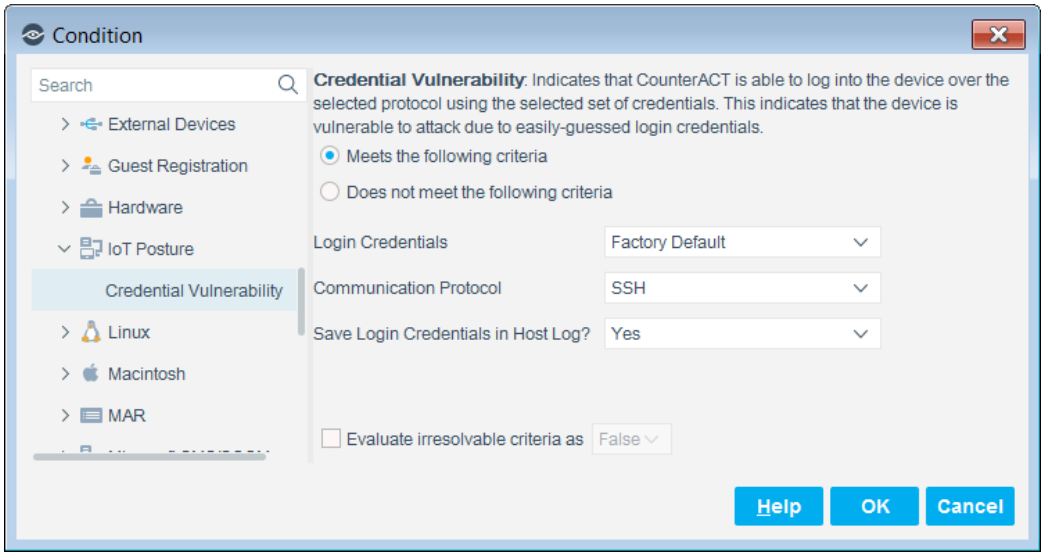
For more information about the IoT Posture Assessment Library, refer to the *Forescout IoT Posture Assessment Library Configuration Guide*. See Additional Forescout Documentation for information about how to access this guide.

The Forescout platform 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. Go 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

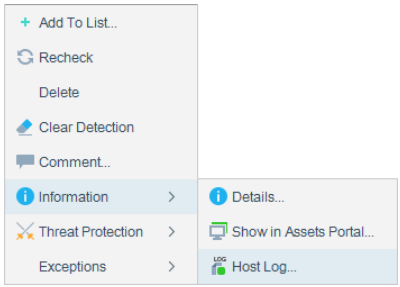
5. To save the login credentials used for successful login so that they can be viewed in the Host Log, select **Yes**. When this option is selected, credentials are saved in clear text in order to support your remediation efforts. See View the Credentials Used for Successful Login.

View the Credentials Used for Successful Login

If the Credential Vulnerability property was configured to save the credentials used for successful login, you can view the credentials in the Host Log.

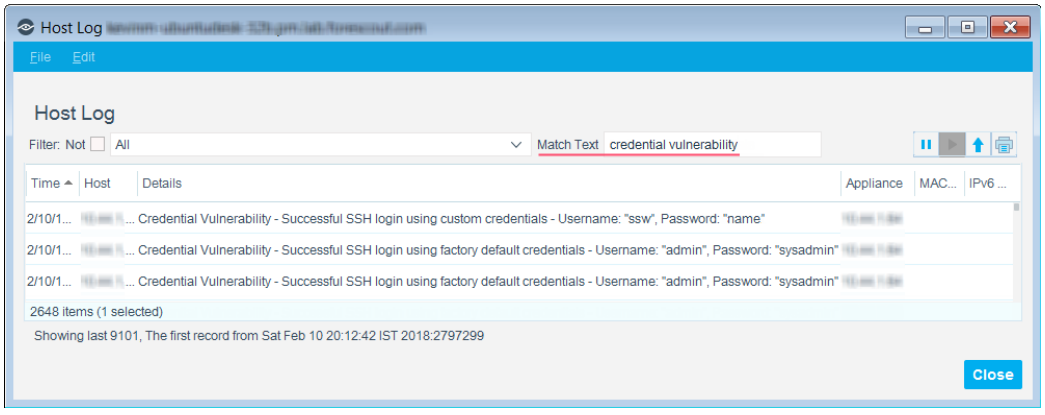
To view the credentials used for successfully logging in:

1. In the Console, right-click the device and select **Information > Host Log**.



2. Enter a time range and select **OK**.
3. In the Match Text field, enter **credential vulnerability**, or any part of that term, and press **Enter**.

   The credentials used by the property for successful login within the specified time range are displayed.



*Other information containing the term **credential vulnerability** may also be displayed.*

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.

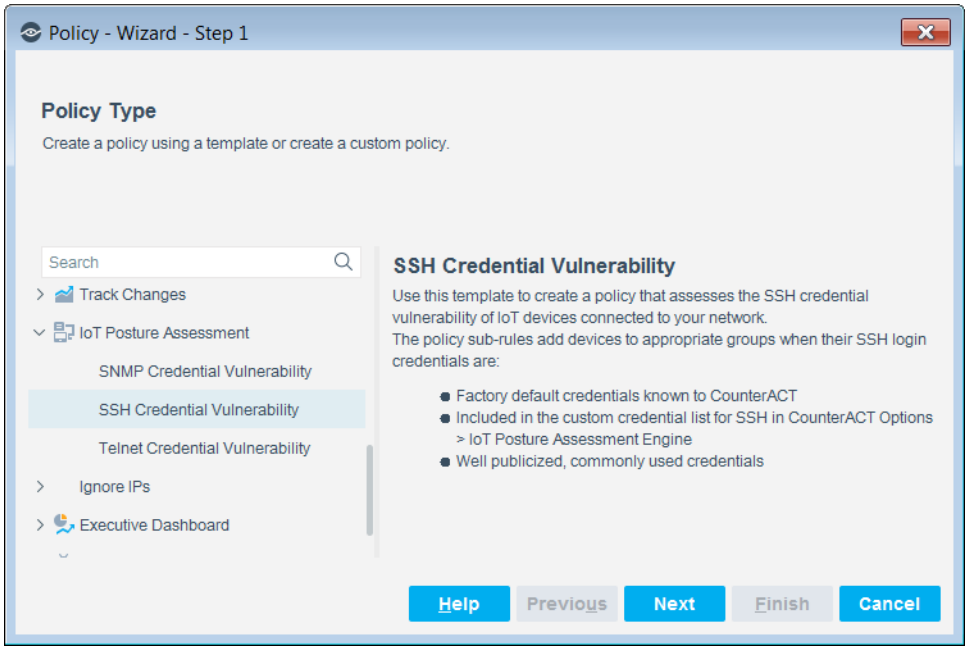
Sub-rules provided by the templates detect endpoints determined to be vulnerable to botnet and other attacks based on the use of weak login credentials. Policy actions add the vulnerable devices to one of the following groups:

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

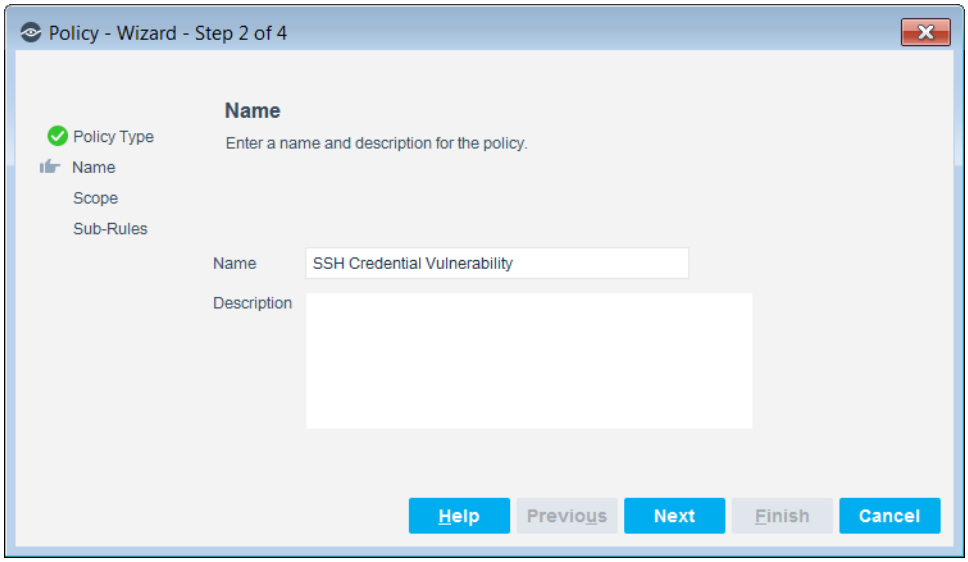
After a policy is run, you can see the endpoints that the policy detected.

To use the IoT Posture Assessment policy templates:

1. Log in to the Console and select **Policy**.
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.**



Name the Policy

The Name pane lets you define a unique policy name and useful policy description. 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.

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

   Naming Tips

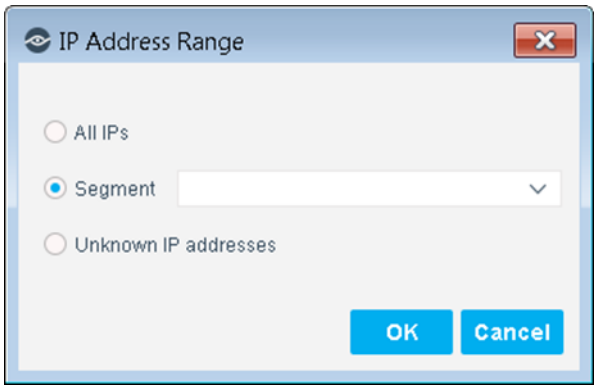
   – Make sure names are accurate and clearly reflect what the policy does. For example, do not use a generic name such as My_Compliance_Policy.

- 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.** Both the Scope pane and the IP Address Range dialog box open.

Define Which Hosts Will Be Inspected - Policy Scope

7. 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.

  Not applicable for this policy template.

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

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

How Devices are Detected and Handled

Policy rules instruct the Forescout platform 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:

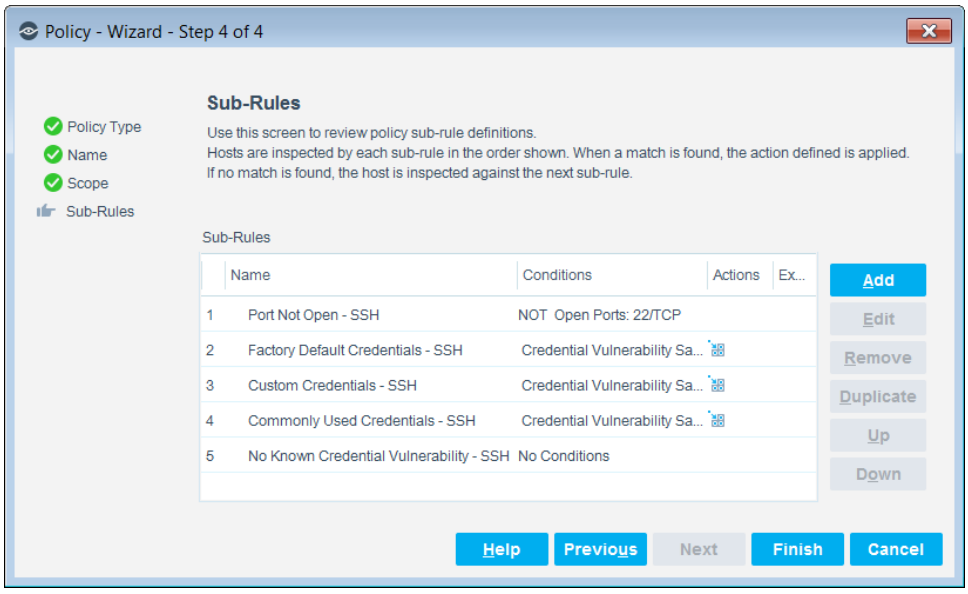
- IP Camera
- Router or Switch
- Printer

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

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

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 *Forescout Administration Guide*. See Additional Forescout Documentation for information about how to access this guide.

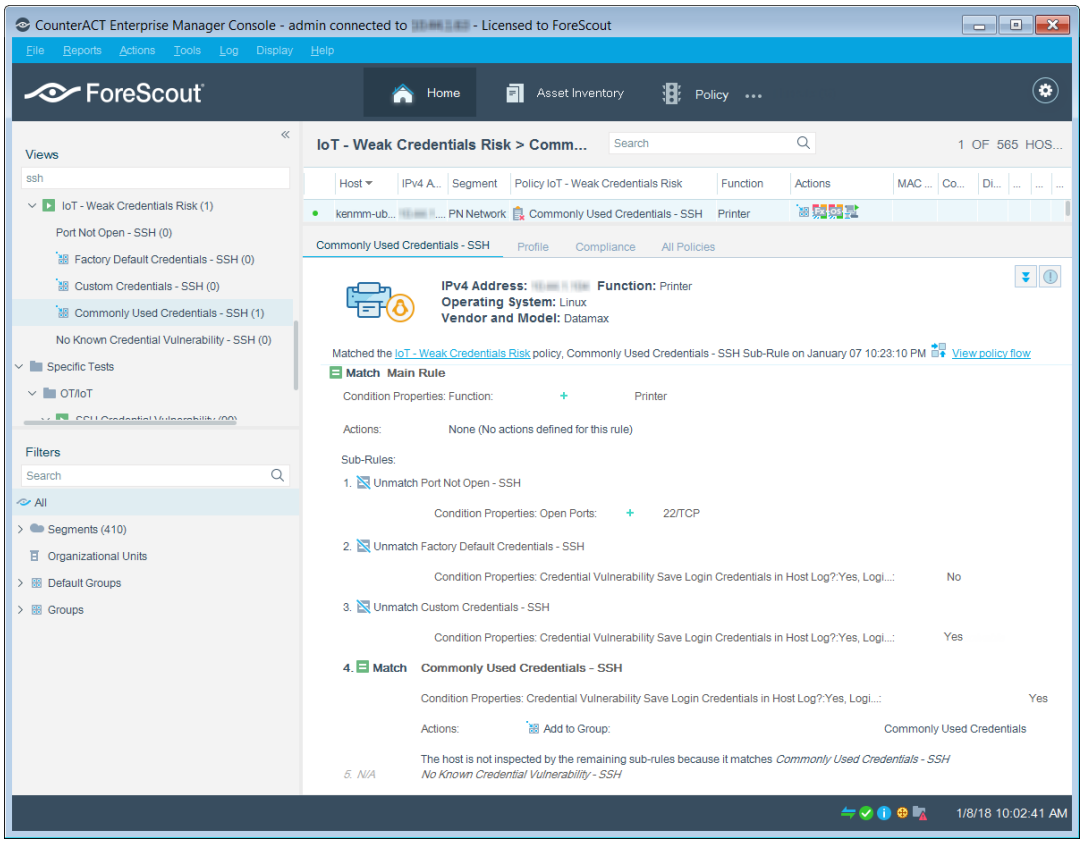
11. Select **Finish**.

12. In the 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

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

Share Data with Forescout

To help Forescout provide better classification and posture assessment services, opt in to the Forescout Research and Intelligent Analytics Program. This voluntary program uploads anonymous information from your environment to be used by Forescout researchers to improve the product. It also lets you share with Forescout additional information that will aid Forescout in capturing your requirements in future content updates. To opt in to the program, go to Tools > Options > Advanced > Data Sharing, and select **Allow selected endpoint properties to be shared with Forescout**. For more information about this program, refer to *The Forescout Research and Intelligent Analytics Program* section in the *Forescout Administration Guide*. See Additional Forescout Documentation for information on how to access the guide.

Core Extensions Module Information

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

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

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

The Core Extensions Module is a Forescout Base Module. Base Modules are delivered with each Forescout release. This module is automatically installed when you upgrade the Forescout version or perform a clean installation.

Additional Forescout Documentation

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

- Documentation Downloads
- Documentation Portal
- Forescout Help Tools

Documentation Downloads

Documentation downloads can be accessed from the Forescout Resources Page, or one of two Forescout portals, depending on which licensing mode your deployment is using.

- ***Per-Appliance Licensing Mode*** – Product Updates Portal
- ***Flexx Licensing Mode*** – Customer Portal

Software downloads are also available from these portals.

To identify your licensing mode:

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

Forescout Resources Page

The Forescout Resources Page provides links to the full range of technical documentation.

To access the Forescout Resources Page:

- Go to https://www.Forescout.com/company/resources/, select **Technical Documentation** and search for documents.

Product Updates Portal

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

To access the Product Updates Portal:

- Go to https://updates.forescout.com/support/index.php?url=counteract and select the version you want to discover.

Customer Portal

The Downloads page on the Forescout Customer Portal provides links to purchased Forescout version releases, Base and Content Modules, and eyeExtend products, 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.

To access documentation on the Forescout Customer Portal:

- Go to https://Forescout.force.com/support/ and select **Downloads**.

Documentation Portal

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

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

To access the Documentation Portal:

- Go to https://updates.forescout.com/support/files/counteract/docs_portal/ and use your customer support credentials to log in.

Forescout Help Tools

Access information directly from the Console.

Console Help Buttons

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

Forescout Administration Guide

- Select **Forescout Help** from the **Help** menu.

Plugin Help Files

- After the plugin is installed, select **Tools** > **Options** > **Modules**, select the plugin and then select **Help**.

Online Documentation

- Select **Online Documentation** from the **Help** menu to access either the Forescout Resources Page (Flexx licensing) or the Documentation Portal (Per-Appliance licensing).