ForeScout® Extended Module for Qualys® VM

Configuration Guide

Version 1.3

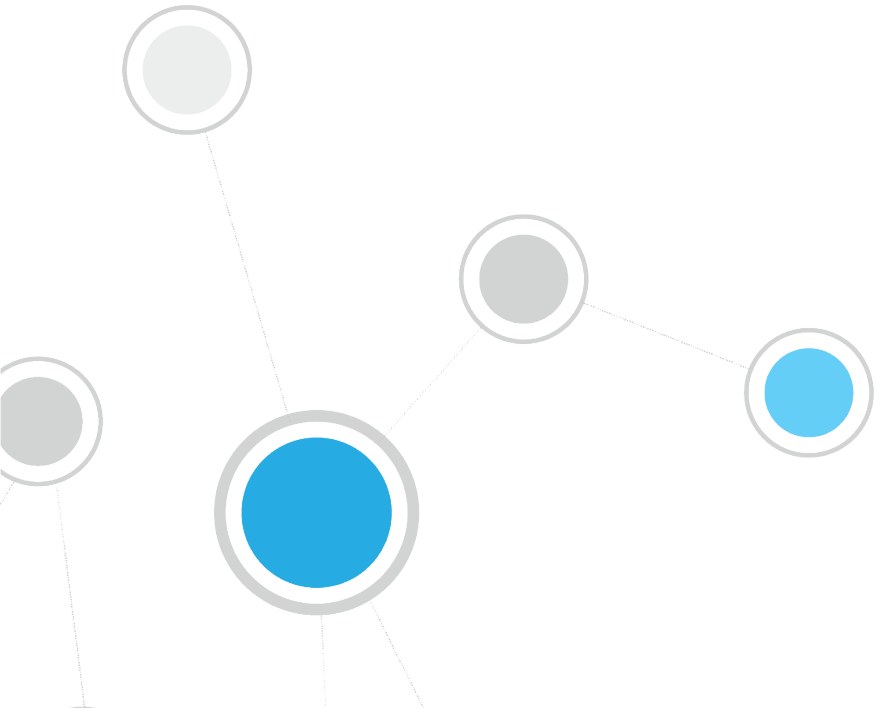


Table of Contents

About the Qualys VM Integration 3
Additional Qualys VM Documentation 3

About This Module 3
Components 4
Considerations 4
What to Do 5

Requirements 5
CounterACT Software Requirements 6
About Support for Dual Stack Environments 6
ForeScout Extended Module License Requirements 6
Per-Appliance Licensing Mode 7
Centralized Licensing Mode 8
More License Information 8

Configure the Qualys Environment 8

Install the Module 9

Configure the Module 10
Add Qualys Option Profiles 11
Add Qualys Scanner Appliances 12
Add a Qualys Cloud Platform 13
Define Test Configuration Parameters 16

Disable Discovery of Qualys Host Properties 18

Test the Module 19

Run Qualys VM Policy Templates 21
Basic Qualys VM Scan Trigger Template 22
Qualys VM Severity Results Template 26

Create Custom CounterACT Policies 29
Detecting Vulnerabilities – Policy Properties 29
Scanning Endpoints - Policy Actions 31
Launch Qualys Scan 31

Display Qualys VM Asset Inventory Information 32

Additional CounterACT Documentation 34
Documentation Downloads 34
Documentation Portal 35

CounterACT Help Tools.....35

About the Qualys VM Integration

Vulnerability assessment is a process that defines, identifies, classifies and prioritizes the security vulnerabilities in a computer, network or communications infrastructure. Vulnerability assessment and management tools play a critical role in enterprise vulnerability management.

Qualys Cloud Platform, formerly known as QualysGuard, is a cloud–based suite of IT security and compliance solutions that includes Qualys VM (Vulnerability Management).

The ForeScout CounterACT® Qualys VM Module lets you integrate CounterACT with Qualys Cloud Platform vulnerability management tools. Create CounterACT policies to monitor, manage, restrict and remediate endpoints in real-time, based on Qualys scan results.

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

Additional Qualys VM Documentation

Refer to Qualys online documentation for more information about the Qualys VM solution:

https://community.qualys.com/docs/DOC-4802

About This Module

CounterACT bi-directional communication with the Qualys Cloud Platform offers several unique capabilities:

- CounterACT can launch a Qualys scan based on detected network activity. For example, scan an endpoint on its admission to the network or if a specific application is installed. See Scanning Endpoints - Policy Actions.
- CounterACT evaluates Qualys scan results and can trigger actions. For example, if a Critical vulnerability severity is detected on an endpoint, CounterACT can apply an action that triggers another scan, or one that restricts corporate network access.
- The CounterACT Asset Inventory displays which endpoints have been identified as vulnerable by the module. See Display Qualys VM Inventory Information.

  Information detected also appears in the CounterACT Dashboard and in CounterACT reports. Refer to the CounterACT Online Help for details about these features.

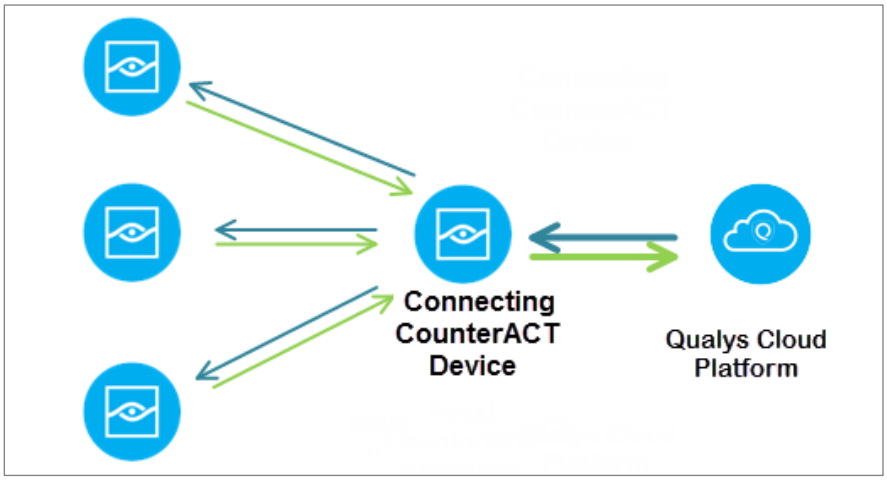
Components

Qualys Cloud Platform: The organization's Qualys Cloud Platform can be located in either a public or a private cloud.

Connecting CounterACT Devices and assigned devices: A CounterACT Appliance or Enterprise Manager must be defined as the Connecting Device through which other CounterACT Appliances or Enterprise Managers communicate with the organization's Qualys Cloud Platform. The Connecting Device functions as a proxy, handing queries and requests submitted by all the devices assigned to it. If there are multiple Qualys Cloud Platform definitions, each requires its own Connecting CounterACT Device. One CounterACT device is defined as the *default* Connecting Device to handle communication for all devices not assigned to any other Connecting Device.

Each Connecting CounterACT Device must have connectivity to its Qualys Cloud Platform. CounterACT devices that are assigned to Connecting Devices do not require connectivity to the Qualys Cloud Platform.

Each CounterACT device can be assigned to only one Connecting Device. Each Connecting Device can communicate with only one Qualys Cloud Platform.



Considerations

CounterACT launches Qualys scans using Qualys Cloud Platform parameters. The following parameters must be either selected during manual scan launch or defined in the policy that launches a scan:

- Qualys Option Profile: controls which information is gathered during a scan
- Qualys Scanner Appliance: controls which Qualys scanner is used

If an Option Profile or Scanner Appliance name is changed or added in the Qualys Cloud Platform, the name in the CounterACT module configuration must be set accordingly. See Add Qualys Option Profiles and Add Qualys Scanner Appliances.

The Qualys operator must ensure the following conditions:

- There is a Qualys Report Template named **ForeScout Vulnerability Report** that is not limited to any Asset Group or IP range. See Configure the Qualys Environment.
- The Option Profile name selected from the names configured in the Qualys VM Module matches the name of a Qualys Option Profile that is not limited to any Asset Group or IP range.
- All endpoints to be scanned:
  - must be included as host assets in the Qualys subscription
  - must be within the scope defined in the CounterACT policy

Consider the following when using the CounterACT Qualys VM Module:

- The module resolves properties using the Qualys host-based **ForeScout Vulnerability Report** data. To configure the report, see Configure the Qualys Environment.
- The module receives updated Qualys Cloud Platform scan results for specific endpoints whenever a CounterACT-initiated scan of those endpoints completes.
- Qualys enforces limits on their customers' API calls based on subscription settings. The default API limit is 300 calls per hour. Qualys blocks API calls that exceed the API call rate limit. Due to the Qualys API call limit, there may be a lag of several minutes between actual scan completion and the module's access to the scan report. See Disable Discovery of Qualys Host Properties.

What to Do

This section lists the steps you should take to set up your system when integrating with Qualys VM:

1. Verify that you have met system requirements. See Requirements.
2. Configure the Qualys Environment.
3. Install the Module.
4. Configure the Module.
5. Test the Module.
6. Create Custom CounterACT Policies.

Requirements

This section describes:

- CounterACT Software Requirements
- About Support for Dual Stack Environments
- ForeScout Extended Module License Requirements

CounterACT Software Requirements

The module requires the following CounterACT release:

- CounterACT version 8.0
- A module license for the Qualys VM Module
- An active Maintenance Contract for the licensed module

About Support for Dual Stack Environments

CounterACT version 8.0 detects endpoints and interacts with network devices based on both IPv4 and IPv6 addresses. However, ***IPv6 addresses are not yet supported by this component.*** 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 component.

ForeScout Extended Module License Requirements

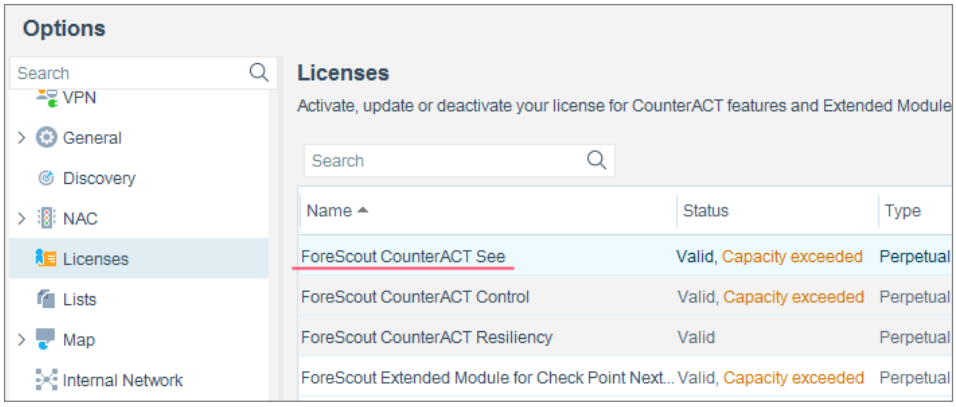
This ForeScout Extended Module requires a valid license. Licensing requirements differ based on which licensing mode your deployment is operating in:

- Per-Appliance Licensing Mode
- Centralized Licensing Mode

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.

Per-Appliance Licensing Mode

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

If you would like to continue exploring the module before purchasing a permanent license, you can request a demo license extension. Consult with your ForeScout representative before requesting the extension. You will receive email notification and alerts at the Console before the demo period expires.

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

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

> *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 CounterACT 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 CounterACT. You can request a license that handles more to ensure that you are licensed for support on additional devices as your deployment grows.

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

To view the number of currently detected devices:

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

Centralized Licensing Mode

When you set up your CounterACT deployment, you must activate a license file containing valid licenses for each feature you want to work with in your deployment, including Extended Modules. After the initial license file has been activated, you can update the file to add additional Extended Module licenses or change endpoint capacity for existing Extended Modules. For more information on obtaining Extended Module licenses, contact your ForeScout 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 Extended Module license has an associated capacity, indicating the number of endpoints the license can handle. The capacity of each Extended Module license varies by module, but does not exceed the capacity of the *See* license.

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

More License Information

Refer to the *CounterACT Administration Guide* for information on Extended Module licenses. You can also contact your ForeScout representative or license@forescout.com for more information.

Configure the Qualys Environment

Configure your Qualys environment for communication with CounterACT.

To configure your Qualys environment:

1. In the Qualys Enterprise Vulnerability Management window, create a Qualys user for the CounterACT module.
   a. Assign the user an email address at which status emails can be received.
   b. Assign the user a **Manager** role.

   c. Configure the user for **API**.

2. Log in as the newly-created user for the CounterACT module.
3. In the Reports Setup, enable **CVSS Scoring**.
4. Create a new Scan Report Template.
   a. Set the template **Title** to **ForeScout Vulnerability Report**.
   b. Set the template owner to the user created for the CounterACT module.
   c. In the Findings tab, select **Host Based Findings**, and set the Asset Groups to **All**. Do not change any other settings in the tab.
   d. In the Display tab, in the Graphics area, select **Vulnerabilities by Severity** and **Potential Vulnerabilities by Severity**.
   e. Do not change any other settings in the template.

*It is strongly recommended that the **ForeScout Vulnerability Report** template not be modified in the future.*

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 - ***Centralized Licensing Mode***

   To find out which licensing mode your deployment is working with, see Identifying Your Licensing Mode in the Console.
2. Download the module **`.fpi`** file.
3. Save the file to the machine where the CounterACT Console is installed.
4. Log into the CounterACT 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 will not proceed if you do not agree to the license agreement.

The installation will begin 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.

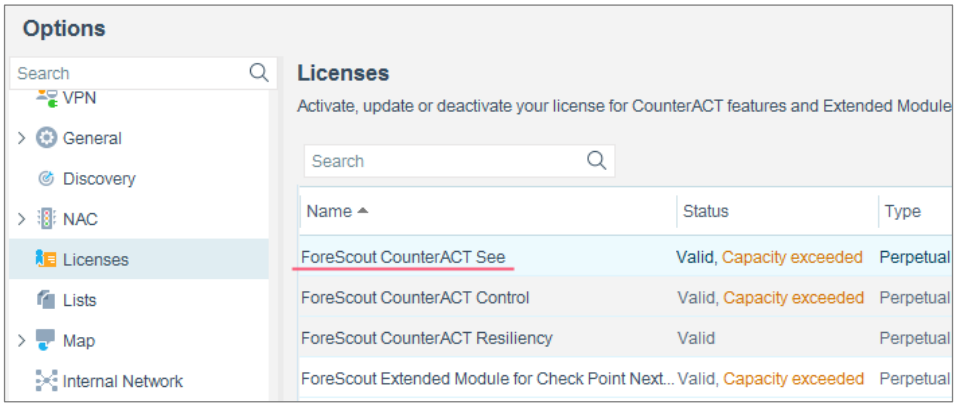
10. When the installation completes, select **Close** to close the window. The installed module is displayed in the Modules pane.

    Some components are not automatically started following installation.

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.



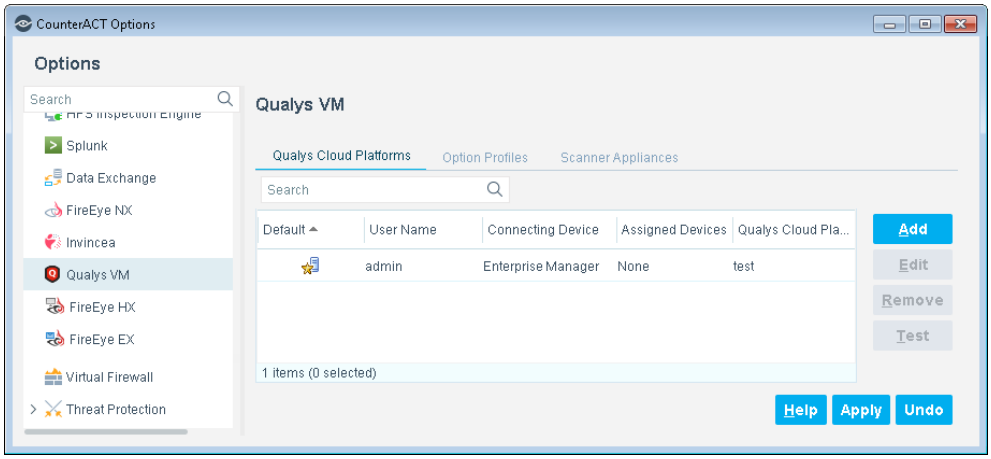
Contact your ForeScout representative if you have any questions about identifying your licensing mode.

Configure the Module

Configure the module to ensure that CounterACT can communicate with the Qualys VM service.

To configure the module:

1. In the CounterACT Console, select **Options** from the **Tools** menu. The Options dialog box opens.
2. Navigate to and select **Modules**.
3. In the **Modules** pane, select **Qualys VM**, and select **Configure**. The Qualys VM pane opens.



4. Do the following:
   a. Add Qualys Option Profiles.
   b. Add Qualys Scanner Appliances.
   c. Add a Qualys Cloud Platform.
   d. Define Test Configuration Parameters.

Add Qualys Option Profiles

Qualys Option Profiles determine which information Qualys gathers during a scan.

When CounterACT initiates a scan, CounterACT must pass to Qualys the name of a specific Option Profile.

Use the Option Profiles tab to add the Qualys Option Profile names to be used during scans launched by CounterACT. Option Profile names must be entered exactly as they appear in the Qualys Cloud Platform configuration.

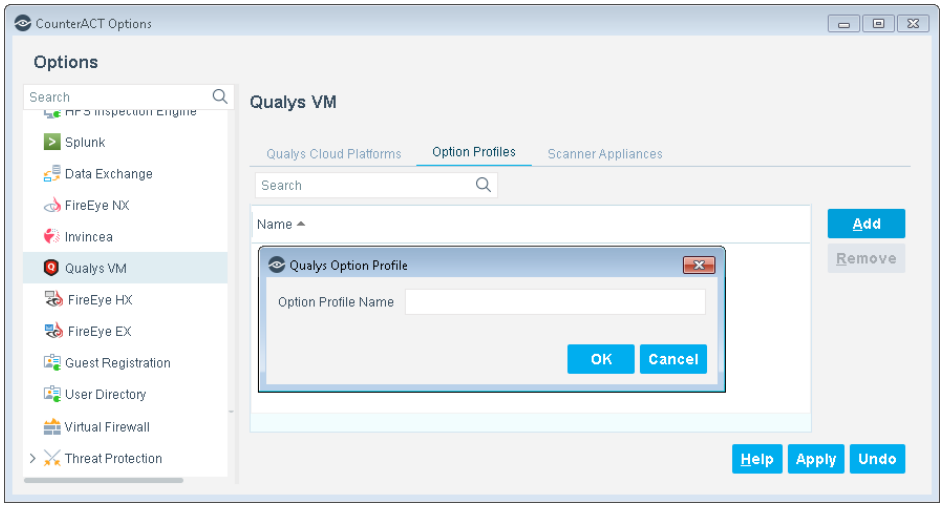
It is recommended to launch scans using the *Initial Options* or *Initial Options with Authentication* Option Profile to ensure complete vulnerability detection.

You cannot edit Option Profile names. To change a name for any reason, remove it and then add the correct name.

If an Option Profile is removed or renamed in the Qualys Cloud Platform, you must update the CounterACT module configuration. Qualys-related property resolution and actions will not be handled correctly in future scans if the Option Profile names in Qualys and in CounterACT do not match.

To add the name of an Option Profile:

1. In the Option Profiles tab, select **Add**. The Qualys Option Profile dialog box opens.



2. Enter the name of an Option Profile exactly as it appears in your Qualys Cloud Platform configuration.
3. Select **OK**. The Option Profile name appears in the Option Profiles pane.

Add Qualys Scanner Appliances

When a scan is launched, CounterACT must pass to Qualys the name of a specific Qualys Scanner Appliance to perform the scan.

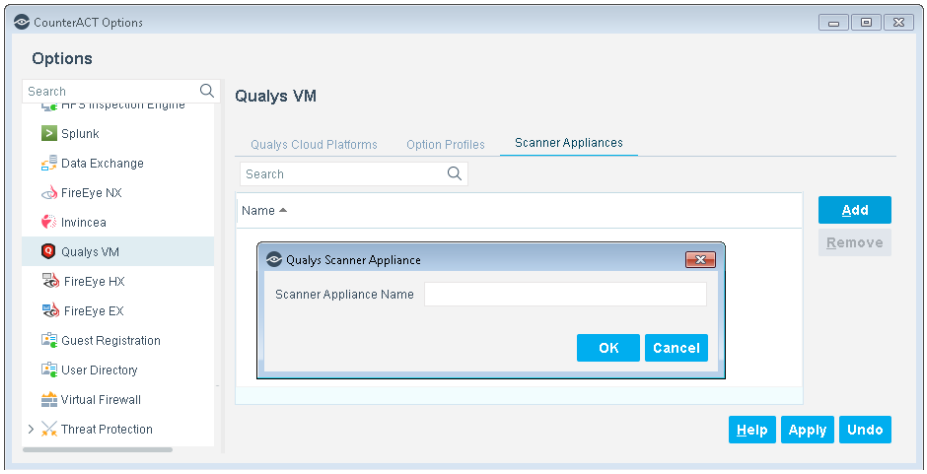
Use the Scanner Appliances tab to add the Scanner Appliance names to be used during Qualys scans launched by CounterACT. Scanner Appliance names must be entered exactly as they appear in the Qualys Cloud Platform configuration.

You cannot edit Scanner Appliance names. To change a name for any reason, remove it and then add the correct name.

If a Scanner Appliance is removed or renamed in the Qualys Cloud Platform, you must update the CounterACT module configuration. Future Qualys scans will not be handled correctly if the Scanner Appliance names in Qualys and in CounterACT do not match.

To add the name of a Scanner Appliance:

1. In the Scanner Appliances tab, select **Add**. The Qualys Scanner Appliance dialog box opens.



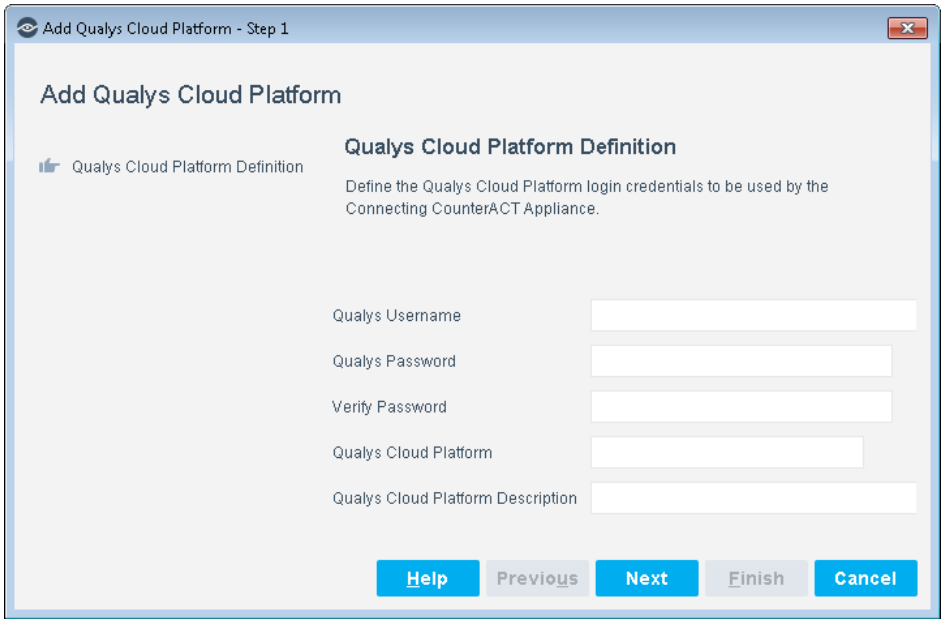
2. Enter the name of a Scanner Appliance exactly as it appears in your Qualys Cloud Platform configuration.
3. Select **OK**. The Scanner Appliance appears in the Scanner Appliances pane.

Add a Qualys Cloud Platform

Enter basic information about the Qualys Cloud Platform and select a Connecting CounterACT Device. You can configure multiple cloud platforms, each with a different Connecting CounterACT Device.

To add a Qualys Cloud Platform:

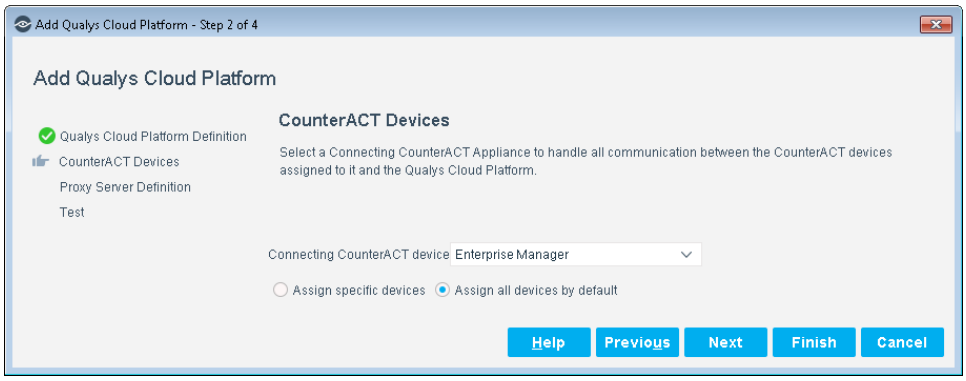
1. In the Qualys Cloud Platforms tab, select **Add**. The Add Qualys Cloud Platform wizard opens.



2. In the **Qualys Cloud Platform Definition** pane, configure the following connection parameters:

Qualys Username	Login name that has full access to the Qualys Cloud Platform. See step 1 of Configure the Qualys Environment.
Qualys Password	Password for the above user.
Verify Password	Retype the password to confirm it.
Qualys Cloud Platform	The URL of the Qualys Cloud Platform.
Qualys Cloud Platform Description	Description of the Qualys Cloud Platform, or a relevant comment.

3. Select **Next**. The **CounterACT Devices** pane opens.



4. In the **CounterACT Devices** pane, select a Connecting CounterACT Device through which other CounterACT devices will communicate with this Qualys Cloud Platform. Each CounterACT device can be assigned to only one Connecting Device. Each Connecting Device can communicate with only one Qualys Cloud Platform.

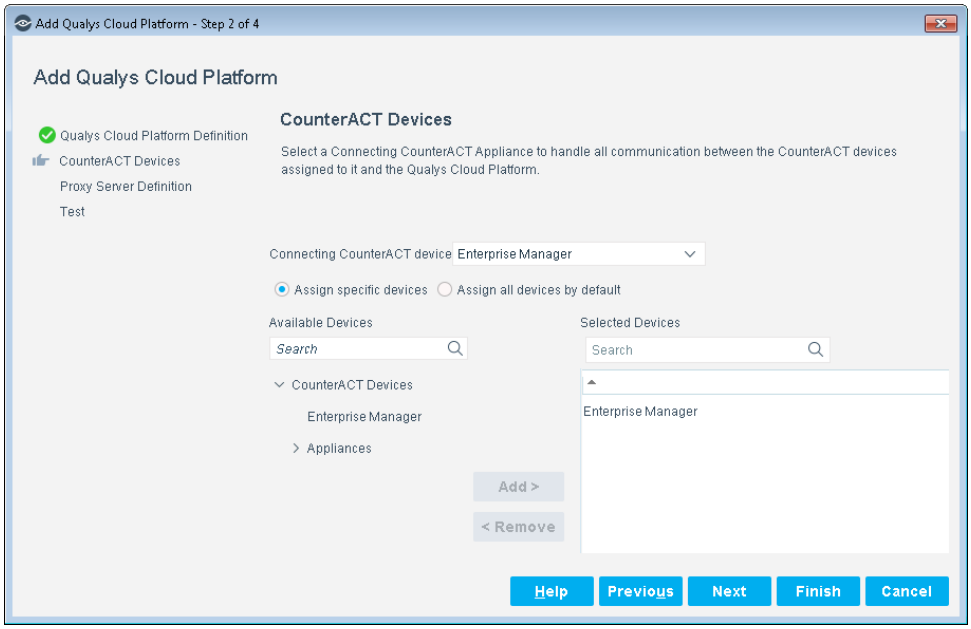
   – **Connecting CounterACT Device**: Select a CounterACT Appliance or Enterprise Manager to communicate with this Qualys Cloud Platform.

     This CounterACT device manages all communication with the defined Qualys Cloud Platform, including forwarding scan requests submitted to it by other CounterACT devices assigned to this Qualys Cloud Platform, and dispatching received scan results back to the appropriate devices.

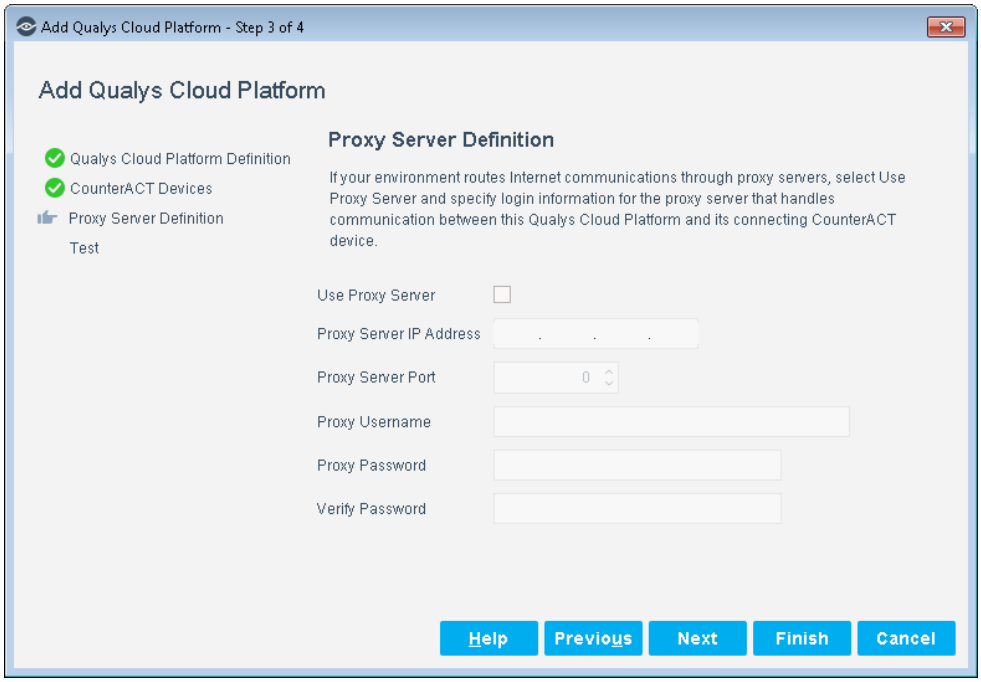
5. Select one of the following options:

   – **Assign all devices by default**: Automatically assign all CounterACT devices to this Connecting Device, excluding devices explicitly assigned to other Connecting Devices. The Connecting Device to which all CounterACT devices are automatically assigned is the *default* Connecting Device. Only one device can be designated as the *default*.

   – **Assign specific devices**: Assign specific CounterACT devices to communicate with the Qualys Cloud Platform through this Connecting Device.



6. Select **Next**. The **Proxy Server Definition** pane opens.



7. When your environment routes Internet communications through proxy servers, configure the following connection parameters for the proxy server that handles communication between this Qualys Cloud Platform and its connecting CounterACT device.

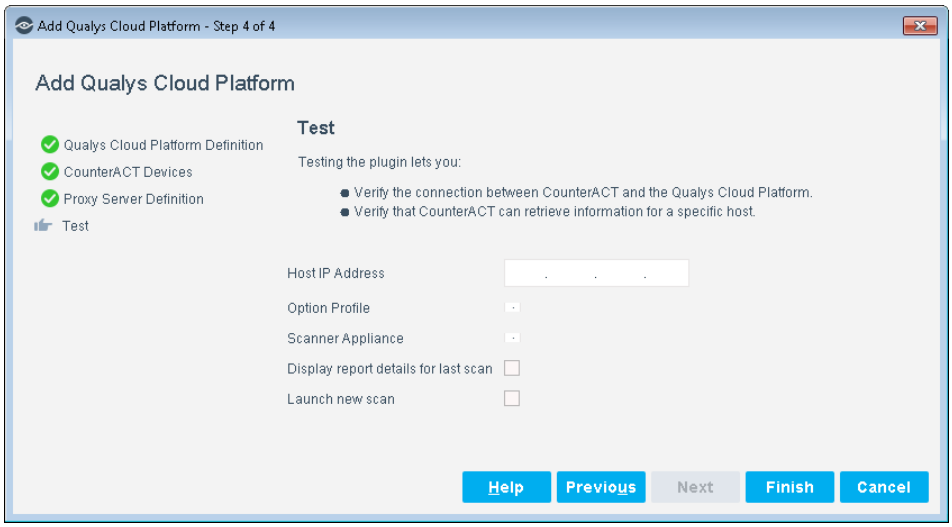
Use Proxy Server	Select this option to use a proxy server to communicate with the Qualys Cloud Platform.
Proxy Server IP Address	The network address of the proxy server.

Proxy Server Port	The port used to communicate with the proxy server.
Proxy Username	Login name for an authorized account defined on the proxy server, if required.
Proxy Password	Password for the above user, if required.
Verify Password	Retype the password to confirm it.

8. Select **Next**. The **Test** pane opens.

Define Test Configuration Parameters

Define the test configuration parameters to use when the module test is run. Completing these parameters does not trigger a test. To run the test, see Test the Module.



1. In the Test pane, configure the following fields to be used when the test is run:

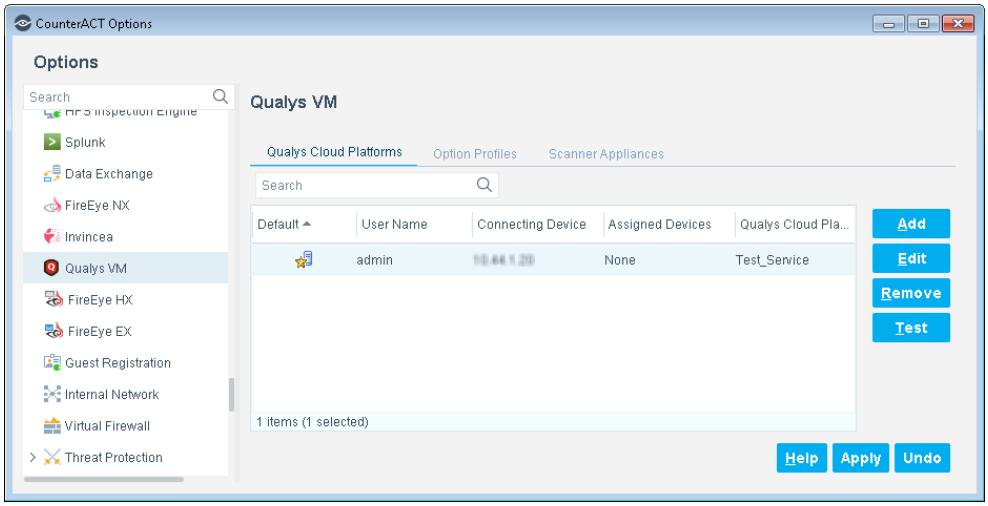
Host IP Address	Define the IP address of the endpoint to be tested. ▪ If **Display report details for last scan** is selected, the scan status and start time of the last scan requested for this endpoint are displayed. ▪ If **Launch new scan** is selected, the selected endpoint is scanned. The endpoint must be connected to the corporate network when the scan is run. If **Launch new scan** and **Display report details for last scan** are not selected, this field can be any valid IP value.

Option Profile	Select a Qualys Option Profile. ▪ If **Display report details for last scan** is selected, details are displayed of the last scan that used the selected Option Profile. ▪ If **Launch new scan** is selected, the selected Option Profile is used in the scan test. If **Launch new scan** and **Display report details for last scan** are not selected, this field is ignored.
Scanner Appliance	Select a Qualys Scanner Appliance. ▪ If **Display report details for last scan** is selected, details are displayed of the last scan that used the selected Scanner Appliance. ▪ If **Launch new scan** is selected, the selected Scanner Appliance is used in the scan test. If **Launch new scan** and **Display report details for last scan** are not selected, this field is ignored.
Display report details for last scan	If the checkbox is selected, the test retrieves the status and the start time of the last CounterACT scan request in which: ▪ the selected endpoint was requested to be scanned ▪ the selected Option Profile was used in the scan request ▪ the selected Scanner Appliance was used in the scan request
Launch new scan	If the checkbox is selected, the test launches a new scan on the test endpoint using the selected Option Profile and Scanner Appliance.

Clear both checkboxes to test only that the Connecting Device can log in to the specified Qualys Cloud Platform.

To run the test, see Test the Module.

2. Select **Finish**. The Qualys Cloud Platform information appears in the Qualys Cloud Platforms pane.



3. Select **Apply** and **Close**. The Qualys VM Module configurations are applied.

Disable Discovery of Qualys Host Properties

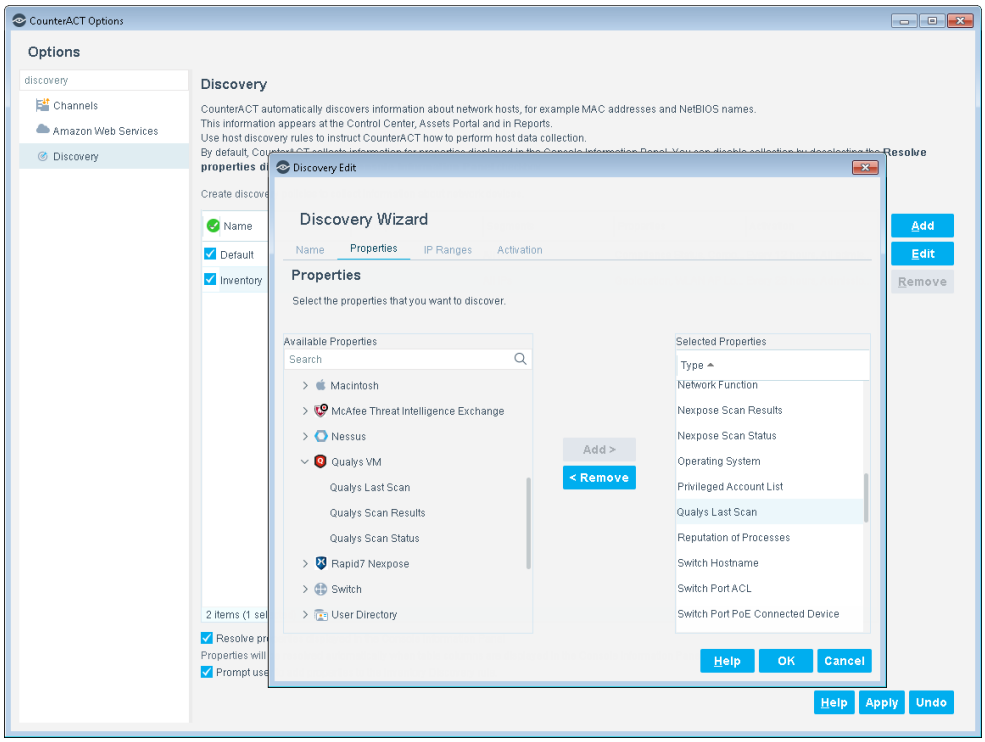
Qualys enforces limits on API calls based on customer subscription settings. The default API limit is 300 calls per hour. Qualys blocks API calls that exceed the API call rate limit.

By default, CounterACT automatically discovers information about endpoints, even if a policy is not applied to the endpoint. This behavior includes regular queries to update host properties. However, this background discovery behavior is not required for properties resolved by querying Qualys, and should be disabled to avoid reaching the API rate limit.

For more information about discovery features, see the CounterACT *Administration Guide*.

To disable background discovery behavior for Qualys host properties:

1. In the CounterACT Console, select **Options** from the **Tools** menu. The Options dialog box opens.
2. Select **Discovery**. The Discovery pane opens.
3. In the Discovery table, select the Inventory record.
4. Select **Edit**. The Discovery Wizard opens.



5. Select the Properties tab of the wizard. This tab lets you select which properties listed in Asset Inventory view are regularly updated in the background.

By default, the **Qualys Last Scan** host property is selected for background discovery. Select this property in the Selected Properties column, and select **Remove**. Verify that no host properties reported by the Qualys module are in the Selected Properties column.

6. Select **OK** to exit the wizard. Select **Apply** in the Discovery pane to save changes.

Test the Module

Run the module test to:

- Verify that the selected endpoint's Connecting Device can log in to the specified Qualys Cloud Platform.
- Launch a scan to verify that a scan can be run. (Optional)

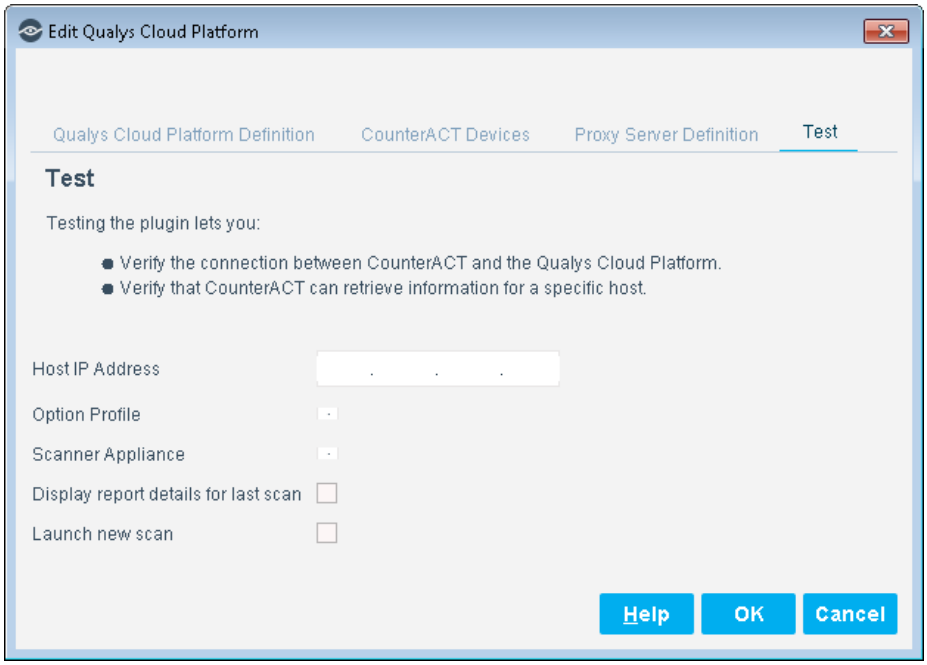
  A successful scan indicates that:

  – The endpoint is connected.
  – The specified Option Profile name exists in the Qualys environment.
  – The specified Scanner Appliance name exists in the Qualys environment.
- Retrieve the status of the selected endpoint's most recent CounterACT scan request that used the specified Option Profile and Scanner Appliance. (Optional)

You can modify the test configuration parameters before running the test. See step 5.

To run the module test:

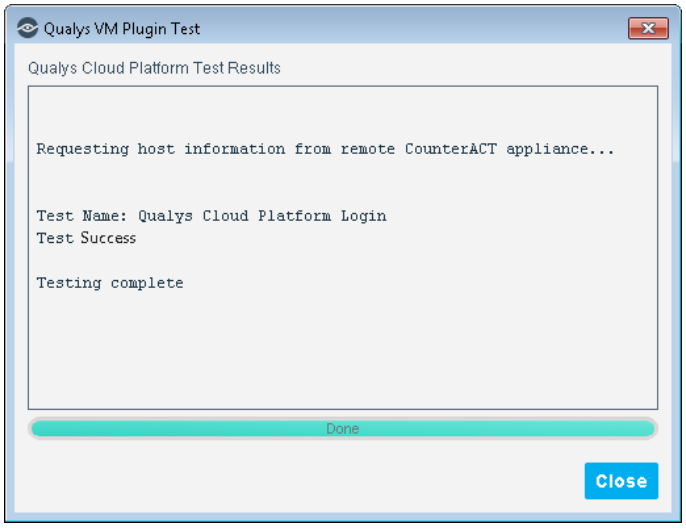
1. In the CounterACT Console, select **Options** from the **Tools** menu. The Options dialog box opens.
2. Navigate to and select **Modules**.
3. In the **Modules** pane, select **Qualys VM**, and select **Configure**. The Qualys VM pane opens.
4. In the Qualys Cloud Platforms tab, select the Connecting Device to be tested.
5. To modify the test parameters:
   a. Select **Edit**. The Edit Qualys Cloud Platform window opens.
   b. Select the Test tab.



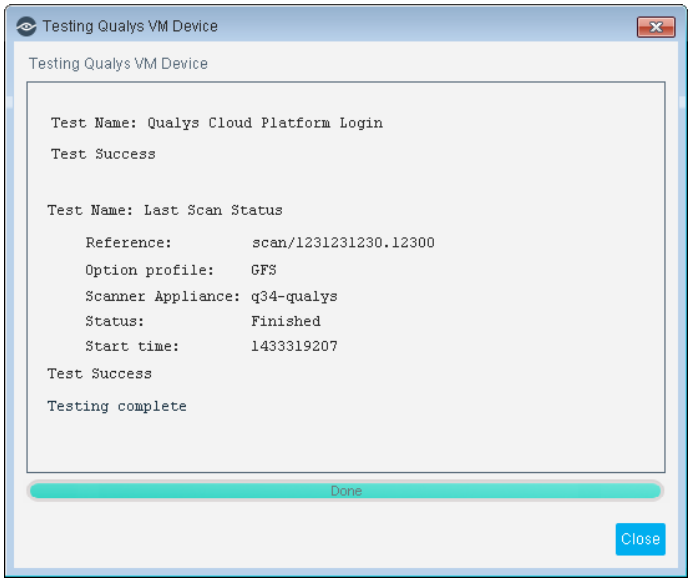
c. Set the values. For details, see Define Test Configuration Parameters.

d. Select **OK** and select **Apply**.

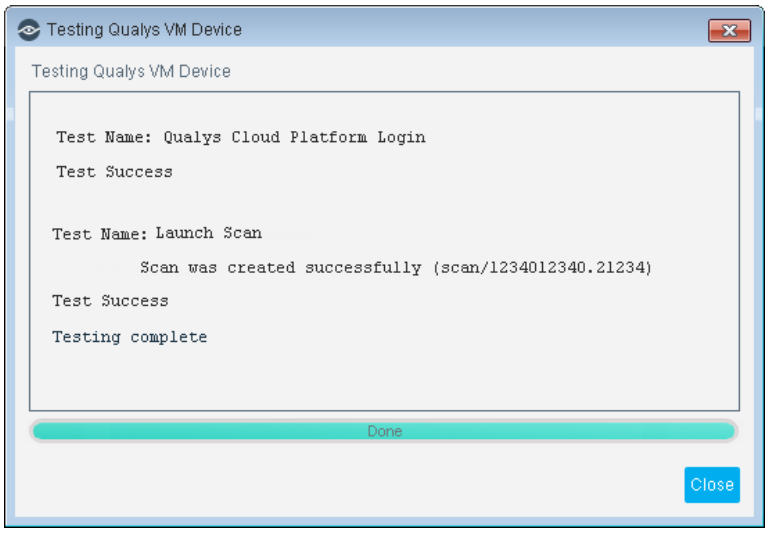
6. Select **Test**. The test runs, and the results are displayed.



Sample test in which no checkboxes were selected



Sample test in which *Display report details for last scan* was selected



Sample test in which *Launch new scan* was selected

7. Select **Close**.

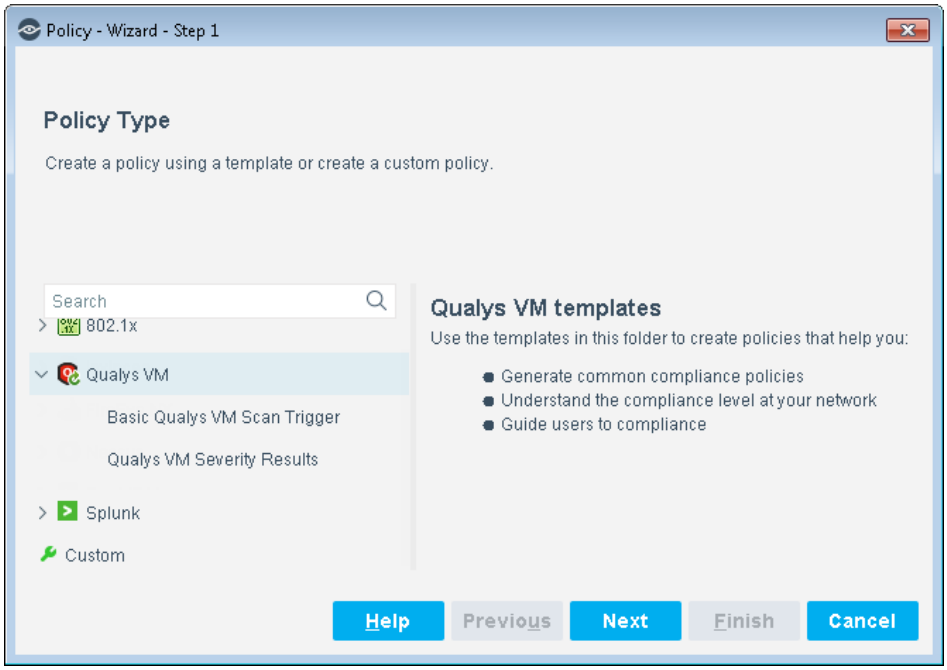
Run Qualys VM Policy Templates

CounterACT templates help you quickly create important, widely used policies, easily control endpoints and guide users to compliance.

Predefined actions – instructions regarding how to handle endpoints that match specified policy rules – are included in the templates.

Two templates are available when working with the Qualys VM Module:

- Basic Qualys VM Scan Trigger Template
- Qualys VM Severity Results Template



Both templates provide baseline capabilities. It is recommended to test the policies on a limited network segment, and then modify and extend them to meet corporate security requirements.

Basic Qualys VM Scan Trigger Template

Before using this template, ensure that the names of the Qualys Option Profiles and Scanner Appliances are defined in the Qualys VM Module configuration. See Configure the Module for details.

Use this template to create a CounterACT policy that launches a Qualys scan request for the selected Qualys Option Profile and Scanner Appliance, based on the following default settings:

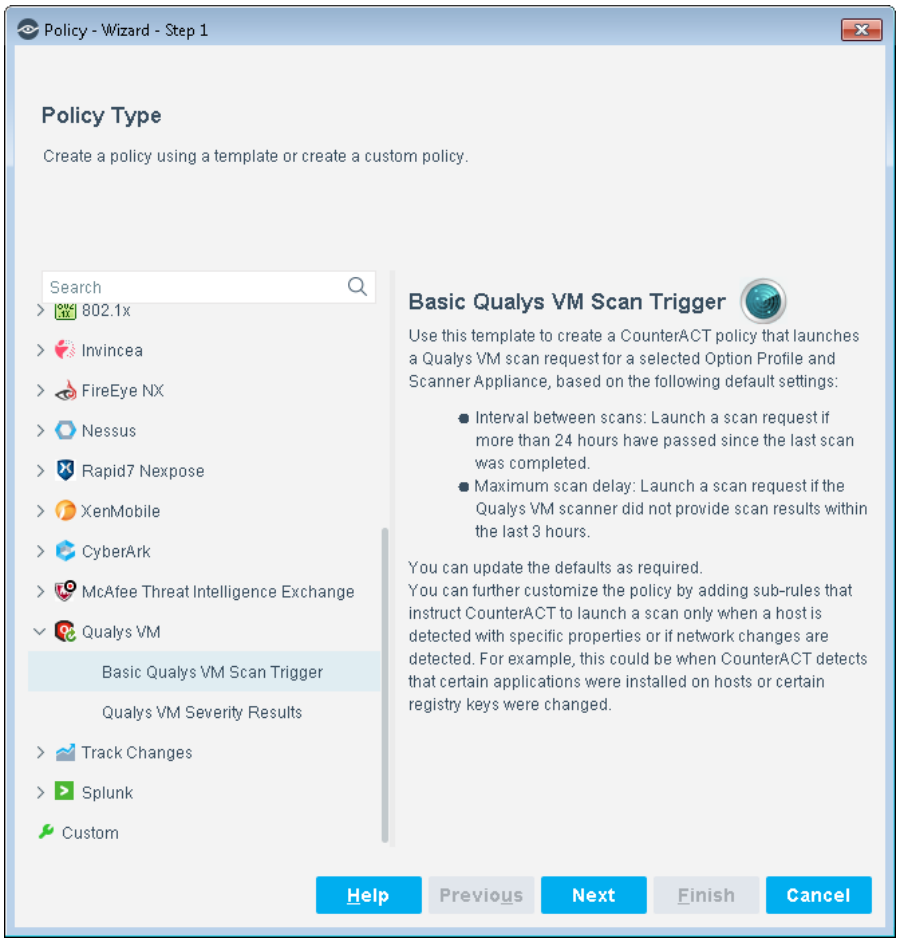
- Interval between scans: Launch a scan request if more than 24 hours have passed since the last CounterACT-initiated scan was completed.
- Maximum scan delay: Launch a scan request if the Qualys Cloud Platform did not provide scan results within the last 3 hours.

This policy template enables CounterACT to launch a basic scan. You can update the defaults as required and can further customize the policy by adding sub-rules that instruct CounterACT to launch a scan only when an endpoint is detected with specific properties. For example, instruct CounterACT to launch a scan request when it detects that certain applications were installed on an endpoint or if certain registry keys were changed on the endpoint. You should have a basic understanding of CounterACT polices to carry out these changes.

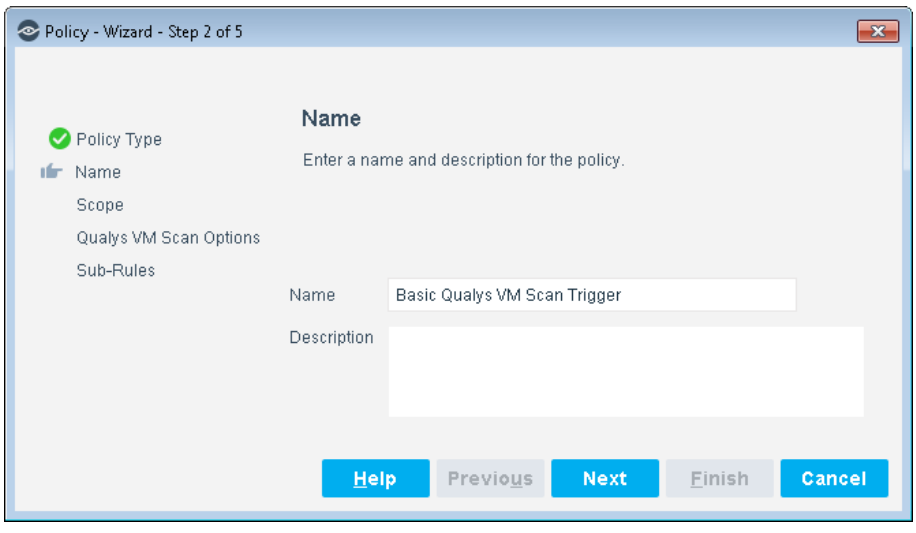
To use the Basic Qualys VM Scan Launch template:

1. Log in to the CounterACT Console and select the **Policy** tab.
2. Select **Add** from the Policy Manager. The Policy Wizard opens.

3. Expand the **Qualys VM** folder and select **Basic Qualys VM Scan Launch**.

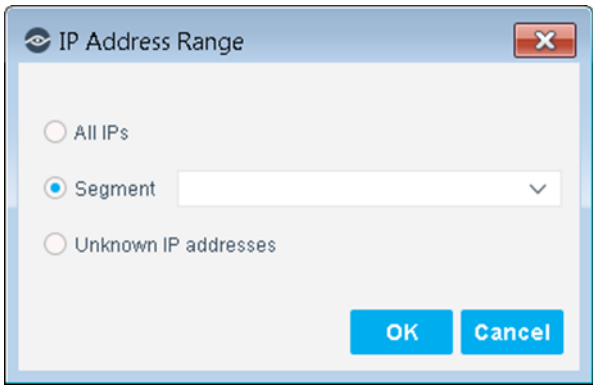


4. Select **Next**. The Name pane opens.



5. Accept the default name or create a new name, and add a description.

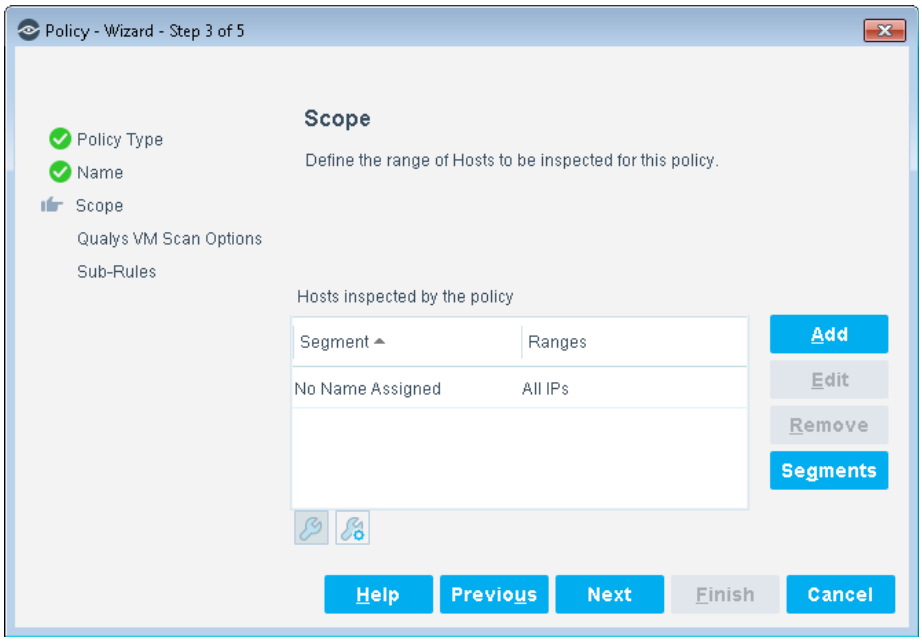
6. Select **Next**. The Scope pane and the IP Address Range dialog box open.
7. Use The IP Address Range dialog box to define which endpoints are inspected.



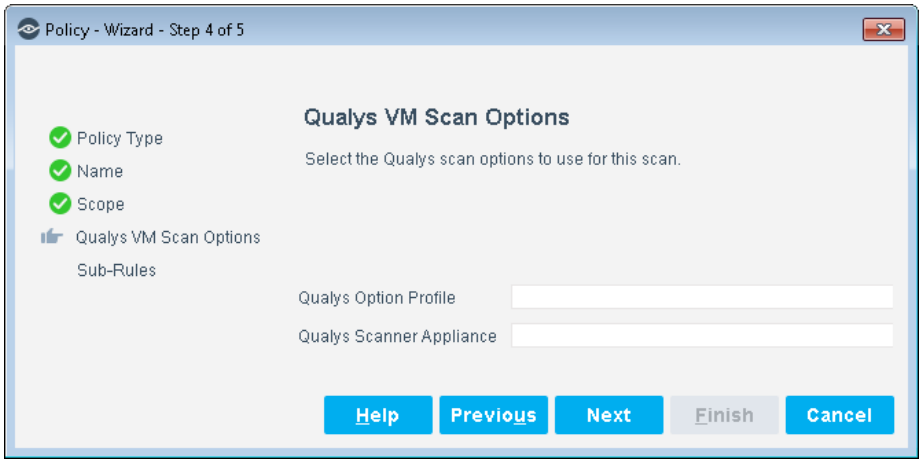
The following options are available:

- **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 page.
- **Unknown IP addresses**: Apply the policy to endpoints whose IP addresses are not known. Endpoint detection is based on the endpoint MAC address.

8. Select **OK**. The added range appears in the Scope pane.



9. Select **Next**. The Qualys VM Scan Options pane opens.



10. Select the Qualys Option Profile and Scanner Appliance to be used when a scan is launched by this CounterACT policy.

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

For all endpoints within the defined scope that match the main rule, these sub-rules instruct CounterACT to launch a Qualys scan on each connected endpoint that:

- has not been scanned within the last 24 hours
- is not currently being scanned

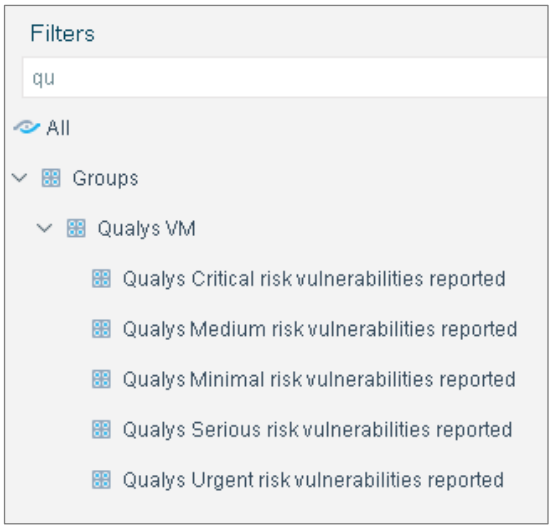
12. Select **Finish** to create the Qualys VM policy.

Qualys VM Severity Results Template

Use this template to create a CounterACT policy that detects Qualys vulnerability severity results assigned to network endpoints. The severity results are based on the most recent Qualys host-based **ForeScout Vulnerability Report** data. To configure the report, see Configure the Qualys Environment.

The default policy created by this template classifies scanned endpoints based on detected vulnerabilities; reported potential vulnerabilities are not considered by the policy. The policy classifies endpoints into the following CounterACT groups:

- Qualys Urgent risk vulnerabilities reported
- Qualys Critical risk vulnerabilities reported
- Qualys Serious risk vulnerabilities reported
- Qualys Medium risk vulnerabilities reported
- Qualys Minimal risk vulnerabilities reported



You can later use these groups in CounterACT policies to control endpoints. For example, assign endpoints detected as having Urgent risk vulnerabilities to an isolated VLAN.

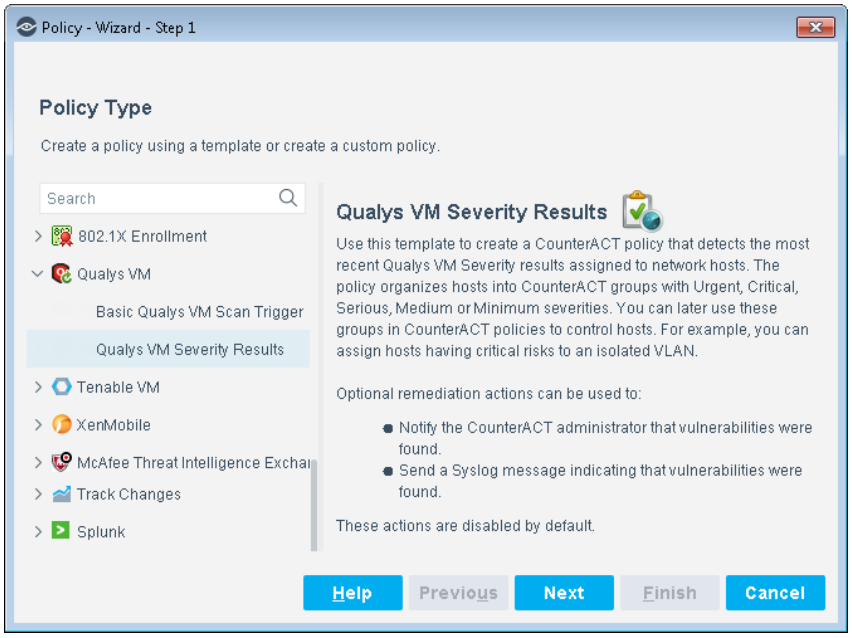
Optional actions are predefined in the template and can be used to:

- Notify the CounterACT administrator that vulnerabilities were found.
- Send a Syslog message indicating that vulnerabilities were found.

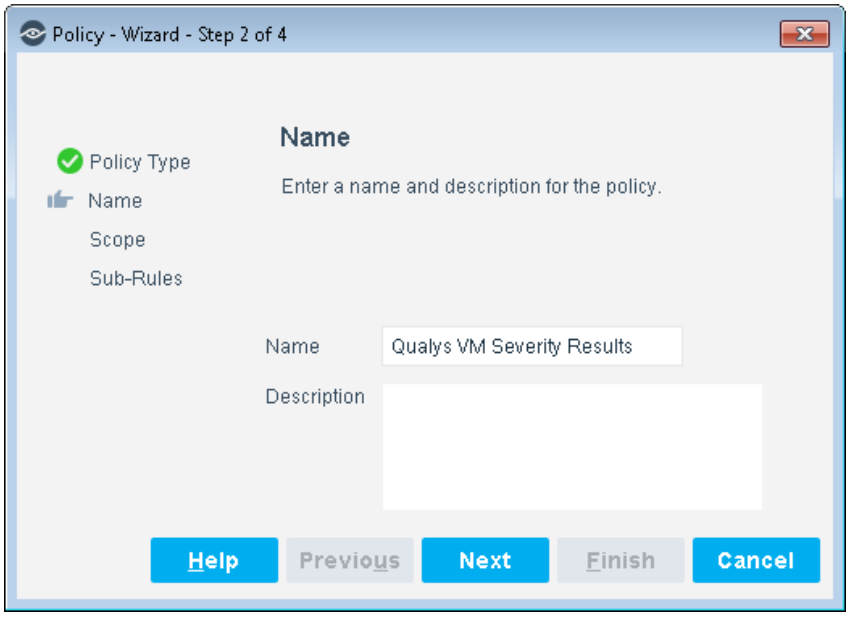
These actions are disabled by default.

To use the Qualys VM Severity Results template:

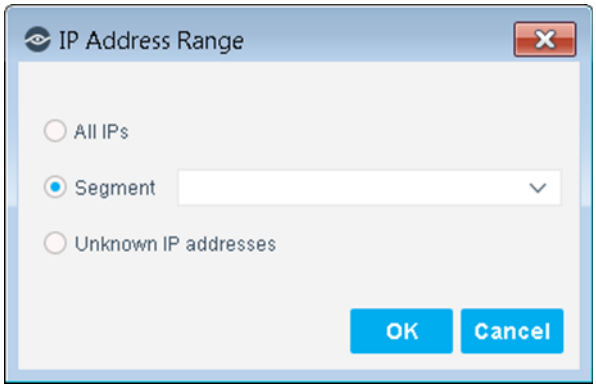
1. Log in to the CounterACT Console and select the **Policy** tab.
2. Select **Add** from the Policy Manager. The Policy Wizard opens.
3. Expand the **Qualys VM** folder and select **Qualys VM Severity Results**.



4. Select **Next**. The Name pane opens.



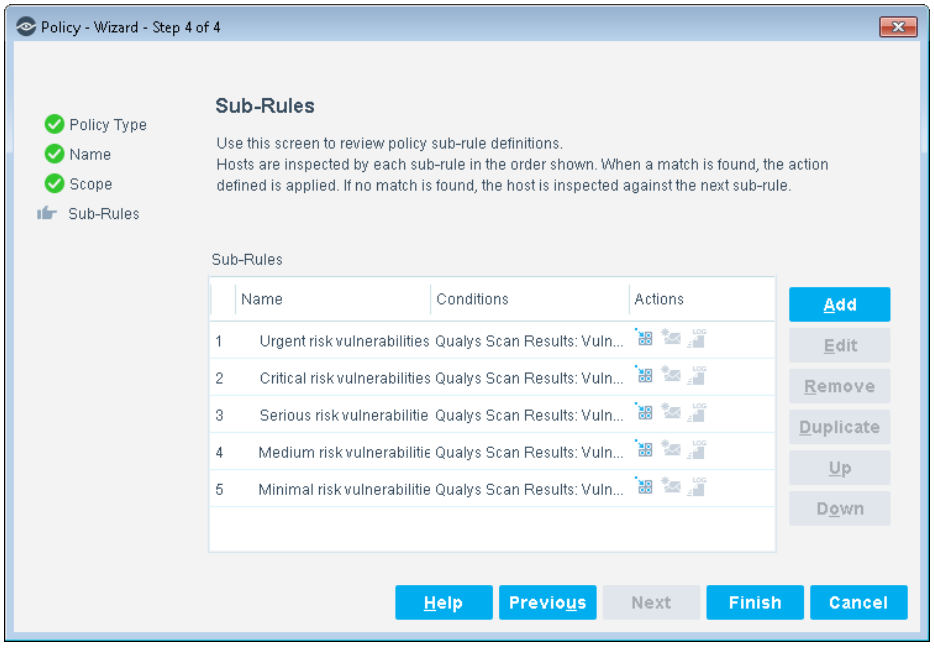
5. Accept the default name or create a new name, and add a description.
6. Select **Next**. The Scope pane and the IP Address Range dialog box open.
7. Use The IP Address Range dialog box to define which endpoints are inspected.



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 page.
- **Unknown IP addresses**: Apply the policy to endpoints whose IP addresses are not known. Endpoint detection is based on the endpoint MAC address.

8. Select **OK**. The added range appears in the Scope pane.
9. Select **Next**. The Sub-Rules pane opens.



For all endpoints within the defined scope, these predefined sub-rules detect endpoints based on the severity of their reported vulnerabilities.

Rules are ordered by decreasing severity: the rule that matches Urgent vulnerabilities is evaluated first, and the rule that matches Minimal vulnerabilities is last. This means that endpoints are sorted into groups based on the *most severe* vulnerability on each endpoint.

Each rule applies the following actions:

- An **Add to Group** action assigns matching endpoints to the appropriate group. This action is enabled by default.
- An optional **Send Email** action notifies the CounterACT administrator that vulnerabilities were found. This action is disabled by default.
- An optional **Send Message to Syslog** action sends a Syslog message indicating that vulnerabilities were found. This action is disabled by default.

10. Select **Finish** to create the Qualys VM policy.

Create Custom CounterACT Policies

In addition to the bundled CounterACT properties and actions available for detecting and handling endpoints, you can work with Qualys VM related properties to create custom policies. These items are available when you install the module.

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

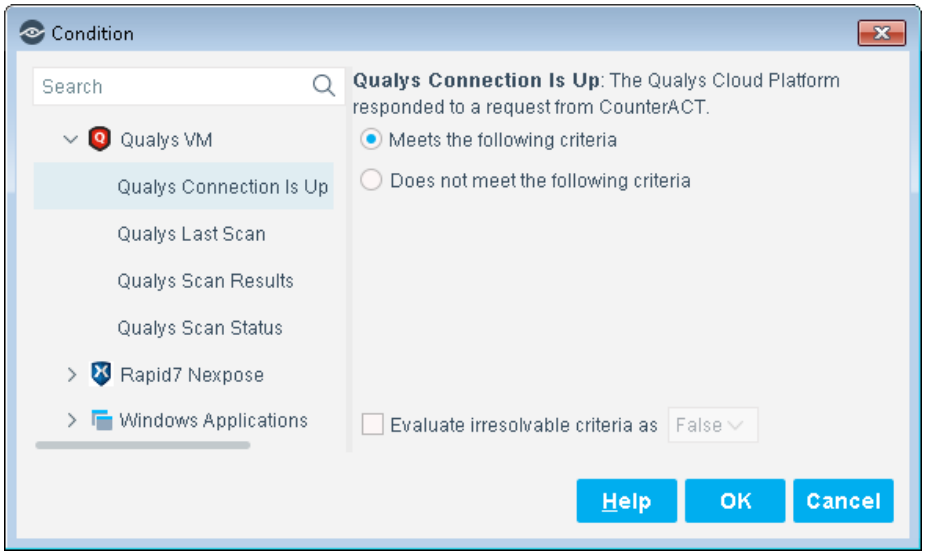
For more information about working with policies, select **Help** from the policy wizard.

To create a custom policy:

1. Log in to the CounterACT Console.
2. On the Console toolbar, select the **Policy** tab. The Policy Manager opens.
3. Select **Add** to create a policy.

Detecting Vulnerabilities – Policy Properties

CounterACT policy properties let you instruct CounterACT to detect endpoints with specific attributes. For example, create a policy that instructs CounterACT to detect endpoints running a certain operating system or having a certain application installed.



To access Qualys VM properties:

1. Open the policy Conditions dialog box.
2. Expand the Qualys VM folder in the Properties tree.

The following properties are available:

Qualys Connection Is Up	Indicates that the Qualys Cloud Platform connected to the module and responded to CounterACT requests.	
Qualys Last Scan	Indicates the time and date of the last scan initiated by CounterACT on an endpoint.	
Qualys Scan Results	Detects the following vulnerability specific information using the most recent Qualys host-based **ForeScout Vulnerability Report** for the endpoint.	
	Vulnerability Title	The descriptive name assigned by Qualys to the specific vulnerability. If you do not specify a value, the property is resolved for all vulnerabilities.
	Vulnerability Type	Indicates if the vulnerability is a confirmed vulnerability or a potential vulnerability.
	Severity	The severity of the vulnerability. Values include: Minimal, Medium, Serious, Critical, and Urgent.
	Category	Qualys vulnerability category of the vulnerability
	CVSSv2 Base Score	Qualys CVSSv2 Base score for the vulnerability
	CVE	CVE associated with the detected vulnerability
Qualys Scan Status	Detects the following status information for scans initiated by CounterACT on an endpoint.	
	Reference	The Qualys Reference of the desired scan. If you do not specify a reference, the values are resolved for all recent scans.

	Option Profile	The Qualys Option Profile name. If you do not select a value, the property is resolved for all Option Profiles.
	Scanner Appliance	The Qualys Scanner Appliance name. If you do not select a Scanner Appliance, the property is resolved for all Scanner Appliances.
	Scan Status	The status of the Qualys scan requested by CounterACT.
	Last Start Scan Time	The most recent time that a scan was successfully launched, regardless of its current status.

Scanning Endpoints - Policy Actions

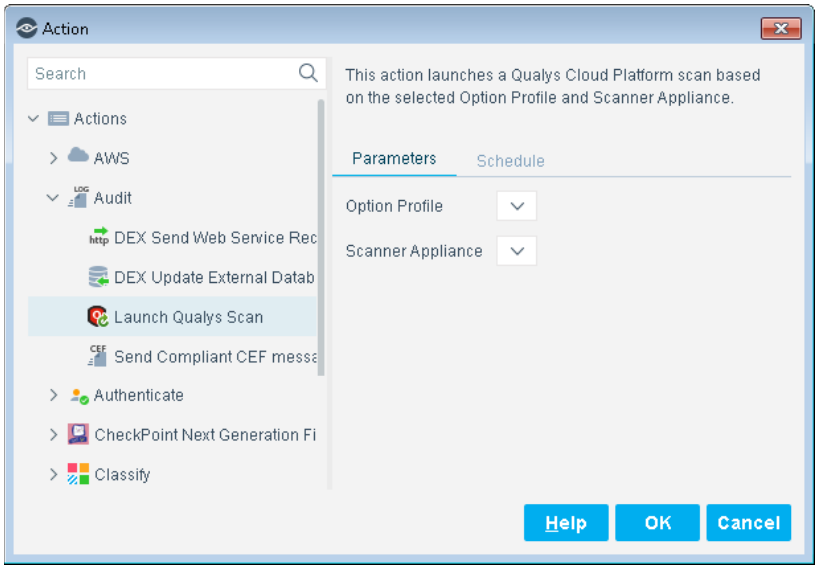
CounterACT policy actions let you instruct CounterACT how to control detected endpoints. For example, assign potentially compromised endpoints to an isolated VLAN, or send the endpoint user or IT team an email.

In addition to the bundled CounterACT actions available for handling endpoints, you can work with the Qualys related action to create custom policies. This action is available when you install the module.

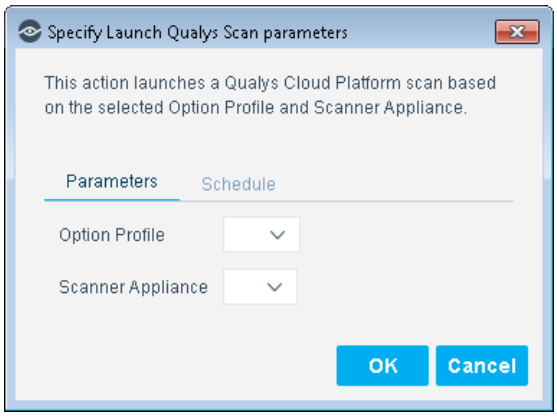
Launch Qualys Scan

Use the *Audit* > *Launch Qualys Scan* action in CounterACT policies to launch a Qualys scan when specified policy conditions are met. For example, create a policy that detects if certain applications were installed on an endpoint or if certain registry keys were changed, and launch a scan when an endpoint meets the condition.

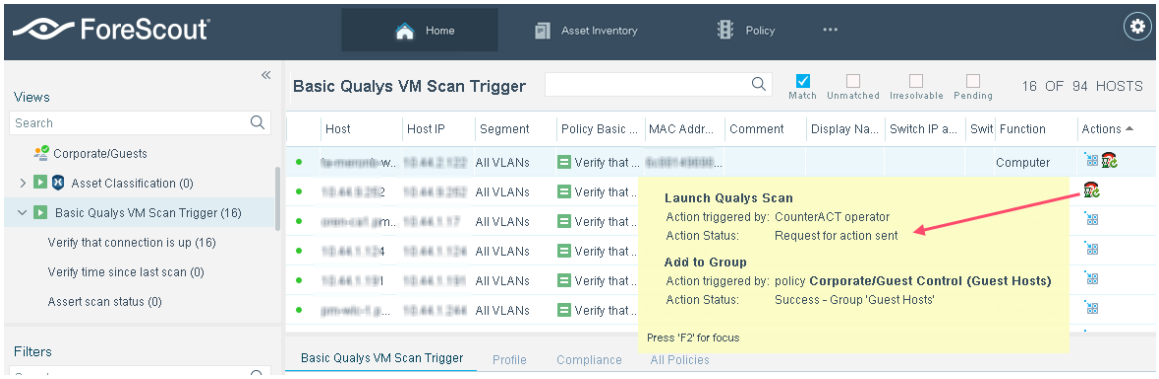
Scans launched automatically by a policy use the Option Profile and the Scanner Appliance set during policy creation.



Manual scans are launched using the *Launch Qualys Scan* action on one or more endpoints. The action prompts the operator to select an Option Profile and a Scanner Appliance.



As with other actions in CounterACT, you can identify successful or failed actions using the CounterACT console.



Display Qualys VM Asset Inventory Information

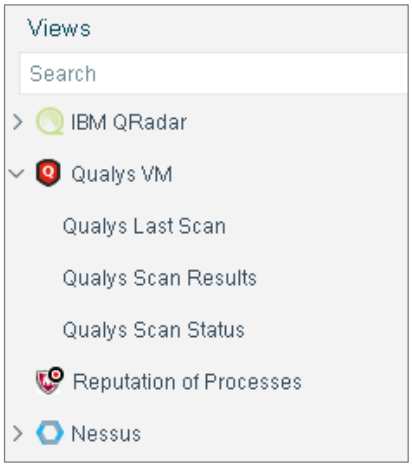
Use the CounterACT Asset Inventory to view aggregate information for each of the Qualys VM properties, such as vulnerability severity, vulnerability category and CVE information. You can browse the inventory to learn which Qualys vulnerability categories were detected on each endpoint, and on how many endpoints a specific category was detected.

The Asset Inventory lets you:

- Broaden your view of the organizational network from endpoint-specific to activity-specific.
- View endpoints that have been detected with specific attributes.
- Incorporate inventory detections into policies.

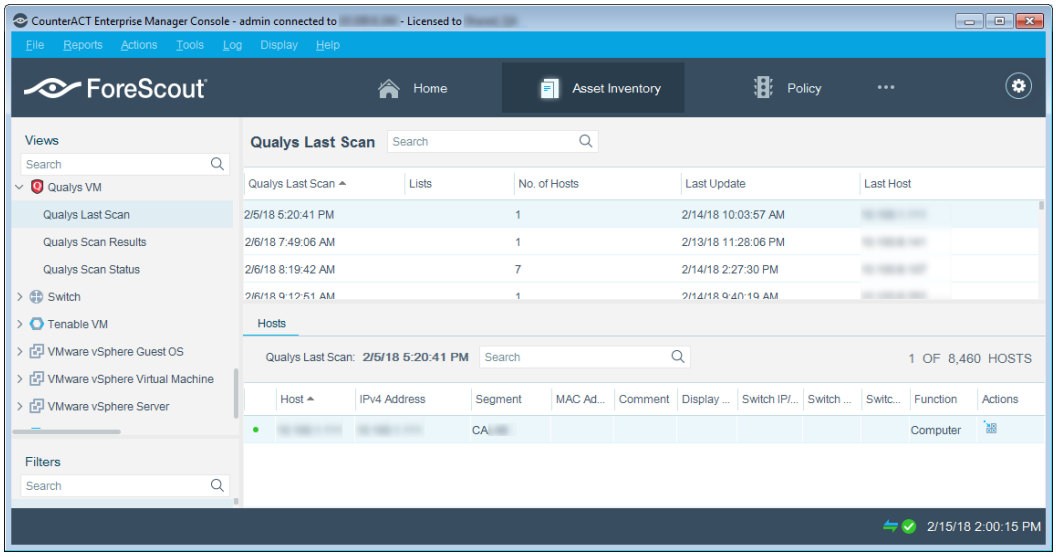
To access the Asset Inventory:

1. Log in to the CounterACT Console and select the Asset Inventory tab.
2. Navigate to **Qualys VM**.

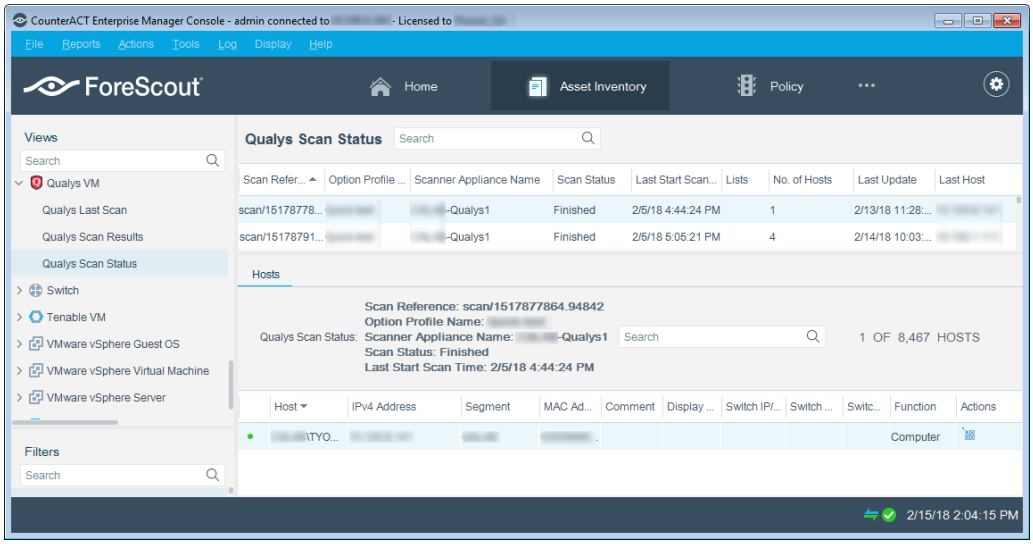


The following information is available:

- ***Qualys Last Scan***: Displays the time the status was set to *Finished*, the last time the status was reported to CounterACT, and the scanned host information from the most recent Qualys scan initiated by CounterACT on an endpoint.



- ***Qualys Scan Results***: Displays the vulnerability results from the most recent Qualys host-based **ForeScout Vulnerability Report** for each endpoint.
- ***Qualys Scan Status***: Displays the Qualys scan parameters, the status, the start time, the last time the status was reported to CounterACT, and the scanned host information of the most recent Qualys scans initiated by CounterACT.



For information about how to work with the CounterACT Asset Inventory, refer to *Working in the Console>Working with Inventory Detections* in the *CounterACT Administration Guide* or the Console Online Help.

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**.

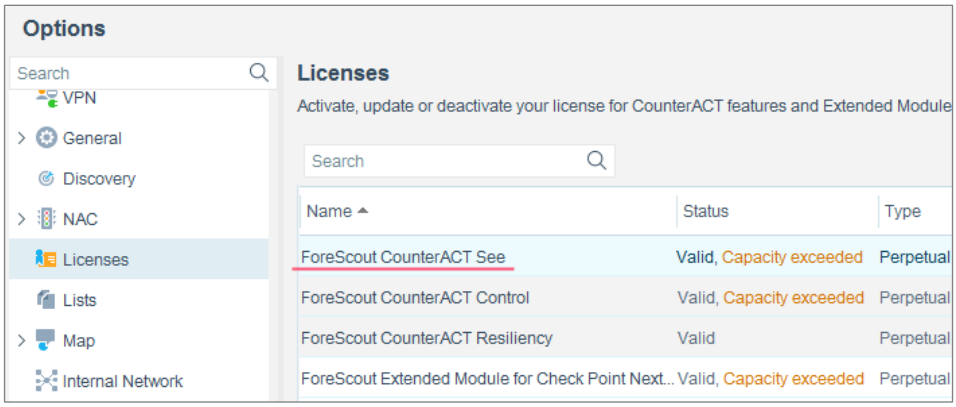
Documentation Portal

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