ForeScout® Extended Module for Tenable™ Vulnerability Management

Configuration Guide

Version 2.7.1

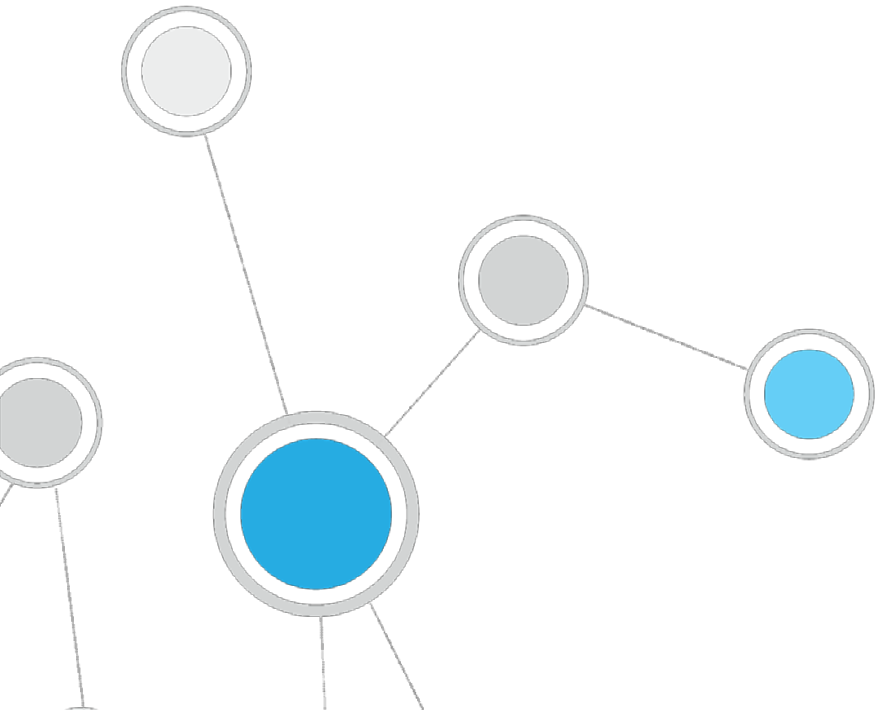
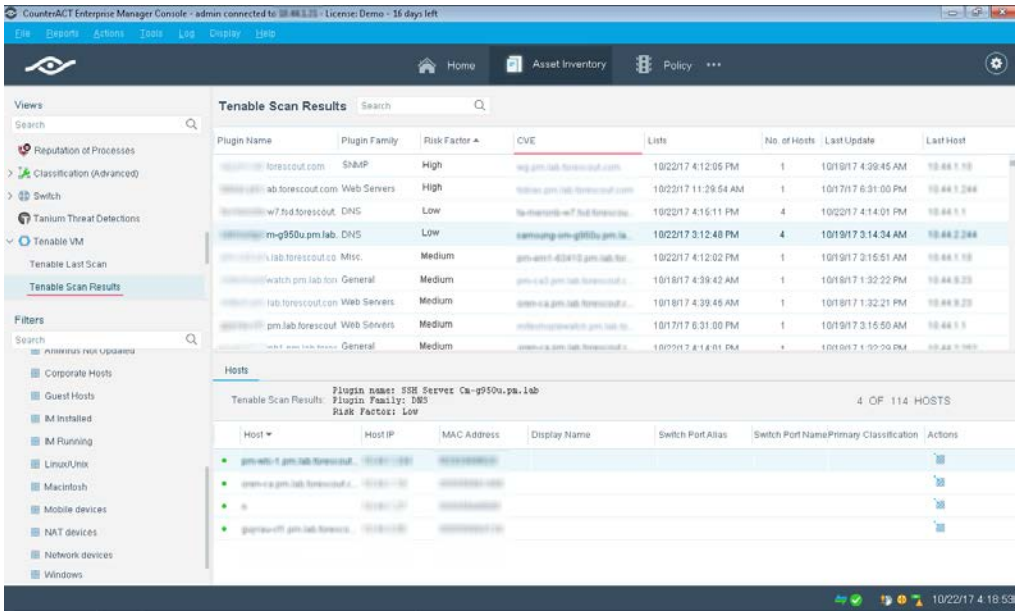


Table of Contents

About Tenable Vulnerability Management Module

The ForeScout CounterACT® Tenable Vulnerability Management (VM) Module lets you integrate CounterACT with Tenable SecurityCenter®, Tenable.io™ and Nessus® scanners so that you can:

- Trigger Nessus scanner, SecurityCenter, or Tenable.io (cloud-based vulnerability management platform) scan requests based on network activity detected by CounterACT. For example, delay a scan if the endpoint is offline, or trigger a scan if a specific application is installed or if the previous scan was not within a certain time frame. See Basic Tenable Scan Trigger Template.
- Monitor, manage, restrict and remediate endpoints based on scan results. See Risk Factor Results Template.
- Use the CounterACT Asset Inventory to see which endpoints have been identified as vulnerable by the module. See Display Tenable VM Asset Inventory Events.



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

Compatible Tenable Vulnerability Products

The module lets you integrate CounterACT with either of the following Tenable Network Security vulnerability products:

- ***Nessus versions 6.0.x through 6.10.x***. Vulnerability and configuration assessment product that features configuration auditing, asset profiling, sensitive data discovery, patch management integration, and vulnerability analysis of your security posture.

- ***SecurityCenter versions 4.8.2, 5.4.2, 5.4.5 and 5.6.x***. Centralized management system to control and view scan data from multiple Nessus scanners deployed throughout your organization.
- ***Tenable.io*** - The Tenable cloud-based vulnerability management platform.

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.

Additional Tenable Documentation

Refer to Tenable online documentation for more information about the Tenable and SecurityCenter solutions:

https://www.tenable.com/products

Concepts, Components, Considerations

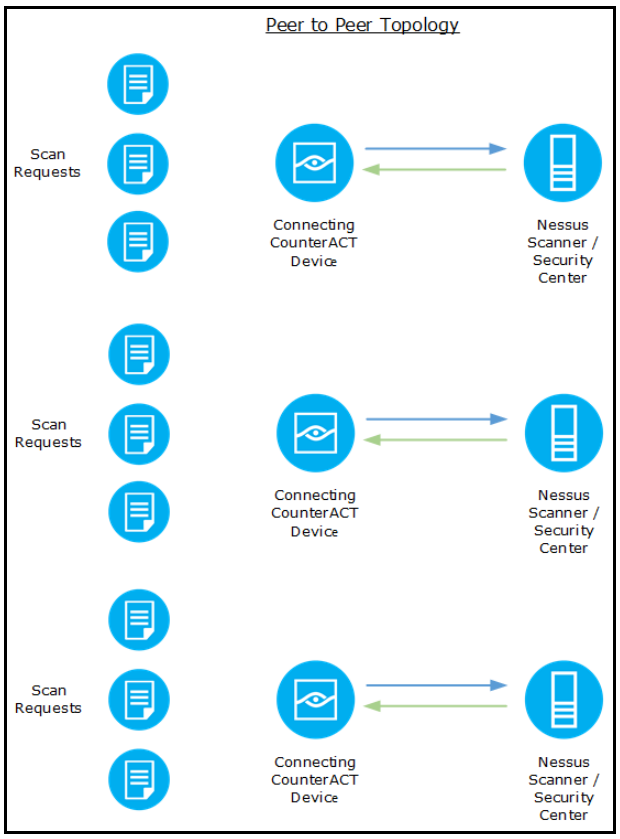
This section provides a basic overview of Tenable VM / CounterACT architecture:

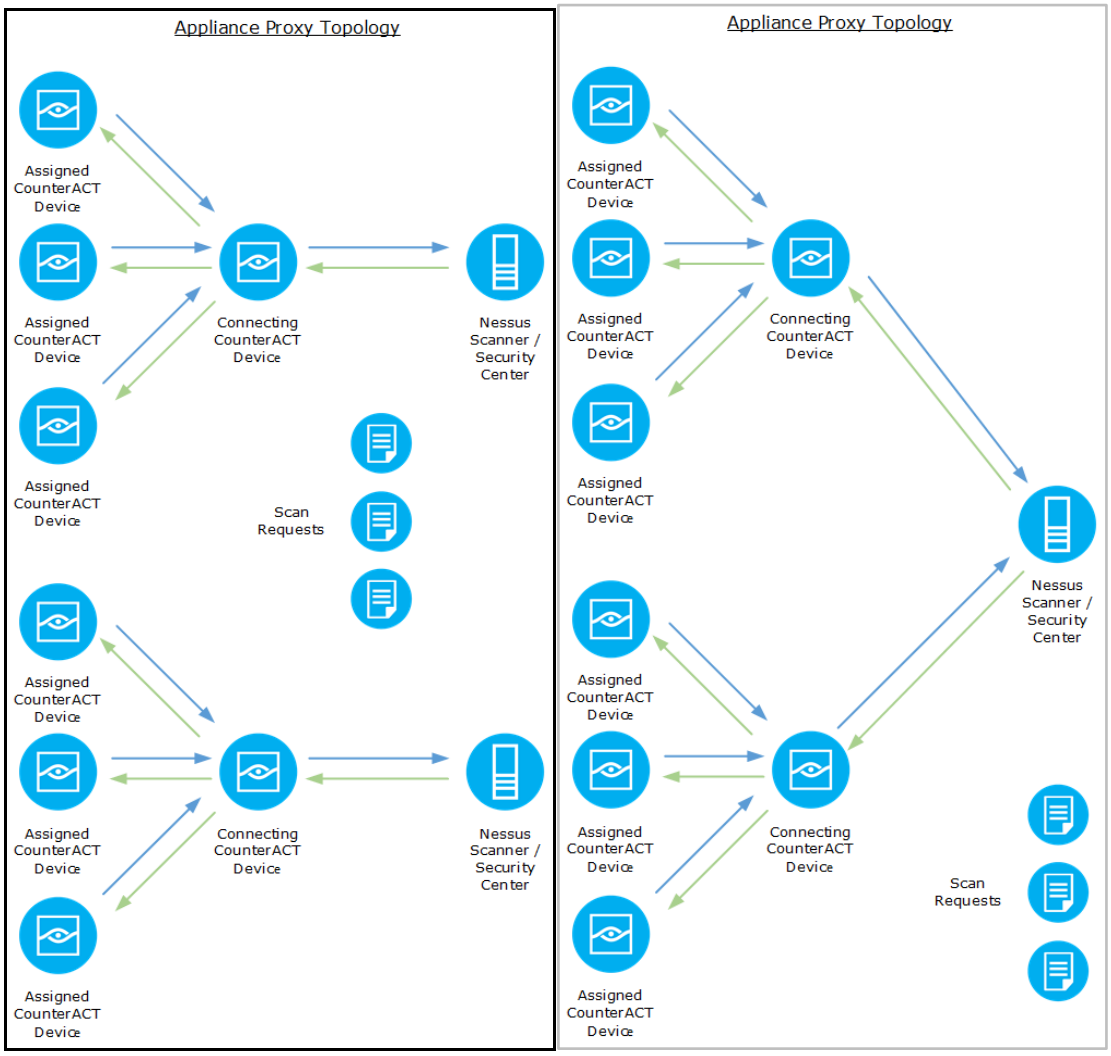
- Concepts – basic integration concepts.
- Components – devices in your network that participate in the integration.
- Considerations – setup details and common network structure issues to keep in mind when you implement this module.

Concepts

A typical deployment requires multiple CounterACT Appliances and Tenable Network Security vulnerability products to provide regular, frequent compliance auditing. The network design of Appliances and vulnerability products should ensure that scanners are not overloaded, and that scan results are available in a timely fashion.

In this integration, each Nessus, Tenable.io or SecurityCenter is connected to one or more CounterACT devices. When configuring the Tenable VM module, ensure that each one can scan the entire range of IP addresses associated with its assigned CounterACT Appliances or Enterprise Manager.


Peer to Peer Topology
Scan Requests
Connecting CounterACT Device
Nessus Scanner / Security Center
Scan Requests
Connecting CounterACT Device
Nessus Scanner / Security Center
Scan Requests
Connecting CounterACT Device
Nessus Scanner / Security Center



Deployment Options

There are two topologies for setting up multiple CounterACT devices and multiple Nessus scanners, Tenable.io or SecurityCenter servers.

- *The actual deployment can combine both topologies to meet particular network requirements.*
- *When the SecurityCenter is configured to allow Session Management (under Security Configuration > Authentication Settings in the Tenable dashboard), you can set the maximum number of registered users that can connect to the SecurityCenter.*

Peer-to-Peer: One or more CounterACT devices communicate directly with one SecurityCenter or Nessus scanner. This is a one-to-one relationship, where each CounterACT Appliance prompts the connected SecurityCenter or Nessus scanner to initiate scans whenever required. This is the typical topology for remote sites in which a remote Tenable vulnerability product and a remote CounterACT device are deployed.

Appliance Proxy: A connecting CounterACT device serves as a channel (proxy) to the SecurityCenter, Tenable.io, or Nessus scanner for other devices. The connecting device queues scan requests from all the assigned CounterACT Appliances, including itself. The connecting device controls the number of scan requests as well as the number of endpoints per any one scan request. This ensures more efficient traffic control and avoids overloading scanners.

Components

Connecting CounterACT Device: This CounterACT device communicates directly with the Nessus scanner, Tenable.io, or SecurityCenter server and handles queries and requests submitted by all the devices assigned to the Tenable vulnerability product. In an environment where more than one CounterACT device is assigned to a Tenable vulnerability product, the connecting device functions as a proxy between the Tenable vulnerability product and all the CounterACT devices assigned to it. The proxy forwards all requests by other CounterACT devices assigned to the Tenable vulnerability product. The connecting CounterACT device functions as a CounterACT device assigned to itself.

Assigned CounterACT Device: This CounterACT device is assigned to a Tenable vulnerability product, but it does not communicate with the Tenable product directly. All communication between the Tenable vulnerability product and its assigned CounterACT devices is handled by the connecting CounterACT device defined for the Tenable product. All the IP addresses handled by an assigned device must also be handled by the Tenable vulnerability product to which the devices are assigned.

Default Nessus Scanner/SecurityCenter: All unassigned CounterACT devices are assigned to this Tenable vulnerability product through its connecting CounterACT device.

Considerations

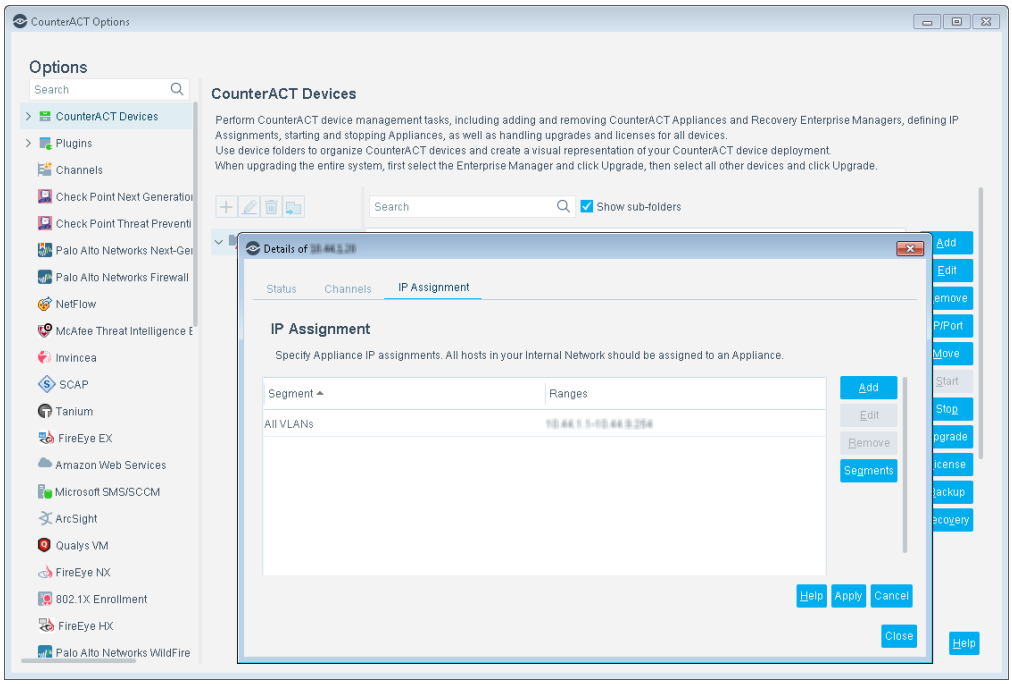
Consider the following when mapping CounterACT devices to Nessus scanners, SecurityCenter or Tenable.io:

Multiple Time Zones: Clock synchronization is required when resolving scanner attributes. If multiple CounterACT devices and scanners are deployed across multiple time zones, all CounterACT devices and scanners must use the same NTP server and regularly synchronize their clocks.

Timing: The module and its policy templates are configured to handle network traffic and to carry out other tasks using default thresholds. Based on network activity or other requirements, you may need to update these defaults.

- By default, a CounterACT policy created using the Basic Tenable Scan Trigger Template checks the Tenable server responsiveness once an hour. This value can be updated by editing the *Recheck* value in the *Scanner is reachable* sub-rule condition.
- By default, the minimum delay between consecutive scan requests is 10 seconds. The maximum number of endpoints per single scan request is 20. It is advised to review the scanner performance over an extended period. Optimize these settings to reduce scanner load and yet minimize scan latency.

Match IP Address Ranges: Verify that Nessus, SecurityCenter or Tenable.io handles the same IP address range as the CounterACT devices assigned to it. To see CounterACT device IP address assignments, on the CounterACT Console select **Tools > Options > CounterACT Devices, double-click the device, and select the IP Assignments** tab.



Synchronization with Scan Policies, Repositories, Zones, and Credentials: When CounterACT triggers a Tenable product scan, it passes certain information to Tenable. For each scan, it passes the specific endpoint IP to be scanned, and a Nessus scan policy name. In addition, when triggering a SecurityCenter scan, CounterACT passes a repository name, an optional zone, and one or more optional credentials for in-depth scanning. These values must be appropriate for the endpoint's group or segment.

Lists of the available scan policies, repositories, scanners, zones and credentials are shown in the Tenable VM module configuration tabs. The SecurityCenter operator can update the Tenable server and their scan policies, repositories, zones, and credentials at any time. However, when a scan is requested, the information passed must match the information stored on the Tenable server. If a scan policy name, repository name, zone, or credential is modified or if additional items are added, be sure to synchronize the Tenable VM module configuration before triggering a scan using that information. To synchronize the configuration, on the CounterACT Console select **Tools > Options > Tenable VM**, and in the Tenable Servers tab, select **Sync**.

Additional Considerations: CounterACT recognizes only those scan reports that it triggered. There is an option to recognize scans that are initiated directly by SecurityCenter, Tenable.io, and Nessus. By default, CounterACT uses the machine generated name for each scan, and deletes each scan 30 days after creation.

> *For complex deployments with multiple CounterACT devices, multiple SecurityCenter servers, Tenable.io or Nessus scanners, and diverse scan compliance policies, see Policy Properties - Detecting Vulnerabilities.*

Tenable Server Authentication

The Tenable VM Module supports two types of credentials for authentication to Tenable servers:

- ***Standard Login:*** When configuring the module to communicate with a Nessus or SecurityCenter using *Standard Login* authentication, enter the Tenable server username and password.
- ***SSL certificate authentication:*** When configuring the module to communicate with SecurityCenter using *SSL* authentication, upload the client certificate and key file to the CounterACT Console. This option is not available for Nessus.

What to Do

1. Verify that you have met system requirements. See Requirements.
2. Download and install the module. See Install the Module.
3. Map CounterACT devices to Nessus, Tenable.io, or SecurityCenter. See Configure the Module.
4. Test the Module Configuration.
5. Run CounterACT policies that detect and manage endpoints tracked by a Nessus scanner, Tenable.io, or SecurityCenter. See Run CounterACT Policy Templates.
6. Create Custom CounterACT Policies.

Requirements

This section describes system requirements, including:

- CounterACT Software Requirements
- ForeScout Extended Module License Requirements
- Supported Tenable Versions

CounterACT Software Requirements

The module requires the following CounterACT releases:

- CounterACT version 8.0.
- A module license for the Tenable VM Module
- An active Maintenance Contract for the licensed module is required

ForeScout Extended Module License Requirements

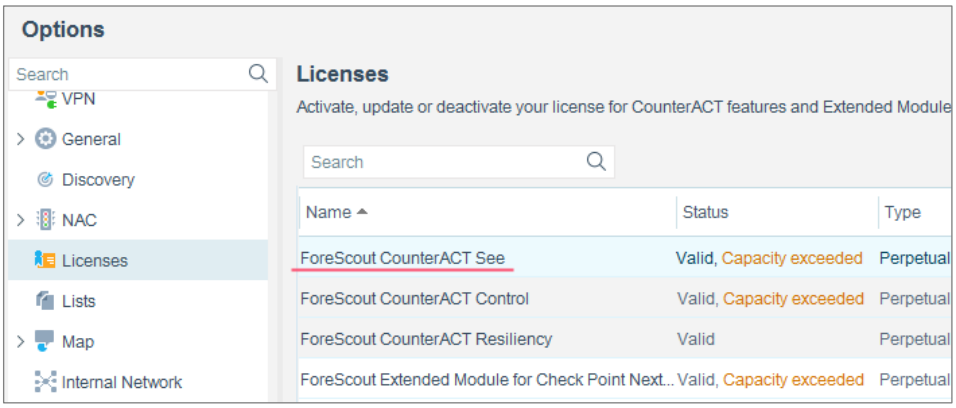
This ForeScout Extended Module requires a valid license. Licensing requirements differ based on which licensing mode your deployment is operating in:

- 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. T*he 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.

Supported Tenable Versions

> *Refer to the Release Notes for the latest supported versions.*

The Tenable VM Module supports the following Tenable Network Security products:

- For communication with Nessus scanners: Nessus scanner versions 6.0.x through 6.10.x
- For communication with SecurityCenter: SecurityCenter versions 4.8.2, and 5.4.2, 5.4.5, and 5.6.x

Verify that your Tenable servers and their connected CounterACT devices regularly synchronize their clocks with the same NTP server.

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.

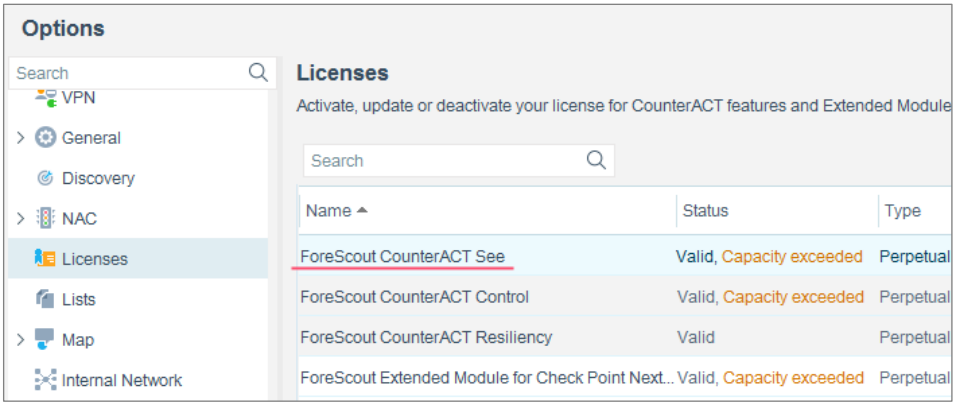
10. When the installation completes, select **Close** to close the window. The installed module is displayed in the Modules pane.

    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

Before configuring the module, review the Concepts, Components, Considerations section.

Perform this procedure after the ForeScout Extended Module for Tenable VM is installed on your targeted CounterACT Appliance.

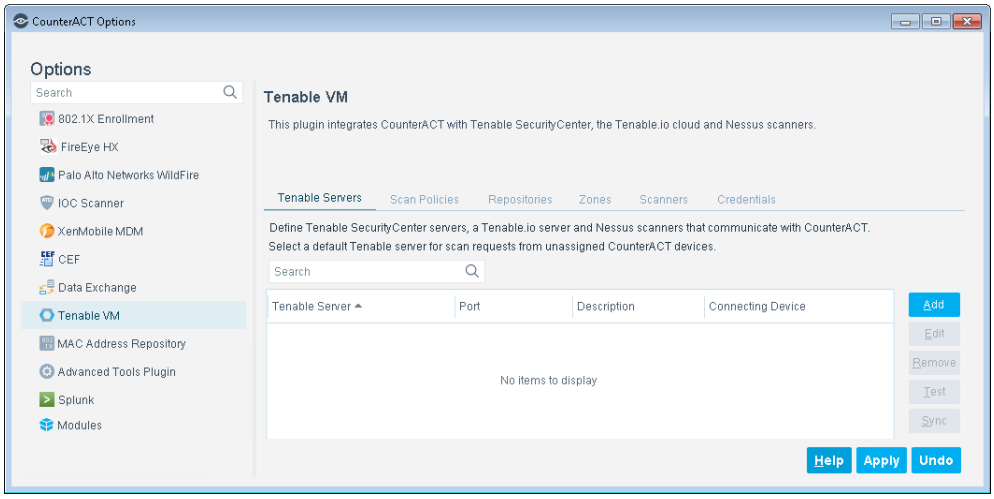
You can configure the module for multiple Nessus, Tenable.io and SecurityCenter. To complete configuration of some of these connections, you must perform the following configuration steps on the Tenable.io instance:

- Synchronize Scan Parameters and Select Defaults
- Set Auto-Deletion of Scan Results
- Test the Module Configuration

- Run Tenable Vulnerability Management Policy Templates

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 the **Modules** folder.
3. In the **Modules** pane, select **Tenable VM**, and select **Configure**. The Tenable VM pane opens.

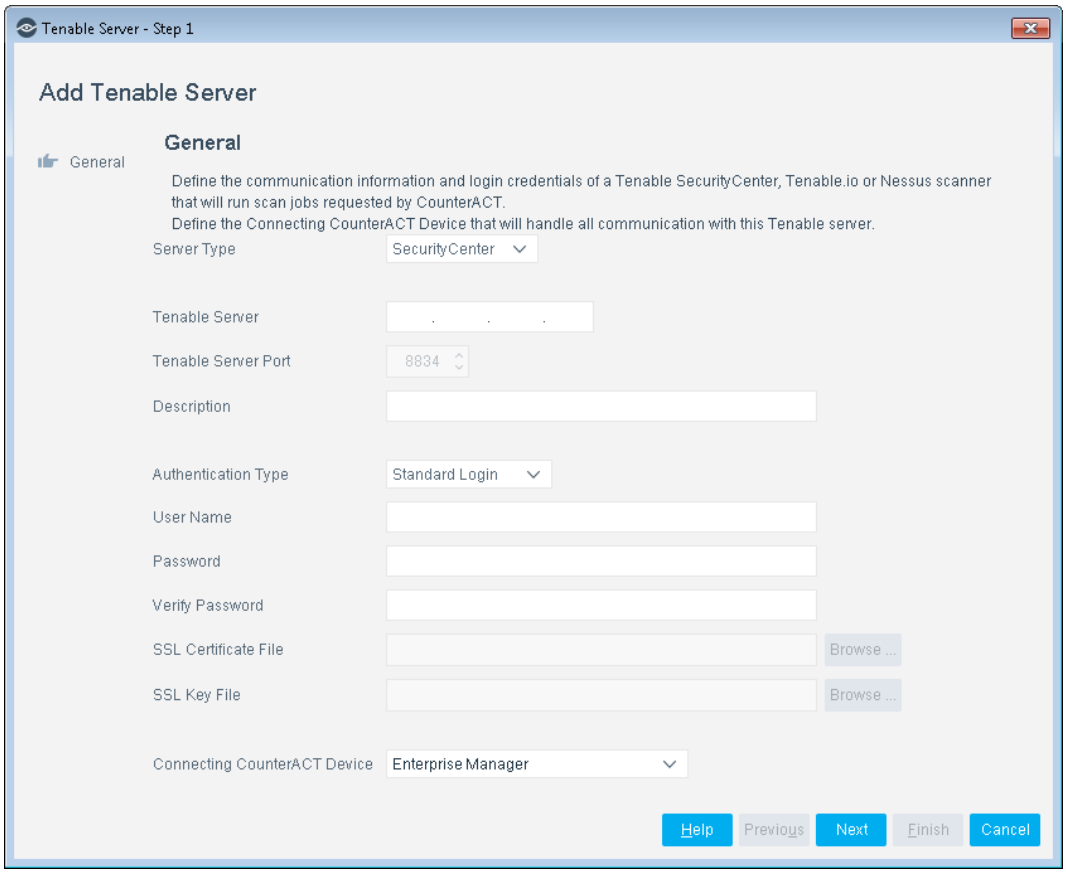


Add a Tenable Server

Enter basic information about the SecurityCenter, Nessus scanner or Tenable.io cloud to be added to the module configuration, and select a connecting CounterACT device.

To add a Tenable server:

1. In the CounterACT Console, select **Options** from the Tools menu. The Options dialog box displays.
2. Select **Tenable VM**. The Tenable VM displays in the right pane.
3. In the Tenable Servers tab, select **Add** to add a SecurityCenter server, Nessus scanner or Tenable.io. The Add Tenable Server wizard opens.

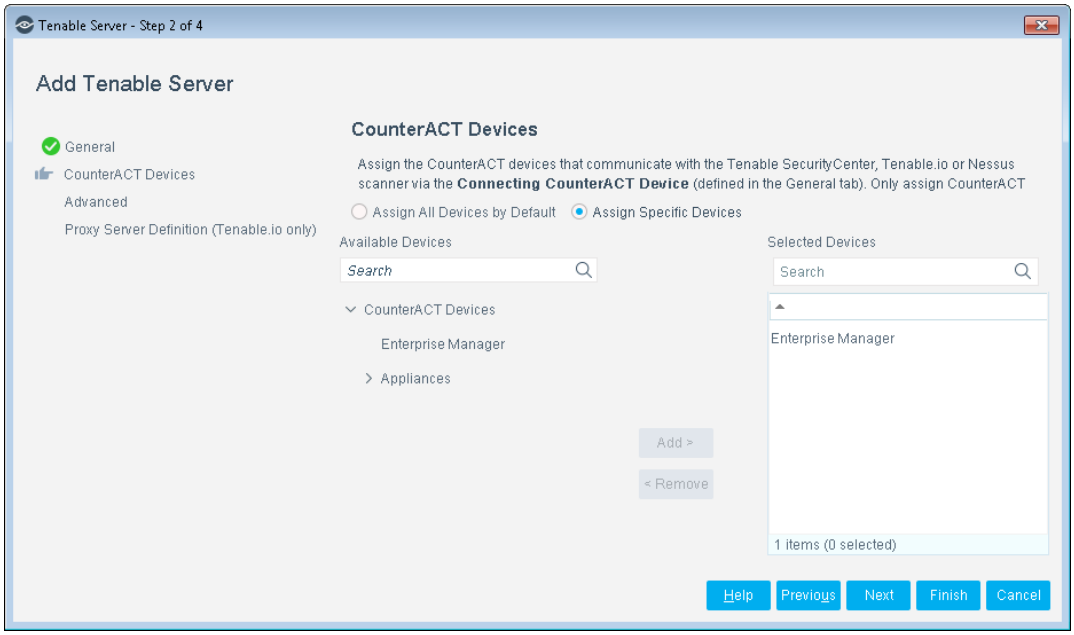


4. In the General pane, configure the following connection parameters:

Server Type	Select a type of Tenable Network Security server. The following options are available: ▪ ***SecurityCenter*** - All fields are active except the Tenable server port. ▪ ***Tenable.io*** - After selecting this option, enter information into the activated Description, User Name, Password and Verify Password fields. All other fields are deactivated. ▪ ***Nessus Scanner*** - when selected, all fields in this pane are active except the Authentication Type and the two SSL fields.
Server Address	IP address of Nessus or SecurityCenter that will execute CounterACT scan requests on one or more identified endpoints. The Nessus scanner or SecurityCenter must be able to handle the IP ranges of its assigned CounterACT devices. If *Tenable.io Server Type* is selected, this field contains a non-editable URL.
Tenable Server Port	Port used to access the SecurityCenter or Nessus scanner. By default, this is port 8834. If *SecurityCenter* or *Tenable.io Server Type* is selected, this field is deactivated.
Description	Provide an optional description or add a relevant comment.

Authentication Type	This option is only available for SecurityCenter server type. Select one of the following: ▪ **Standard Login** for username/password authentication to the scanner or SecurityCenter. ▪ **SSL Authentication** for SSL certificate authentication to SecurityCenter.
User Name	▪ If SecurityCenter server type with **Standard Login** authentication is selected: a *Security Manager* account defined in SecurityCenter is required. ▪ If Tenable.io or Nessus server type is selected, enter the User Name.
Password **Verify Password**	Enter the password for the above User Name. Retype the password to confirm it.
SSL Certificate File	If SecurityCenter server type and SSL Authentication type is selected, select the **SSL Certificate File**. Enter or browse to the full path of the client certificate to be used for SecurityCenter authentication.
SSL Key File	After selecting the SSL Certificate File, enter or browse to the full path of the certificate key to be used for SecurityCenter authentication.
Connecting CounterACT Device	Select a CounterACT device to be assigned to the defined Tenable vulnerability product. This CounterACT device manages all communication with the defined server, including forwarding scan requests submitted by all CounterACT devices assigned to this Tenable vulnerability product, and dispatching received scan results back to the appropriate devices.

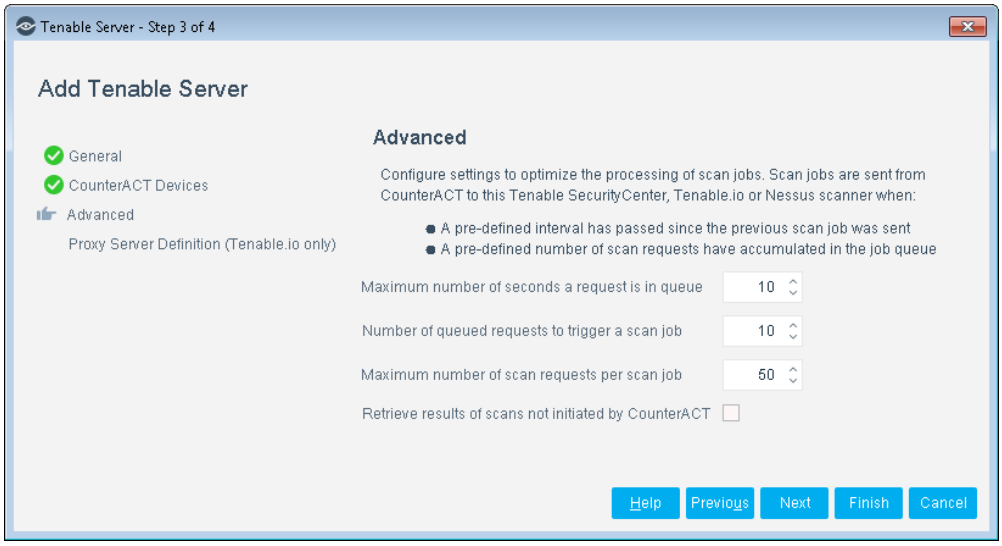
5. Select **Next**. The CounterACT Devices pane opens.



6. In the CounterACT Devices pane, assign the CounterACT devices that will work with the defined SecurityCenter, Tenable.io or Nessus, communicating via the connecting CounterACT device. Only assign CounterACT devices whose IP range fall entirely within the IP range that is handled by the SecurityCenter or Nessus scanner. Each CounterACT device can be assigned to *only* one SecurityCenter, Tenable.io, or Nessus scanner. Select one of the following options:
   - **Assign All Devices by Default:** Automatically assigns all unassigned CounterACT devices to the defined SecurityCenter, Tenable.io, or Nessus scanner. When selected, it becomes the *default* Tenable vulnerability product. Exactly one vulnerability product must be designated the *default.*
   - **Assign Specific Devices:** Assigns specific CounterACT devices to work with the defined SecurityCenter, Tenable.io, or Nessus scanner.

   If no other Tenable Network Security servers have been added to the module, all devices are assigned to this server by default. In an environment with multiple servers, consider the topology of your network when deciding which CounterACT devices to assign to each server.

7. Select **Next**. The Advanced pane opens. The Advanced tab is for defining advanced configuration parameters. Endpoint scan requests can be generated by CounterACT policies and by manual actions. A collection of endpoint scan requests is called a scan job. Configure settings to optimize the processing of scan jobs.

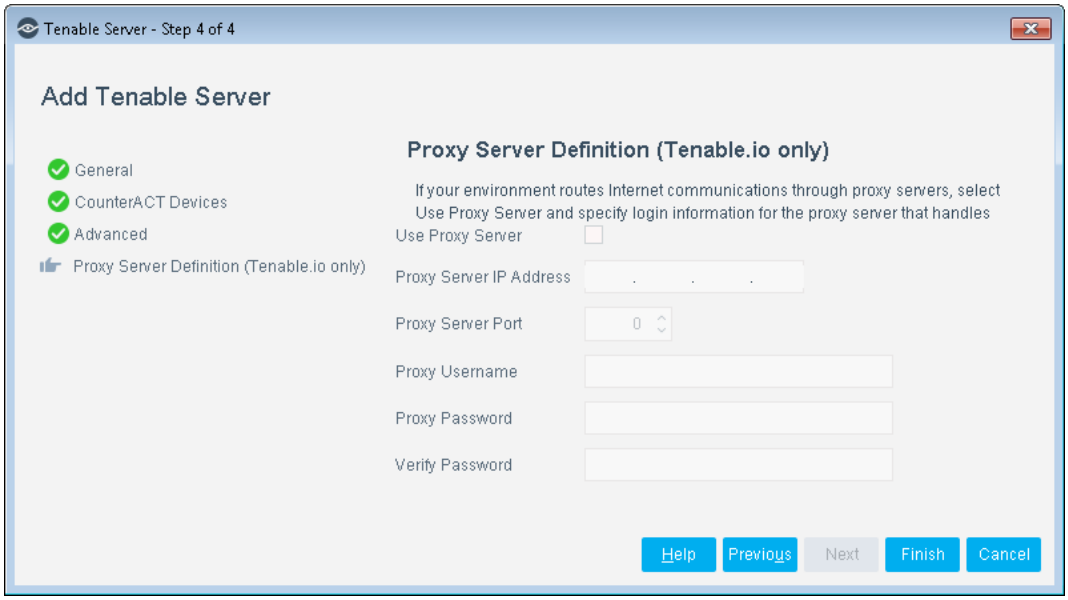


8. In the Advanced pane, configure the following scan job processing settings:

Maximum number of seconds a request is in queue	The interval, in seconds, in which the module collects endpoint scan requests from assigned devices and adds them to its scan job queue. When this interval expires, the module sends the collected endpoint scan requests in a scan job to the relevant Tenable vulnerability product.

Number of queued requests to trigger a scan job	The number of queued scan requests that triggers an expedited scan job even before the defined interval elapses. During a collection interval, host scan requests are added by the module to its scan job queue. When the queue reaches the value defined for **Number of queued requests to trigger a scan job**, the module submits an expedited scan job to the relevant Tenable vulnerability product. The number of hosts to scan per job never exceeds the **Maximum number of scan requests per scan job** value.
Maximum number of scan requests per scan job	The maximum number of hosts that the module can include in any scan job that it sends to the relevant Tenable vulnerability product. This setting helps balance between scanner efficiency (where submitted scan jobs include a large number of hosts to scan) and quicker compliance verification (where submitted scan jobs include a small number of hosts to scan).
Retrieve results of scans not initiates by CounterACT	When this box is checked, the following policy properties will report results from ALL scans, not just CounterACT-initiated scans: ▪ Tenable Scan Results ▪ Tenable Scan Status

9. Select **Finish**. Optionally, if a Tenable.io proxy needs to be configured, select **Next**. The Proxy Server Definition pane displays.



10. When your environment routes Internet communications through proxy servers, configure the following connection parameters for the proxy server that handles communication between this Tenable.io cloud platform and its Connecting CounterACT device. In the Proxy Server Definition pane, configure the following settings.

User Proxy Server	Select this option to use a proxy server to communicate with Tenable.io.

Proxy Server 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. A management level (or higher) account defined in SecurityCenter is required.
Proxy Password	Enter the password for the above Proxy User Name.
Verify Password	Retype the password to confirm it.

11. Select **Finish**. The scanner appears in the Tenable Servers tab.
12. In the Tenable VM pane, select **Apply**.

Synchronize Scan Parameters and Select Defaults

CounterACT incorporates the following Tenable information into its scan requests:

- ***Scan policies*** - Specifies which vulnerabilities will be tested during the scan. One name per scan.
- ***Repositories*** - Specifies the location where the scan results will be stored. One name per scan for SecurityCenter servers; ignored for Nessus scanners.
- ***Zones*** - Upon syncing, the Zones tab populates based upon the settings within SecurityCenter. This occurs if SecurityCenter allows the zones to be selected in the parameters dialog box right before a scan is launched. If this tab is empty, it means that the SecurityCenter did not allow selection of the zones.
- ***Scanners*** - The Scanners tab is populated for Tenable.io devices and displays all managed Nessus scanners.
- ***Credentials*** - Enables in-depth endpoint scanning by authorizing access to specific information that would otherwise be protected. One or more names per scan are optional for SecurityCenter servers; ignored for Nessus scanners.

Use the Tenable Servers tab to synchronize CounterACT with the up-to-date list of scan parameters. Use the other tabs to view the lists of synchronized parameters.

To synchronize scan parameters with all Tenable servers and set defaults:

1. In the CounterACT Console, select **Options** from the Tools menu. The Options dialog box opens.
2. In the left pane, select **Tenable VM**. The Tenable VM pane displays.
3. In the Tenable Servers tab, select **Sync**.
4. The lists in the **Scan Policies, Repositories, Zones, Scanners** and **Credentials** tabs are updated.
5. Select the **Scan Policies** tab, select a scan policy to be used for scans and then select **Make Default**. If more than one Tenable server is defined, each one needs a default policy.

6. For Tenable.io, navigate to the **Scanners** tab, select the scanner and then select **Make Default**.
7. For SecurityCenter, select the **Repositories** tab, select a repository name and then select **Make Default**.
8. Select **Apply**.

If a scan policy, repository, zone, scanner or credential is added, removed or renamed in the Tenable server, you must re-sync the scan parameters in the module configuration. Tenable-related property resolution and actions will not be handled in CounterACT if the scan parameter names do not match.

9. To ensure that the scan parameters are up-to-date, Run a Module Test.

Set Auto-Deletion of Scan Results

By default, after 30 days, any CounterACT-initiated scans will automatically be deleted from the Tenable server. You can manually make your own settings for the Scan results.

1. Open a terminal and change to the following directory:

`/usr/local/forescout/plugin/nessus`

2. Open the install.properties file
3. Copy the following property code:

`config.nessus_reports_older_than.value=2592000`

The value of 2592000 (seconds) is the equivalent of 30 days.

4. Open the local.properties file and paste the code.
5. Change to the desired value.

Entering a value of 0 switches off the automatic deletion of scans.

6. Select **Save**.
7. **Restart** the Tenable VM Module.

Test the Module Configuration

This section describes the following:

- Define Test Configuration Parameters
- Run a Module Test
- Export the Test Results

Define Test Configuration Parameters

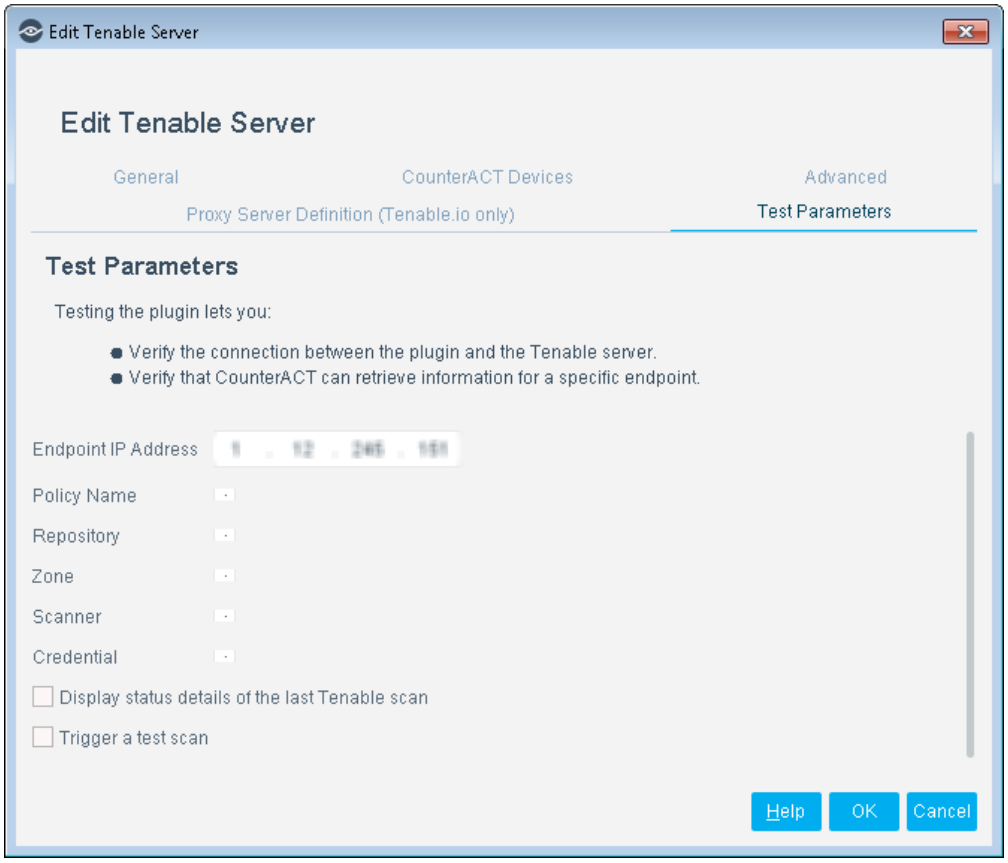
Define test configuration parameters to use when testing the module configuration. Completing these parameters does not trigger a test. To run the test see Run a Module Test.

Use this feature to:

- Test the connection between the module and Nessus, Tenable.io, or SecurityCenter.
- Verify that CounterACT can retrieve information for a specific endpoint.
- Trigger a scan request.

To set test parameters:

1. In the Tenable Servers tab, select the scanner or SecurityCenter to be tested, and select **Edit**. The Edit Tenable Server dialog box opens.
2. Select the **Test Parameters** tab.



3. In the **Test** Parameters tab, configure the following fields to be used when the test is run:

Endpoint IP Address	Enter the IP address of the endpoint on which to carry out the test. ▪ 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 **Trigger a test scan** is not selected, enter any IP value.

Policy Name	Select the Tenable scan policy for which the scan test requested will be carried out.
Repository	Select a repository to save the SecurityCenter scan to.
Zone	Select a zone if this drop-down is populated. It is not an error if this field is empty.
Scanner	If this is a Tenable.io scan, select a scanner.
Credential	Select the credential for the scan test (optional).
Display status details of the last Tenable scan	Retrieve scan status details of the endpoint to be tested. See Tenable Scan Status for more information.
Trigger a test scan	Trigger a scan on the endpoint to test the scan trigger.

For descriptions of the other tabs listed in the Edit Tenable Server wizard, see Add a Tenable Server.

4. Select **OK**. The scan test parameters are saved.
5. In the Tenable VM pane, select **Apply**.
6. Select **Close**.

Run a Module Test

Run the module configuration test to test the following:

- The connection of the module to the Tenable server
- The ability of CounterACT to retrieve scan results
- That the scan policy name, repository and credentials selected in the **Test** Parameters tab of the module configuration are synchronized with the Tenable server

To run a module test:

1. Be sure the test settings are appropriate for the test. See Define Test Configuration Parameters.
2. In the Tenable Servers tab, select the **scanner** or **SecurityCenter** to be tested. You can select more than one SecurityCenter server, Tenable.io or Nessus scanner.
3. Select **Test**. The test is run.
4. When finished, select **Close**.

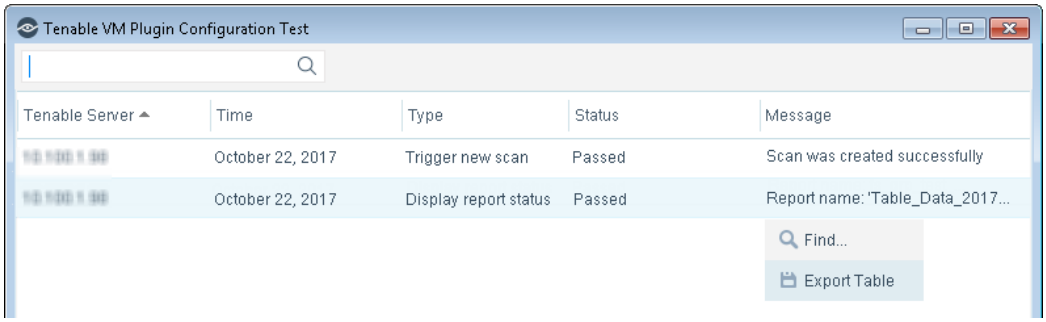
Export the Test Results

You can export the test results as a report in a user-friendly format. The available report formats are:

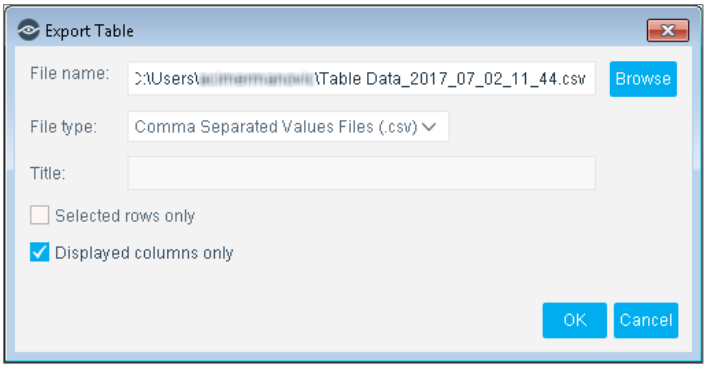
- CSV (viewable in spreadsheet applications, such as Microsoft Excel)
- PDF (viewable in Adobe Acrobat)

To export the report:

1. Right-click anywhere on the report.
2. Select **Export Table...** from the popup menu.



3. Select a name and format for the information to export.



4. Select **OK** to export the report.

Run Tenable Vulnerability Management Policy Templates

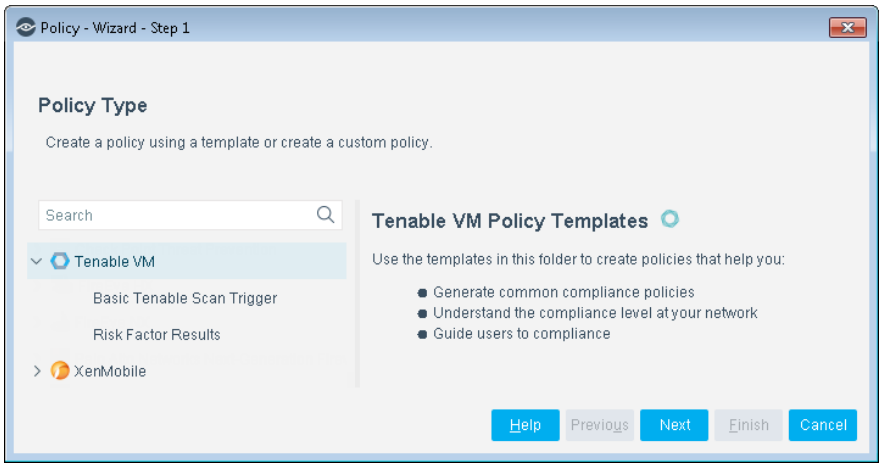
CounterACT policy templates help you quickly create important, widely-used policies, easily control endpoints and guide users to compliance.

Predefined actions – instructions regarding how to handle endpoints – are generally disabled by default when working with templates. You should only enable actions after testing and fine-tuning the policy.

Working with Tenable VM templates requires you to incorporate Tenable information. See Synchronize Scan Parameters for details.

The following templates are available for detecting and managing endpoints:

- Basic Tenable Scan Trigger Template
- Risk Factor Results Template



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

CounterACT Policy Coordination Considerations

Before creating or modifying Tenable VM-related CounterACT policies, it is important to consider the following points:

In large-scale deployments, with multiple scanners and Appliances, the host and SecurityCenter server, Tenable.io, or Nessus scanner are connected via the CounterACT Appliance. The CounterACT Appliance determines which endpoints will connect with it, and to which server the scan requests will be sent. This is configured in the Tenable VM Module Configuration Settings.

This means that the Tenable Server IP may differ between endpoints. Therefore it is important to add the Tenable Server IP property to any CounterACT policy condition that checks the scanner status.

CounterACT can handle multiple concurrent Tenable scan policies. This allows concurrent triggers for individual Tenable scan policies as well as the management of multiple scan results stemming from these triggers. This means that CounterACT requires a specific Tenable scan policy name to trigger a scan, but it does not require a Tenable scan policy name when handling the scan result. CounterACT policy actions are based on the scan results and the host properties. If there is a situation where this is insufficient, it is up to the CounterACT operator to ensure that the necessary changes are made.

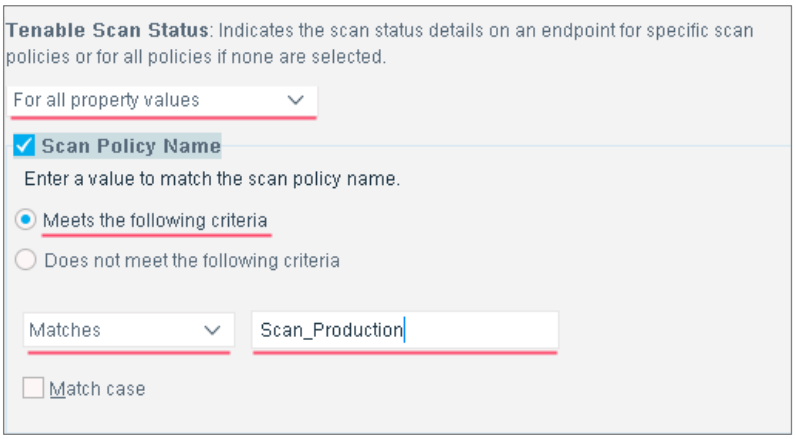
A CounterACT host property can accommodate multiple scan results if they differ by their associated Tenable scan policy. When referencing properties such as *Tenable Scan Status*, it is important to specify which *Scan Policy Name* this condition applies to. For example, assume you have defined the Tenable scan policies N1 & N2 and that CounterACT triggers scans using these policies at T1 & T2 respectively.

To define a condition to rescan the host:

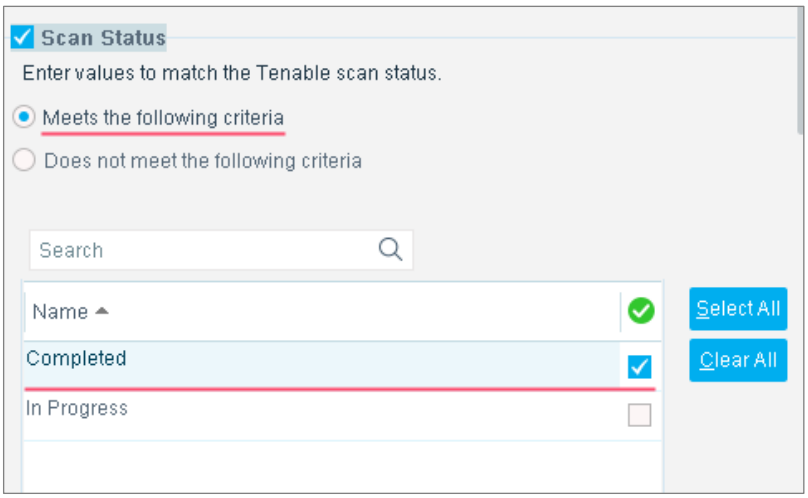
If you would like to define a condition to rescan the host after X1, X2 number of minutes elapsed since its last scan:

If ((*Last Scan* > X) AND (*Scan Policy Name* = N1)) --> trigger scan (N1)

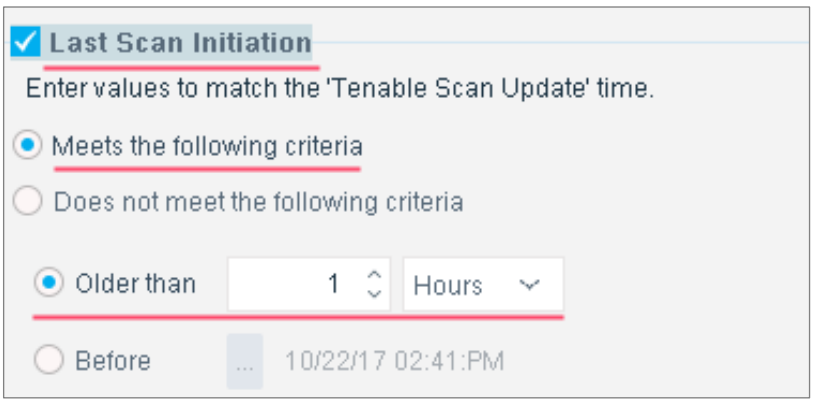
1. Select *For all property values*.
2. In the **Scan Policy Name** section, set the parameters to:



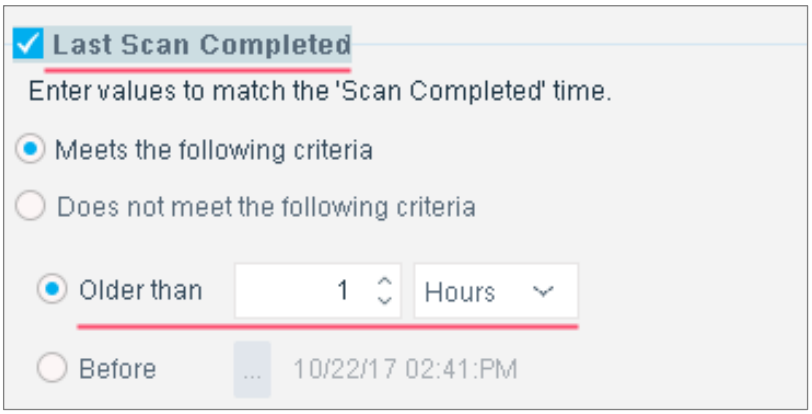
3. In the **Scan Status** section, set the parameters to:



4. In the **Last Scan Initiation** section, set the parameters to:



5. In the **Last Scan Completed** section, set the parameters to:



6. Select **OK** to complete the settings.

If you do not specify a Tenable *Scan Policy Name* in the above condition, CounterACT will assume that ***any*** *Last Scan* that is greater than X is sufficient to satisfy the above condition.

Basic Tenable Scan Trigger Policy Template

The Basic Tenable Scan Trigger policy template provides basic triggering capacity. You can update the defaults as required and can further customize the policy.

Use this template to create a policy that triggers a scan request for a selected scan policy, based on the following default settings:

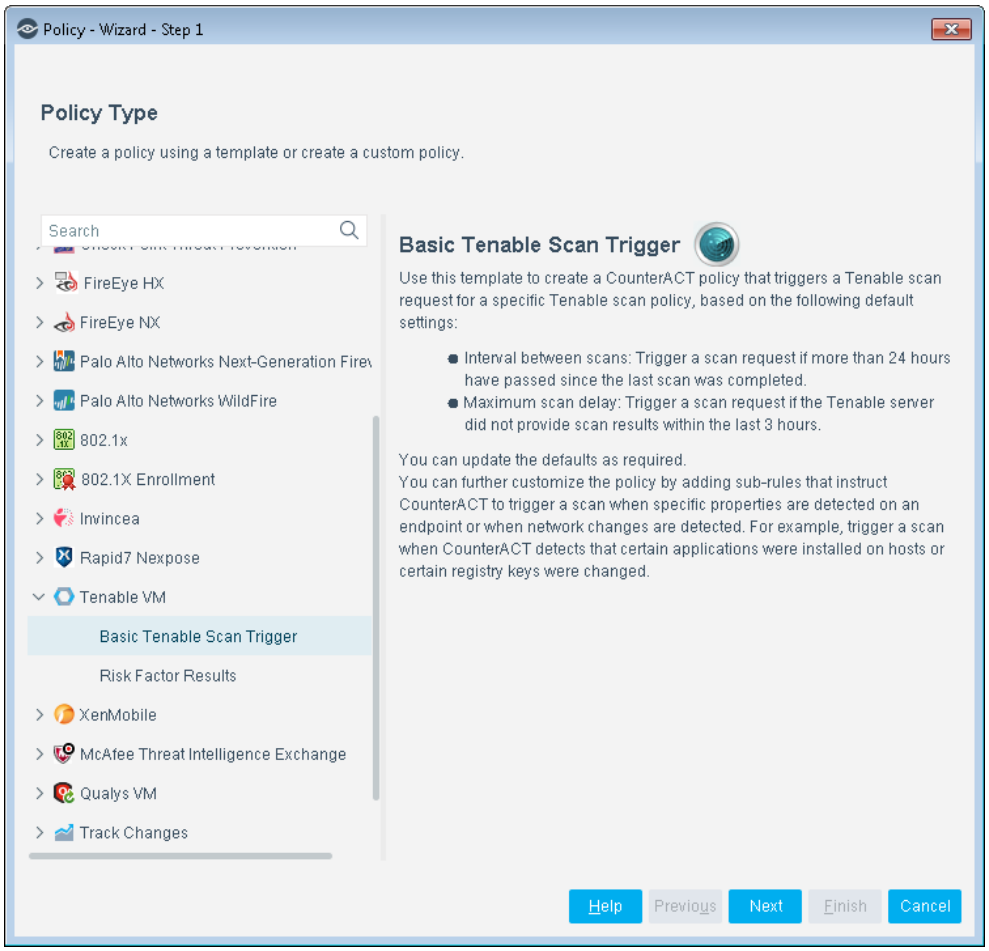
- Interval between scans: Trigger a scan request if more than 24 hours have passed since the last scan was completed.
- Maximum scan delay: Trigger a scan request if the SecurityCenter, Tenable.io, or Nessus scanner did not provide scan results within the last 3 hours.

Before triggering the scan request, the policy verifies that the Tenable VM module and the Nessus scanner, Tenable.io, or SecurityCenter are connected. If no connection is established, the module does not carry out further inspection on the endpoint. By default, module-to-scanner connectivity is checked once an hour.

This policy template provides basic triggering capacity. You can update the defaults as required and can further customize the CounterACT policy by adding sub-rules that instruct CounterACT to only trigger a scan when an endpoint is detected with specific properties. For example, instruct CounterACT to trigger a scan request when it detects that certain applications were installed on endpoints 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 Tenable Scan Trigger policy template:

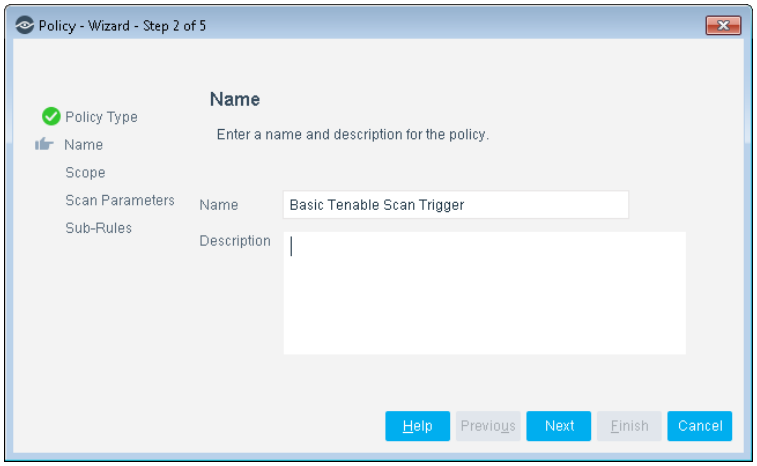
1. Log in to the CounterACT Console and select the **Policy** tab.
2. In the Policy Manager pane, select **Add**. The Policy Wizard opens.
3. Under Templates, expand **Tenable VM** and then select **Basic Tenable Scan Trigger**. The Basic Tenable Scan Trigger pane displays.



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

Name the Policy

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



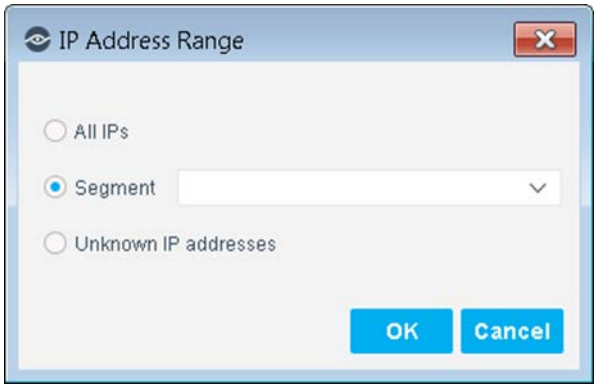
5. Define a unique name for the policy you are creating based on this template, and enter a description.

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

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

Define Which Endpoints Will Be Inspected - Policy Scope

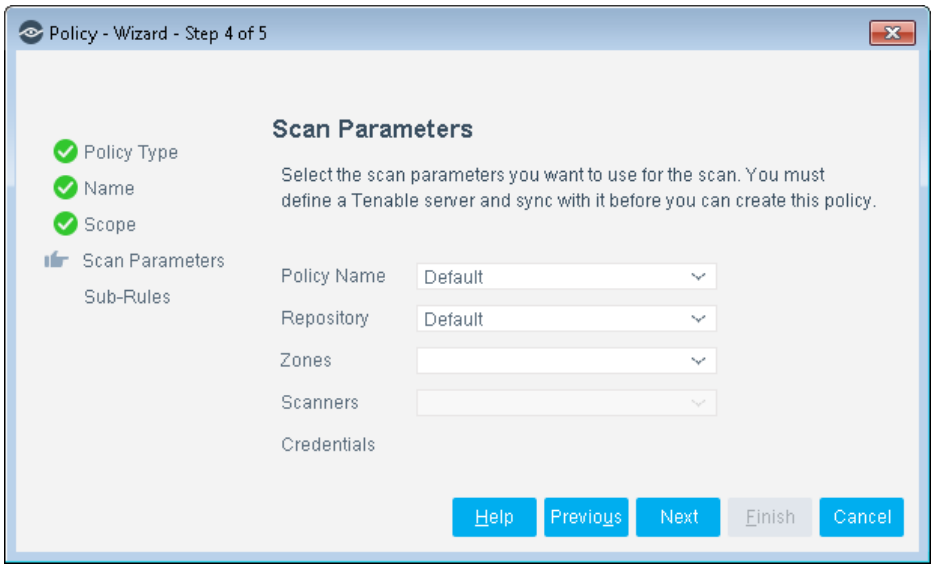
7. Use The IP Address Range dialog box to define which endpoints are inspected.



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 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 displays in the Scope pane. You can add multiple rows to the scope list by selecting **Add** and repeating steps 7-8.
9. Select **Next**. The Scan Parameters pane opens.

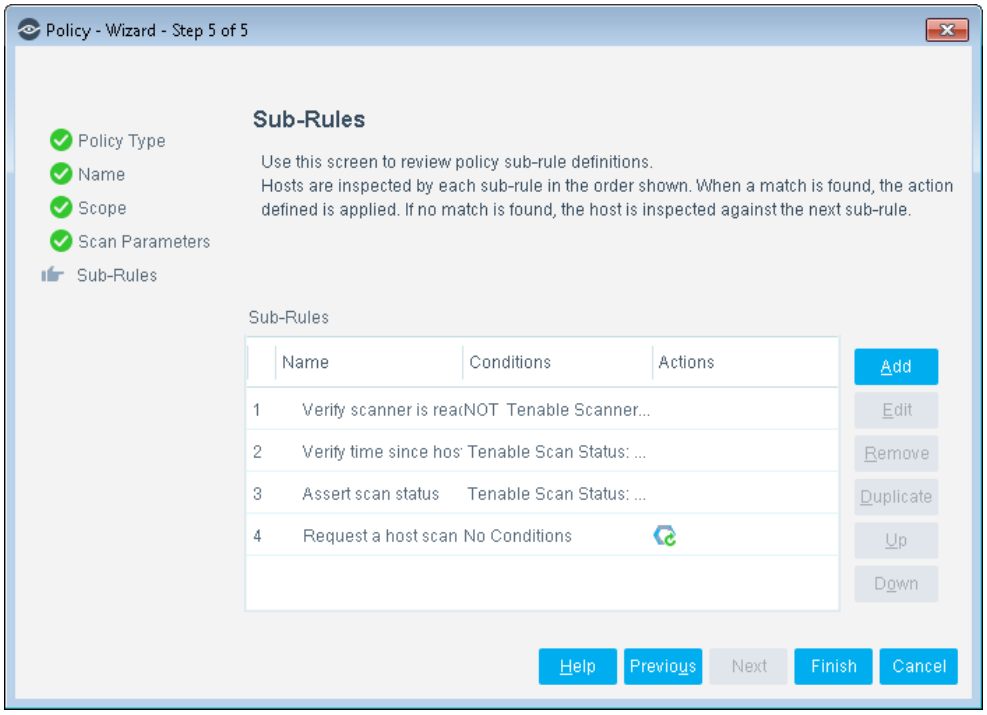


Set the Scan Parameters

10. Select the scan parameters to apply in this Tenable policy:

- **Policy Name** - Specifies which vulnerabilities are tested during the scan. One scan policy name is required for each scan.
- **Repository** - Specifies the location where the scan results will be stored. One repository name is required for SecurityCenter servers; ignore for Nessus scanners.
- **Zones** – Specifies the scan zone to use in some cases. It is not an error if the dropdown is empty.
- **Scanners** – Select the scanner type to use for Tenable.io. Ignore for SecurityCenter and Nessus scans.
- **Credentials** - Enables in-depth endpoint scanning by authorizing access to specific information that would otherwise be protected. One or more credentials are optional for SecurityCenter servers; ignore for Nessus scanners.

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



Sub-Rules

The Sub-Rules instruct CounterACT how to detect and handle endpoints. They also define how often the module-to-scanner connectivity is checked. The rules are predefined to detect the interval elapsed between scans, and the maximum scan delay on the endpoints you defined in the Tenable policy scope. A scan request is triggered on any endpoint that meets the default requirements. See Policy Properties - Detecting Vulnerabilities.

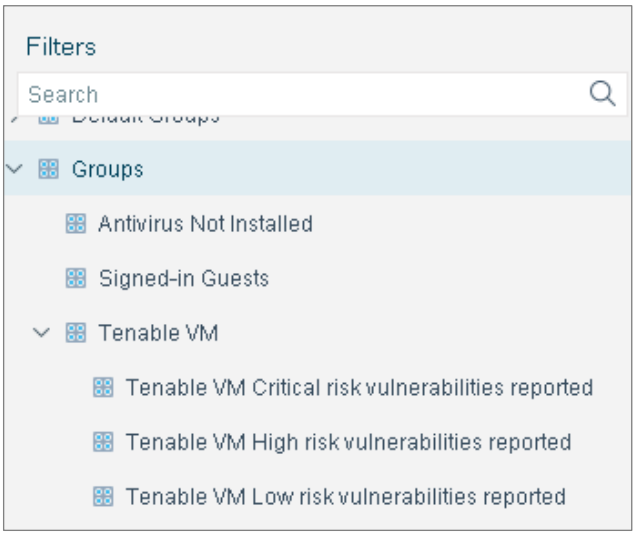
12. Select **Finish**.

Risk Factor Results Policy Template

Use the Risk Factor template to create a policy that detects the most current Tenable VM Module Risk Factor results assigned to network endpoints.

Risk factor results are based on all Tenable scan policies synchronized with the module. See Synchronize Scan Parameters for details.

The template organizes endpoints into CounterACT groups with critical, high, medium, or low.



You can later use these groups in CounterACT policies to control hosts. For example, assign endpoints with critical risks to an isolated VLAN.

Additional information about endpoints is also provided, such as the Tenable scan policy name, port scanned and protocol.

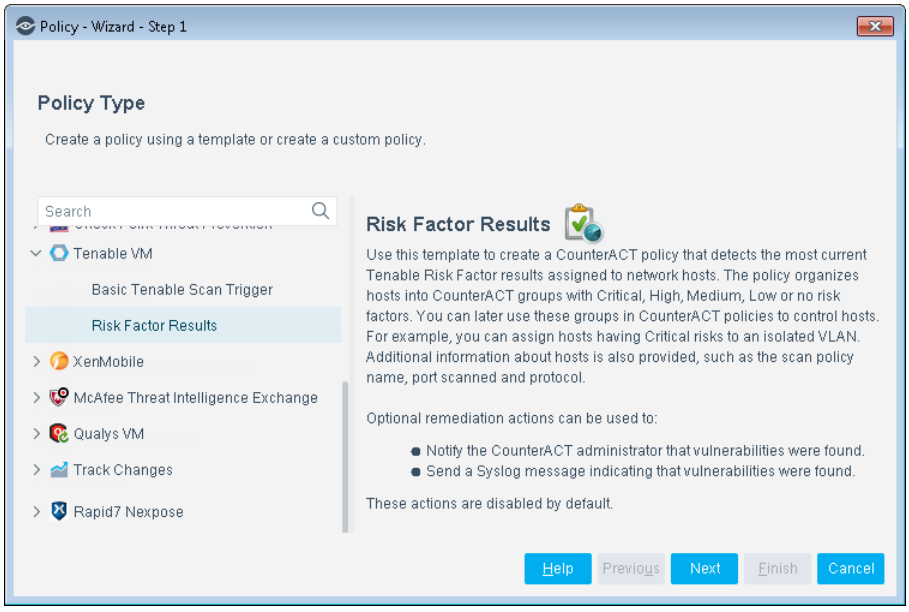
Optional remediation actions are predefined in the template and can be used to:

- 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 Risk Factor Results policy template:

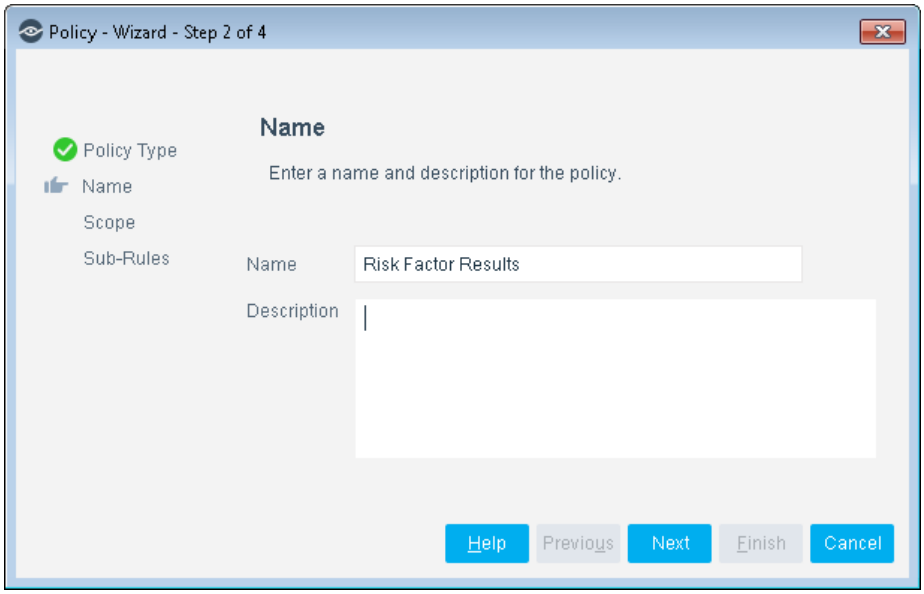
1. Log in to the CounterACT Console and select the **Policy** tab.
2. In the Policy Manager, select **Add**. The Policy Wizard opens.
3. Expand **Tenable VM** and select **Risk Factor Results**. The Risk Factor Results pane displays.



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

Name the Policy

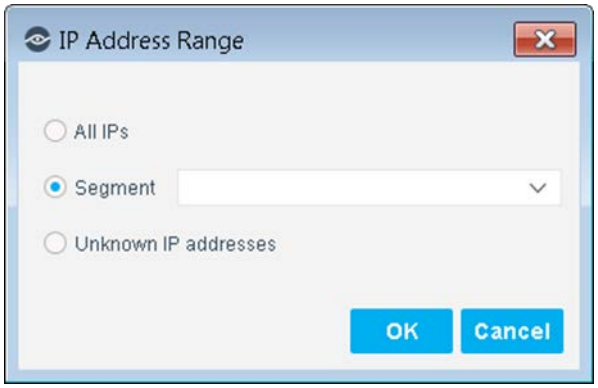
The Name pane lets you define a unique policy name and useful policy description. Policy names appear in the Policy Manager, the Views pane, NAC Reports and in other features. Precise names make working with policies and reports more efficient.



5. Define a unique name for the policy you are creating based on this template, and enter a description.
   - Make sure names are accurate and clearly reflect what the policy does. For example, do not use a generic name such as My_Compliance_Policy.
   - Use a descriptive name that indicates what your policy is verifying and which actions will be taken.
   - Ensure that the name indicates whether the policy criteria must be met or not met.
   - Avoid having another policy with a similar name.
6. Select **Next**. The Scope pane and the IP Address Range dialog box opens.

Define Which Endpoints Will Be Inspected - Policy Scope

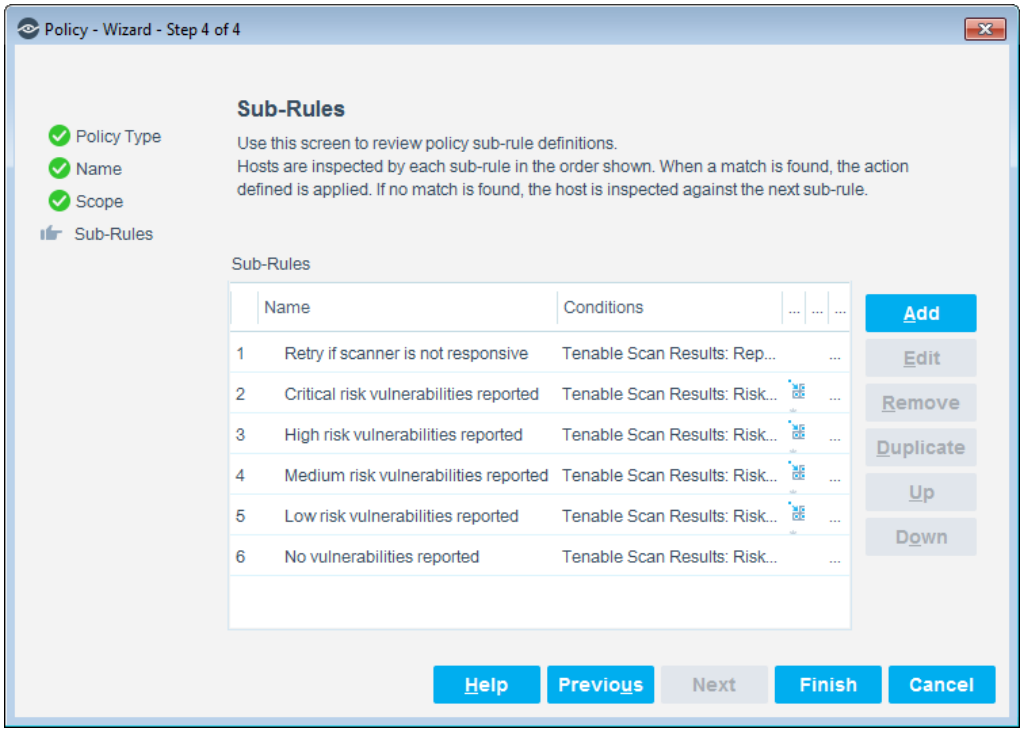
7. Use The IP Address Range dialog box to define which endpoints are inspected.



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 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. You can add multiple rows to the scope list by selecting **Add** and repeating steps 7-8.
9. Select **Next**. The Sub-Rules pane opens.



Sub-Rules

The Sub-Rules instruct CounterACT how to detect and handle endpoints. They also define how often the module-to-scanner connectivity is checked. The rules are predefined to detect the interval elapsed between scans, and the maximum scan delay on the endpoints you defined in the Tenable policy scope. A scan request is triggered on any endpoint that meets the default requirements. See Policy Properties - Detecting Vulnerabilities.

10. Select **Finish**.

Create Custom Tenable Vulnerability Management Policies

Custom policy tools provide you with an extensive range of options for detecting and handling endpoints. Specifically, use the policy to instruct CounterACT to

apply a policy action to endpoints that match (or do not match) property values defined in policy conditions.

For more information see CounterACT Policy Coordination Considerations.

To create a custom Tenable Vulnerability Management policy:

1. Log in to the CounterACT Console and select the **Policy** tab. The Policy Manager pane displays.
2. Select **Add**. The Policy Wizard opens.
3. Select **Custom**. The Custom policy type pane displays.
4. Select **Next**. The Name pane displays.
5. Enter a name and add a description (optional).
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. By default, the template excludes network printers from the scope.
8. Select **OK**. The new host address displays in the Scope pane. You can add multiple rows to the scope list by selecting **Add** and repeating steps 7-8.
9. (Optional) Select the wrench icon. The Advanced fields display. It is recommended to select **Add** from the Filter by Group section to include only Windows, Linux/Unix and Macintosh machines.
10. Select **Next**. The Main Rule pane opens.

How Endpoints Are Detected and Handled

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

Endpoints that match the Main Rule are included in the policy inspection. *Endpoints that do not match this rule are not inspected for this policy*. Sub-rules automatically follow up with endpoints after initial detection and handling, streamlining separate detection and actions into one automated sequence.

Sub-rules are performed in order until a match is found. When a match is found, the corresponding action is applied to the endpoint. If the endpoint does not match the requirements of the sub-rule, it is inspected by the next rule.

1. In the Conditions section, select **Add**. The Condition dialog box displays.
2. Expand the **Tenable VM** folder in the Properties tree. The following properties are available. For more information, select a link from the list to jump to the relevant section.
   - Tenable Scanner is Reachable
   - Tenable Scan Results
   - Tenable Scan Status
   - Tenable Server IP
   - Tenable Vulnerability Summary

Every property has the option to set the evaluation of irresolvable criteria as True/False.

3. When finished, select **OK** to close the Condition dialog box.
4. In the Group section of the Main Rule pane, select **Add**. The Action dialog box displays.
5. Expand **Audit** in the Actions tree and then select **Start Tenable Scan**.
6. Add Conditions and Actions based on the expected behavior of the custom policy.
7. Select **Next**. The Sub-Rules pane opens.
8. Sub-Rules are additional Condition / Action pairs. For definitions, see Policy Properties - Detecting Vulnerabilities.
9. Select **Finish**.

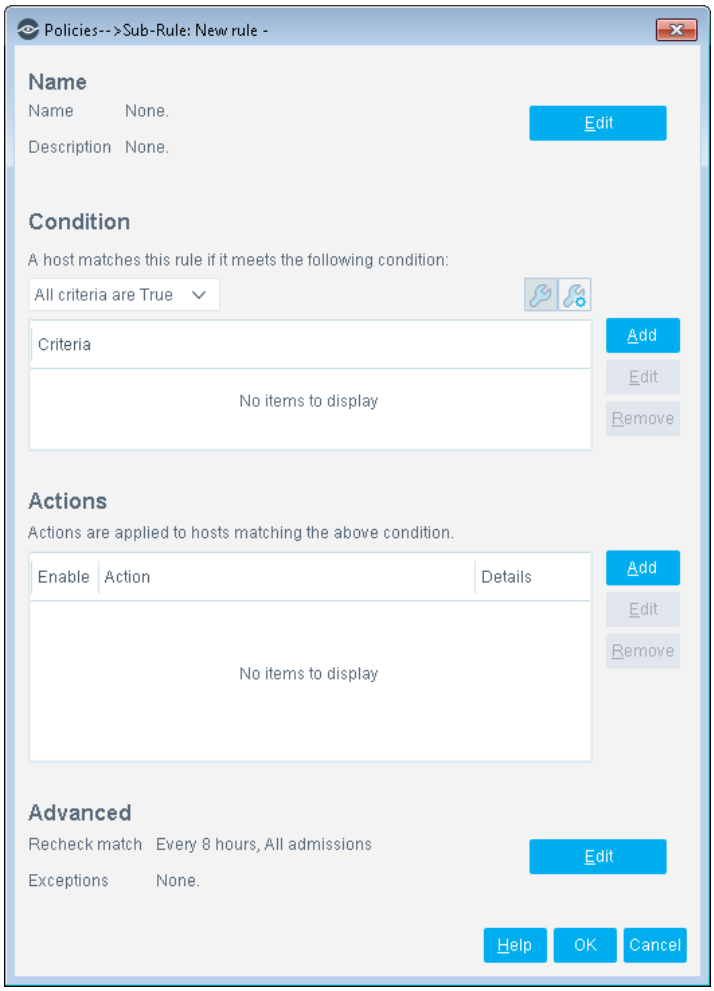
Policy Properties - Detecting Vulnerabilities

Policy Properties let you instruct CounterACT to detect endpoints with specific attributes or conditions. These conditions are set in the Sub-Rules section in the Policy Wizard. For example, you can create a policy that instructs CounterACT to determine the last Tenable scan.

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

To access Tenable Vulnerability Management properties:

1. In the Sub-Rules pane of a Policy Wizard or edit a policy.
2. In the Sub-Rules pane, select **Add**. The Name dialog box opens.
3. Enter a name and description of the sub-rule.
4. Select **OK**. The Sub-Rule: New Rule pane displays with the Name and Description field populated.



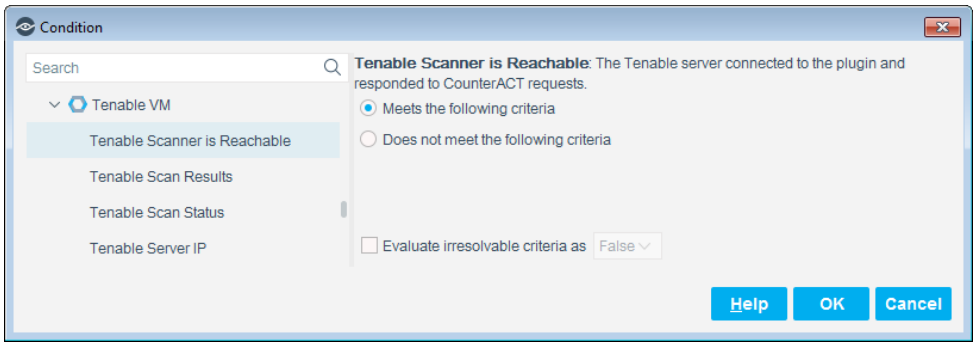
5. In the Condition section, select **Add**. The Condition dialog box opens.
6. Expand the **Tenable VM** folder in the Properties tree. The following properties are available. For more information, select a link from the list to jump to the relevant section.
   - Tenable Scanner is Reachable
   - Tenable Scan Results
   - Tenable Scan Status
   - Tenable Server IP
   - Tenable Vulnerability Summary

Every property has the option to set the evaluation of irresolvable criteria as True/False.

7. When finished, select **OK** in the Conditions dialog box. Your new criteria displays in the Sub-Rule: New Rule dialog box.
8. To continue, go to Policy Actions - Scanning Endpoints.

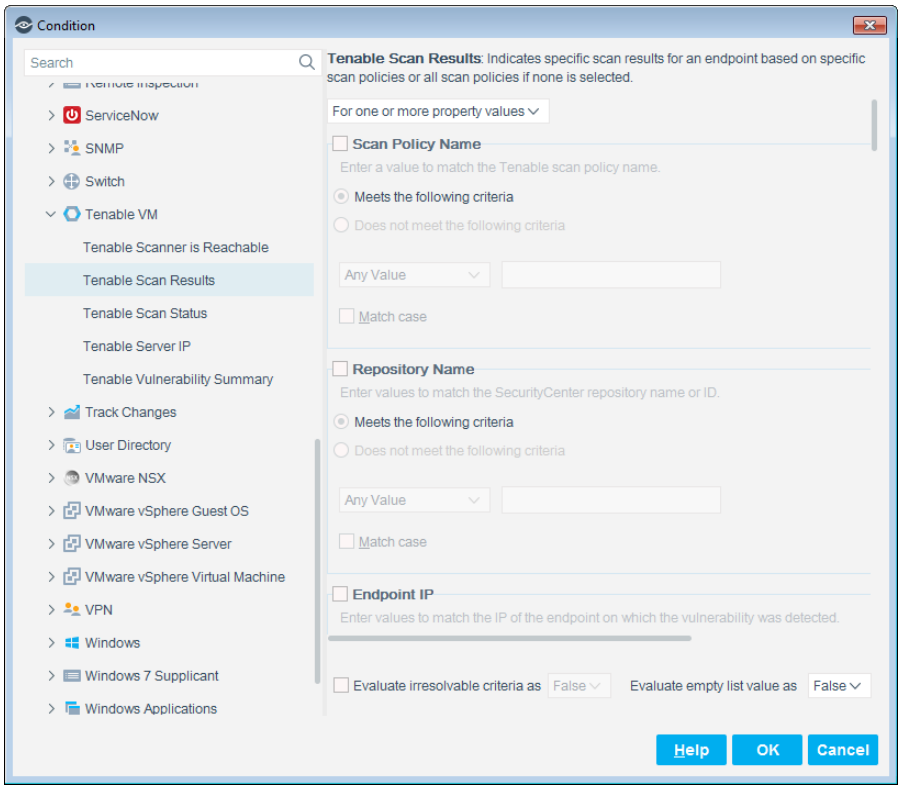
Tenable Scanner is Reachable

Set whether to indicate if the SecurityCenter server, Tenable.io, or Nessus scanner connected to the Tenable VM module responds to CounterACT requests.



Tenable Scan Results

Specify scan results for an endpoint based on a selected Tenable scan policy. If all items are deselected, the scan results will apply to all Tenable scan policies.



None of the properties in the Scan Results pane are selected by default, except for *Evaluate irresolvable criteria as*, which is set by default to *True*. Select if you want to apply the sub-field of the property.

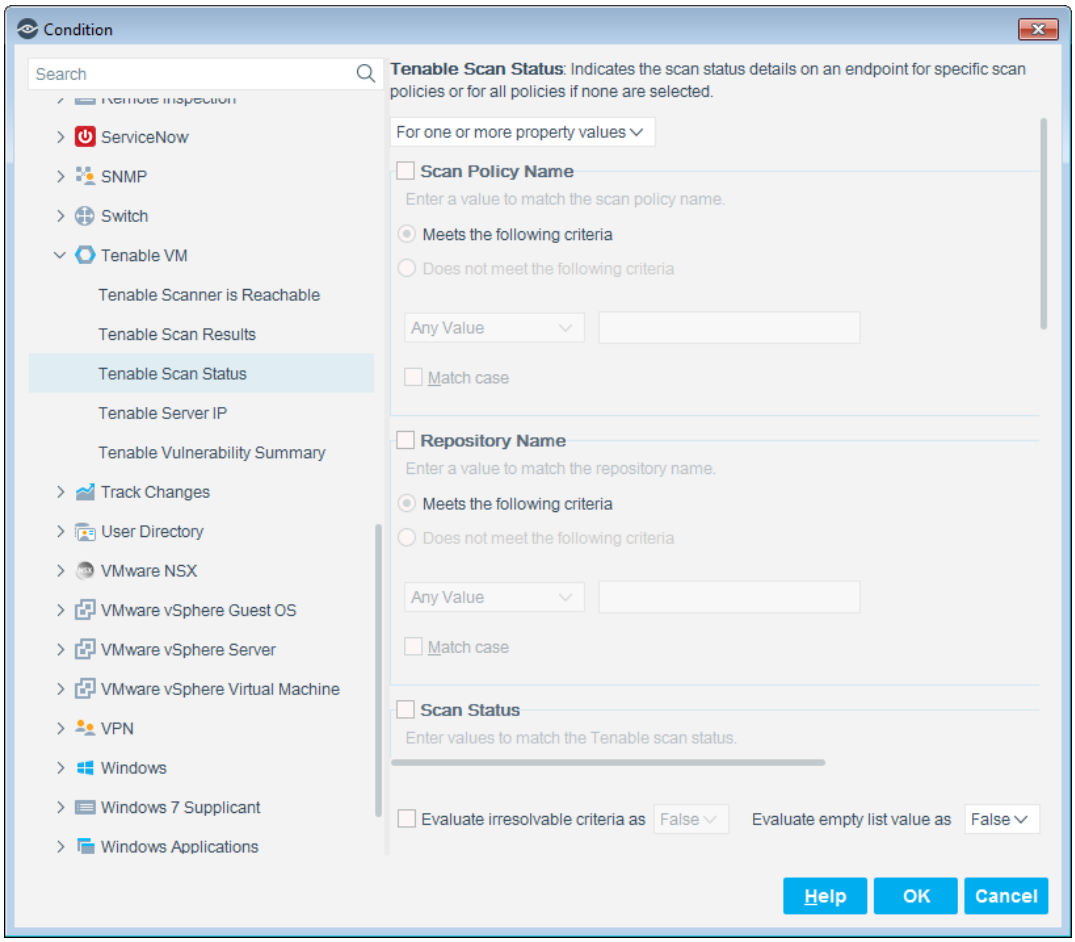
Scan Policy Name	The Tenable scan policy name. If you do not select a policy, the values will be resolved for all policies.
Repository Name	The name or ID of the SecurityCenter repository where the scan results are written. This applies to SecurityCenter servers only.

Endpoint IP	The IP address of the endpoint to be matched.
Port	The TCP/IP port of the scanned endpoint.
First Discovery Time	The time that the vulnerability was first discovered in a scan.
Last Discovery Time	The last time that the vulnerability was discovered in a scan.
Service	The name of the service detected by Tenable.
Protocol	The protocol used by the scanned endpoint to communicate; for example, TCP, UDP
Accept Risk	Enter a value to match the SecurityCenter Accept Risk value.
Severity	Any of the following vulnerability severities detected: None (Nessus scanner only) or Information (SecurityCenter only), Low, Medium, High, Critical.
Plugin ID	The human-readable ID of the reporting Tenable VM Module.
Plugin Name	The human-readable name of the reporting Tenable VM Module.
Plugin Family	The family to which the reporting Tenable VM Module belongs.
Synopsis	Brief description of the detected vulnerability.
Risk Factor	The human-readable form of the perceived risk factor of the vulnerability or vulnerabilities reported: None, Low, Medium, High, Critical.
Vulnerability Publication Date	Date the vulnerability was published.
Plugin Publication Date	Date the reporting Tenable VM Module was published.
Plugin Modification Date	Date the reporting Tenable VM Module was last modified.
CVSS Base Score	CVSSv2 base score.
CVE	CVE ID.
BID	Tenable Bugtraq ID (bug identifier).
Xref	Pointers to other vulnerability databases such as IAVA, MSFT, OSVDB.

If you enabled the Retrieve results of scans not initiated by CounterACT option, then the Tenable Last Scan condition will report results from ALL scans, not just CounterACT-initiated scans.

Tenable Scan Status

Set the scan status details on an endpoint for a specified Tenable scan policy. If none of the items are selected, the scan status details will apply to all Tenable scan policies.



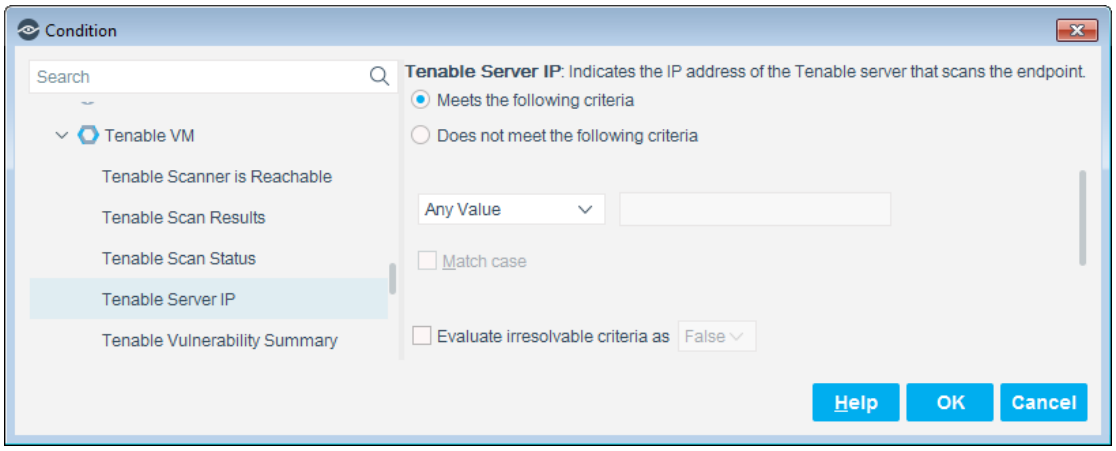
None of the properties in the Scan Status pane are selected by default. Select if you want to apply the sub-field of the property.

Scan Policy Name	The Tenable scan policy name. If you do not select a policy, the values will be resolved for all policies.
Repository Name	The name or ID of the SecurityCenter repository where the scan results are written. This applies to SecurityCenter servers only.
Scan Status	The status of the scan: ▪ *Completed* - Scan results received ▪ *In Progress* - The scan request was triggered by the module and activated by the SecurityCenter server, Tenable.io, or Nessus scanner
Last Scan Initiation	If the scan is in progress, the time the last scan request was made will be reported. Otherwise, the time the last scan was initiated by the Tenable vulnerability product is reported.
Last Scan Completed	Enter the values to match the *Scan Completed* time. If the scan is In Progress, then this field will contain the same value as the *Last Scan Initiation* field.

Tenable Server IP

This property indicates the IP address of the Nessus scanner that scans the endpoint or of the SecurityCenter server that manages the scanner.

Set the parameters and then select **OK**.

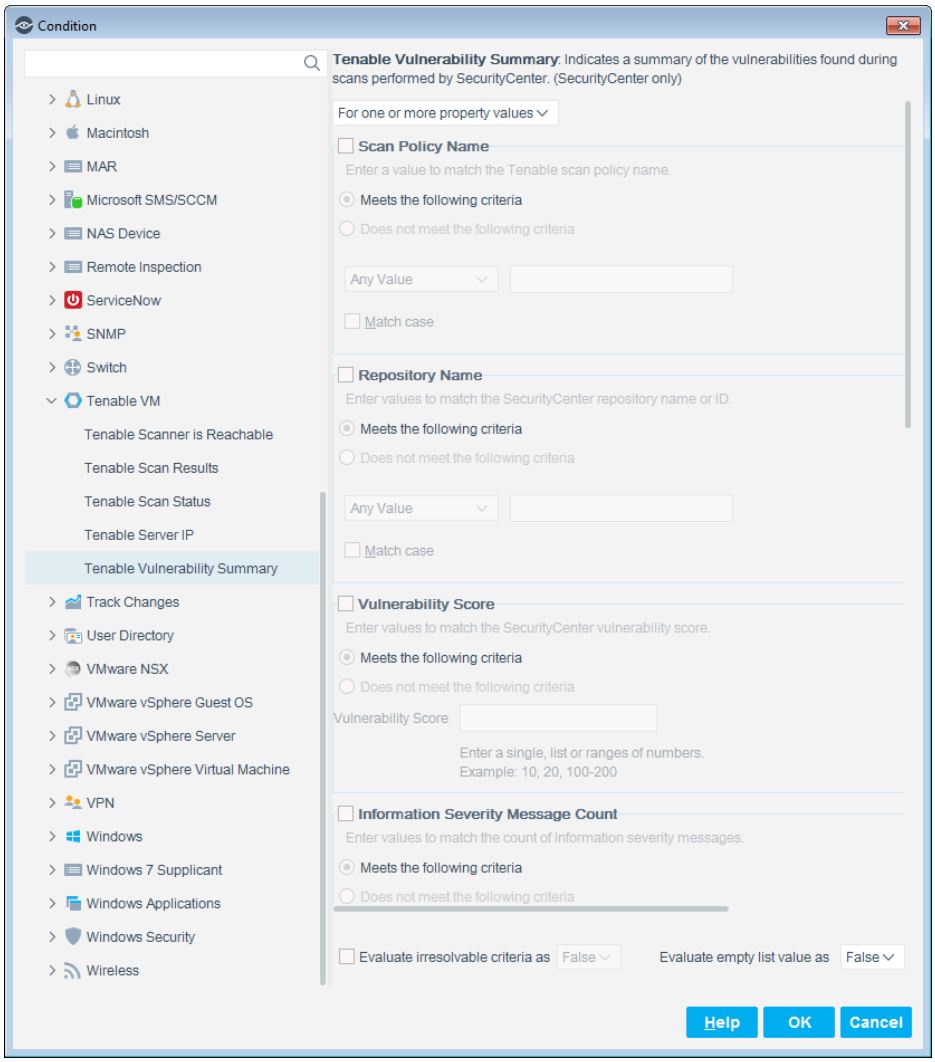


Tenable Vulnerability Summary

The Tenable Vulnerability Summary property indicates details of the vulnerabilities found by routine SecurityCenter scans on a specific endpoint.

If you are using SecurityCenter, set the parameters. If you are using a Nessus scanner or Tenable.io, this property does not apply.

> *The* SecurityCenter Vulnerabilities Found *property was made obsolete in release 2.6. If you migrated from a Tenable VM Module version 2.5 or earlier, the scan title will state Tenable Vulnerabilities Found Obsolete.*



Scan Policy Name	The Tenable scan policy name. If you do not select a policy, the values will be resolved for all policies.
Repository Name	The name or ID of the SecurityCenter repository where the scan results are written. This applies to SecurityCenter servers only.
Vulnerability Score	Enter vulnerability score values to match the SecurityCenter's vulnerability score.
Information Severity Message Count	Enter Information Severity Message Count values to match the count of Information severity messages.
Low Severity Defect Count	Enter Low Severity Defect Count values to match the count of Low Severity Defects.
Medium Severity Defect Count	Enter Medium Severity Defect Count values to match the count of Medium Severity Defects.
High Severity Defect Count	Enter High Severity Defect Count values to match the count of High Severity Defects.
Critical Severity Defect Count	Enter Critical Severity Defect Count values to match the count of Critical Severity Defects.
All Severity Counts	Enter a comma-separated list of the counts of the five severity levels, from Critical to Information.

Policy Actions - Scanning Endpoints

The CounterACT policy actions let you instruct CounterACT how to control detected devices. 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 Tenable-related actions to create custom CounterACT policies. This action is available when you install the Tenable VM module.

Start Tenable Scan

Use the Start Tenable Scan action in CounterACT policies to run a scan when certain policy conditions are met. For example, create a policy that runs a Tenable scan when CounterACT detects if an endpoint has a bad Linux credential.

To apply the Start Tenable Scan action to a policy:

1. Open the policy Actions dialog box.
2. Expand the **Audit** folder in the Actions tree.
3. Select **Start Tenable Scan**. The Parameters tab displays in the right panel.
4. Enter the following:

Policy Name	Enter a brief name to represent the policy the Tenable scan uses, for example, DNS Name or IPs.
Repository	Enter the values to match the SecurityCenter repository ID or name.
Zones	If SecurityCenter is configured in selectable mode, then the Zone drop-down is populated for selection.
Scanners	This option is activated for Tenable.io.
Credentials	Select the appropriate credential for this scan (optional).

5. Select the **Schedule** tab and select one of the following schedules:
   - ***Start action when host matches policy condition:*** A Tenable scan is started on the endpoint immediately upon a condition sub-rule match.
   - ***Customize action start time:*** Define when the Tenable scan on the endpoint should begin following a condition sub-rule match.
6. Select **OK**.

You can identify action success or failure in the CounterACT Console Detections pane.

Using the Tenable VM Module

Now that you have established communication between the ForeScout Extended Module for Tenable Vulnerability Management and a Tenable server, you can use this module to launch scans and create policies based on scan results.

Display Tenable VM Asset Inventory Events

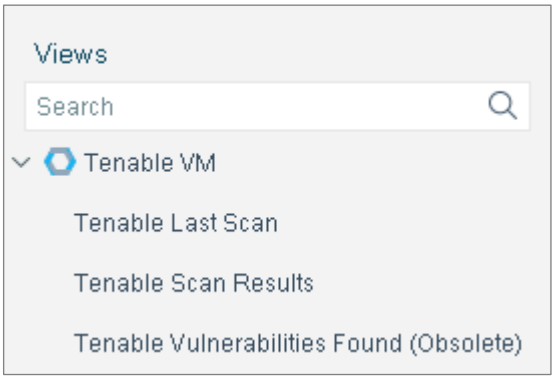
Use the CounterACT Asset Inventory to view a real-time display of Tenable scan result activity at multiple levels, for example, module family, risk factor or CVE information. You can browse the inventory to learn what CVEs have been detected on your network, and acquire information about endpoints with similar findings.

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 CounterACT policies.

To access the Asset Inventory:

1. Log in to the CounterACT Console and select the **Asset Inventory** tab.
2. Navigate to the Tenable entries or run a search on **Tenable**.



The following information is available:

– **Tenable Last Scan**: Displays the time of the last scan initiated by the Tenable plugin.
– **Tenable Scan Results**: Displays specific scan results for an endpoint based on a selected Tenable scan policy or all Tenable scan policies if none is selected.
– **Tenable Vulnerabilities Found (Obsolete)** - The *SecurityCenter Vulnerabilities Found* property was made obsolete in release 2.6. If you migrated from a Tenable VM Module version 2.5 or earlier, the scan title will state *Tenable Vulnerabilities Found Obsolete*.

Refer to *Working in the Console>Working with Inventory Detections* in the *CounterACT Administration Guide* or the Console online help for information about how to work with the CounterACT Asset Inventory.

Start Tenable Scan

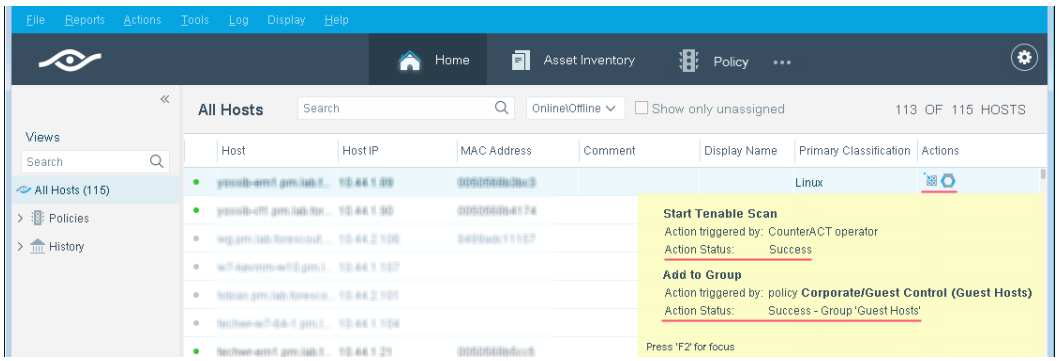
Use the ***Start Tenable Scan*** action in CounterACT to launch a scan after selected parameters are set. For example, create a CounterACT policy that detects if certain applications were installed on endpoints or if certain registry keys were changed, and trigger the scan when an endpoint meets this condition.

To manually start a scan:

1. In the CounterACT Console, select the **Home** tab.
2. In the Detections pane, right-click on an IP address, select **Audit** and then select **Start Tenable Scan**.
3. The Specify Start Tenable Scan parameters dialog box opens.
   - If SecurityCenter is configured to allow you to select a scan zone, then the Zones drop-down is populated for your selection.
   - If Tenable.io is configured, then the Scanner drop down is populated for selection.
4. Select your parameters and then select **OK**.

To view the results of a scan:

1. In the Detections pane of the **Home** tab, select the endpoint / IP address you just ran the scan on.
2. In the Actions column, an icon indicates the status of the scan.
3. Hover your mouse over the icon. The scan results display in a popup.



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**.

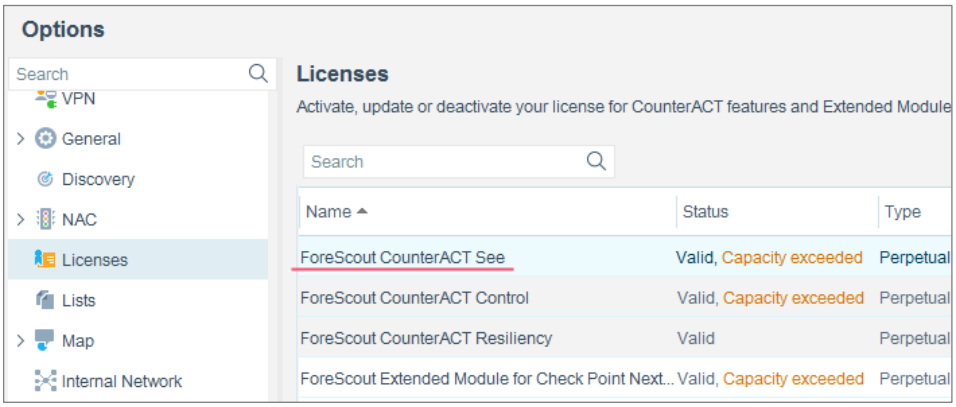
Documentation Portal

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

2018-07-29 11:32