



Forescout

eyeExtend for Tenable Vulnerability Management

Configuration Guide

Versions 3.0.2 and 3.0.3



Contact Information

Forescout Technologies, Inc.

190 West Tasman Drive

San Jose, CA 95134 USA

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

Toll-Free (US): 1.866.377.8771

Tel (Intl): 1.408.213.3191

Support: 1.708.237.6591

About the Documentation

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

Legal Notice

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

2020-08-24 07:37

Table of Contents

About the Tenable VM Integration	4
eyeExtend for Tenable VM – Concepts, Components, Considerations	5
How to Work with eyeExtend for Tenable VM.....	9
Install eyeExtend for Tenable VM Module.....	12
Configure eyeExtend for Tenable VM Module.....	13
Add Tenable Server	14
Synchronize Scan Parameters and Select Defaults	21
Set Auto-Deletion of Scan Results.....	25
Edit Tenable Server	25
Test eyeExtend for Tenable VM Configuration	26
Create Tenable VM Policies Using Templates.....	30
Forescout Platform Policy Coordination Considerations.....	31
Create a Basic Tenable Scan Trigger Policy	33
Create a Risk Factor Results Policy.....	38
Create Custom Tenable VM Policies.....	41
Tenable VM Policy Properties – Detect Vulnerabilities.....	49
Tenable VM Policy Actions – Scan Endpoints	57
Tenable VM – Asset Inventory and Scan Results	58

About the Tenable VM Integration

Forescout eyeExtend for Tenable® Vulnerability Management (VM) integrates the Forescout platform with Tenable.sc™ (formerly SecurityCenter) for Vulnerability Management On-Prem and Tenable.io® for Vulnerability Management in the Cloud so that you can:

- Trigger Tenable.sc or Tenable.io scan requests based on network activity detected by the Forescout platform. 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 [Create a Basic Tenable Scan Trigger Policy](#).
- Monitor, manage, restrict, and remediate endpoints based on scan results. See [Create a Risk Factor Results Policy](#).
- Use the Forescout Asset Inventory to see those endpoints that 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 Forescout platform policies and other basic features work.

Supported Forescout Platform Version

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

Version	Forescout Platform Version
3.0.2	Minimum version: 8.1.2
3.0.3	Minimum version: 8.1.2

Compatible Tenable Vulnerability Products

This eyeExtend module lets you integrate the Forescout platform with the following Tenable Network Security vulnerability products:

- **Tenable.sc:** A centralized management system to control and view scan data from multiple scanners deployed throughout your organization.
- **Tenable.io:** The Tenable cloud-based vulnerability management platform.

Additional Tenable Documentation

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

<https://www.tenable.com/products>

eyeExtend for Tenable VM – Concepts, Components, Considerations

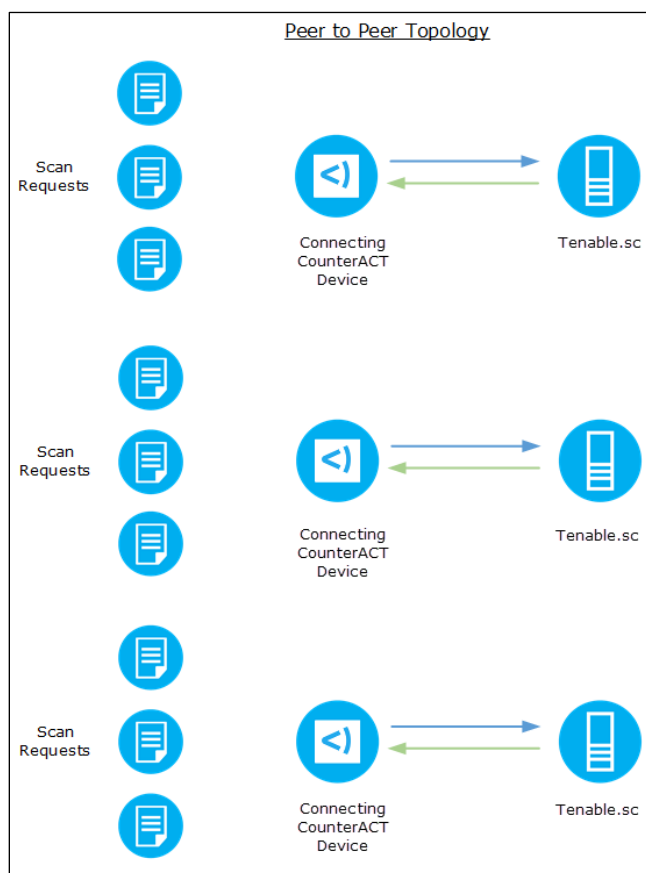
This topic provides a basic overview of the Forescout platform and Tenable VM architecture:

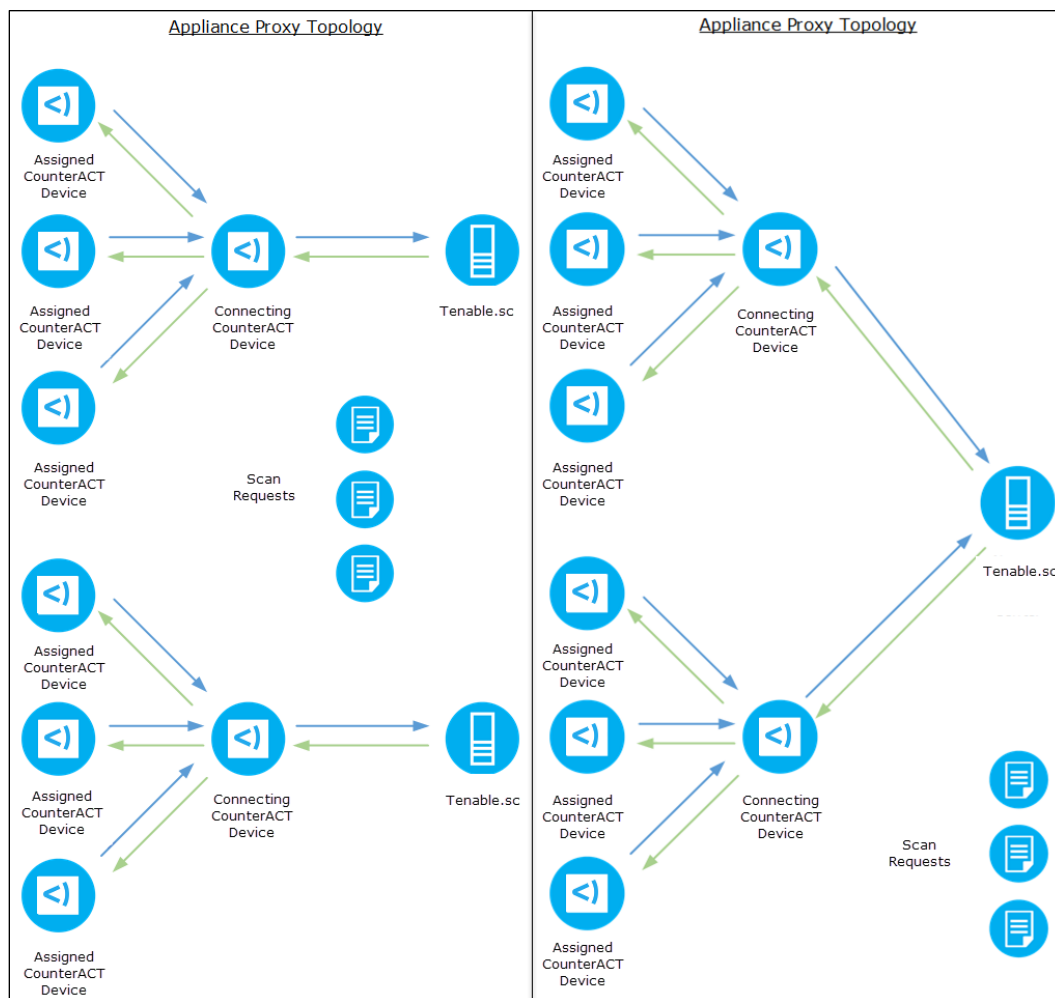
- [Concepts](#): the basic integration concepts.
- [Components](#): the devices in your network that participate in the integration.
- [Considerations](#): the setup details and common network structure issues to keep in mind when you implement this eyeExtend module.

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 Tenable.io or Tenable.sc server is connected to one or more CounterACT devices. When configuring Forescout eyeExtend for Tenable Vulnerability Management, ensure that each server can scan the entire range of IP addresses associated with its assigned CounterACT Appliances or Enterprise Manager.





Deployment Options

There are two topologies for setting up multiple CounterACT devices and multiple Tenable.io or Tenable.sc servers. A deployment can combine both topologies to meet particular network requirements.

- When Tenable.sc is configured to Allow Session Management (under System > Configuration > Security > Authentication Settings in the Tenable.sc Dashboard), you can set the maximum number of registered users that can connect to the Tenable.sc.

Peer-to-Peer: One or more CounterACT devices communicate directly with one Tenable.sc. This is a one-to-one relationship, where each CounterACT Appliance prompts the connected Tenable.sc 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 Tenable.sc or Tenable.io server 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

The key components of a typical deployment include:

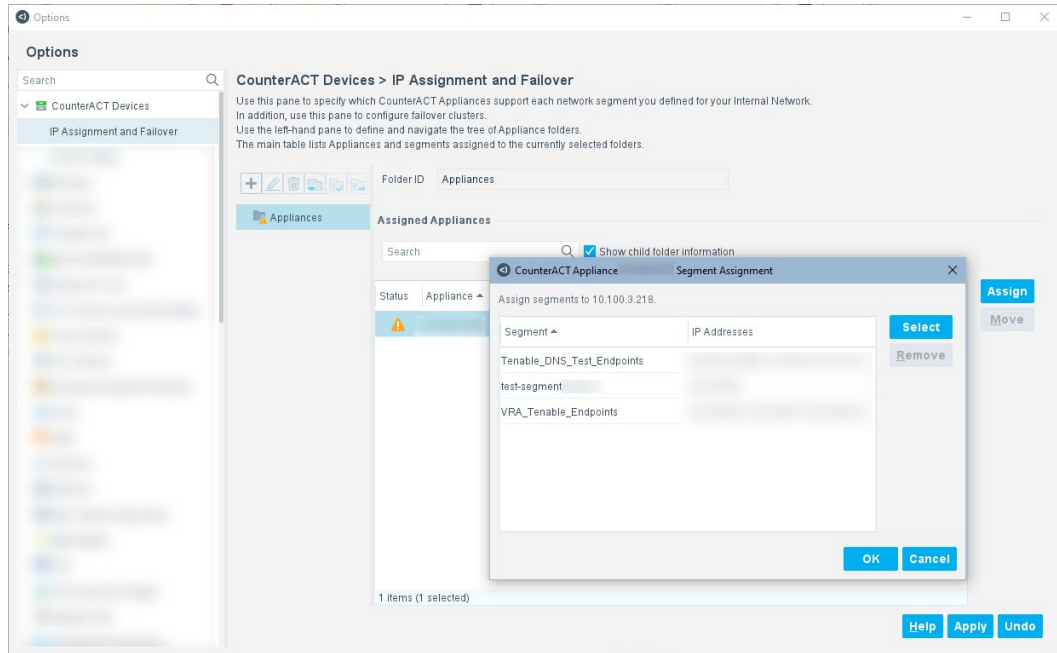
- **Connecting CounterACT Device:** This CounterACT device communicates directly with the Tenable.io or Tenable.sc server and handles queries and requests submitted by all the devices assigned to the Tenable vulnerability product. In an environment where more than one CounterACT device is assigned to 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 Tenable.sc:** 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 Tenable.sc or Tenable.io servers:

- **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:** Forescout eyeExtend for Tenable VM 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 Forescout platform policy created using the [Create a Basic Tenable Scan Trigger Policy](#) 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 Tenable.sc or Tenable.io servers handle the same IP address range as the CounterACT devices assigned to it. To see CounterACT device IP address assignments, in the Console select **Tools > Options > CounterACT Devices > IP Assignment and Failover**, then double-click the Appliance.



- **Synchronization with Scan Policies, Repositories, Zones, and Credentials:** When the Forescout platform triggers a Tenable scan, it passes information to Tenable including the specific endpoint IP to be scanned, and a scan policy name. In addition, when triggering a Tenable.sc scan, the Forescout platform 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 configuration tabs of Forescout eyeExtend for Tenable VM. The Tenable.sc 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, you must synchronize the configuration in Forescout eyeExtend for Tenable VM before triggering a scan using that information. To synchronize the configuration, in the Console select **Tools > Options > Tenable VM**, and in the Tenable Servers tab, select a Tenable server, and then select **Sync**.

Additional Considerations

The Forescout platform recognizes only those scan reports that it triggered. There is an option to recognize scans that are initiated directly by Tenable.sc and Tenable.io servers. By default, the Forescout platform uses the machine-generated name for each scan and then deletes each scan 30 days after creation.

On Tenable.io, generated names prefixed with fs_, include the policy name and a timestamp. Do not change these names on Tenable.

- *For complex deployments with multiple CounterACT devices, multiple Tenable.sc or Tenable.io servers, and diverse scan compliance policies, see [Tenable VM Policy Properties – Detect Vulnerabilities](#).*

How to Work with eyeExtend for Tenable VM

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

What to Do

Perform the following steps to set up the integration:

1. Verify that all requirements are met. See [Requirements](#).
2. Download and install the module. See [Install eyeExtend for Tenable VM Module](#).
3. Map CounterACT devices to Tenable.io or Tenable.sc servers. See [Configure eyeExtend for Tenable VM Module](#).
4. [Test eyeExtend for Tenable VM Configuration](#).
5. Run Forescout platform policies that detect and manage endpoints tracked by a Tenable.io or Tenable.sc server. See [Create Tenable VM Policies Using Templates](#).
6. [Create Custom Tenable VM Policies](#).

Requirements

Verify that the following requirements are met:

- [Forescout Requirements](#)
- [Forescout eyeExtend \(Extended Module\) Licensing Requirements](#)
- [Supported Tenable Versions](#)

Forescout Requirements

The module requires the following Forescout releases and components:

- A module license for Forescout eyeExtend for Tenable Vulnerability Management. See [Forescout eyeExtend \(Extended Module\) Licensing Requirements](#).

Forescout eyeExtend (Extended Module) Licensing Requirements

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

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

To identify your licensing mode:

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

**Per-Appliance Licensing Mode**

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

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

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

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

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

Requesting a License

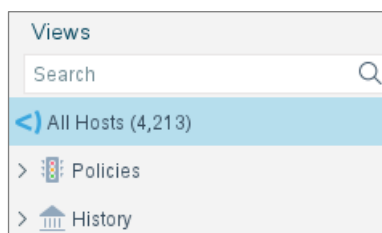
When requesting a demo license extension or permanent license, you are asked to provide the device *capacity* requirements. This is the number of devices that you want this license to handle. You must define at least the number of devices currently detected by the Forescout platform. You can request a license that handles more to ensure that you are licensed for support on additional devices as your deployment grows.

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



To view the number of currently detected devices:

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




Flexx Licensing Mode

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

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

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

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

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

More License Information

For more information on eyeExtend (Extended Module) licenses:

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

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

Supported Tenable Versions

- Forescout eyeExtend for Tenable VM supports the following Tenable Network Security product for communication: Tenable.sc versions 5.6.x, 5.9.x, 5.10.x, 5.11.x, and 5.12.0.
- For information about the vendor models (hardware/software) and versions (product/OS) that are validated for integration with this Forescout component, refer to the [Forescout Compatibility Matrix](#).

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

Install eyeExtend for Tenable VM Module


This topic describes how to download and install the module.


To install the module:

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


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

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

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

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

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

 *Some components are not automatically started following installation.*

Configure eyeExtend for Tenable VM Module

Before configuring the eyeExtend module, review the [eyeExtend for Tenable VM – Concepts, Components, Considerations](#) topic.

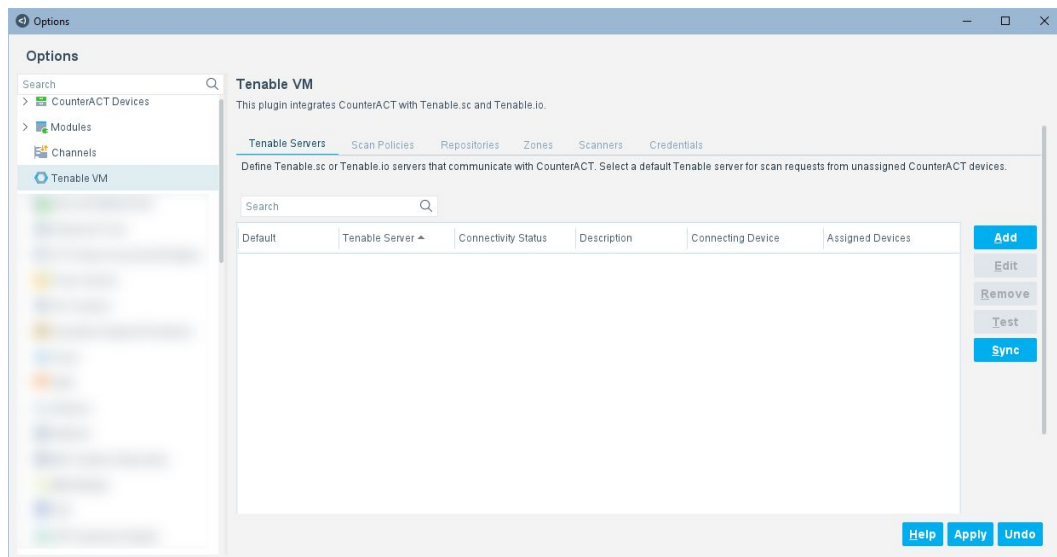
After Forescout eyeExtend for Tenable VM is installed on your targeted CounterACT Appliance, you can configure it for multiple Tenable.io and Tenable.sc servers.

To complete configuration of some of these connections, you must perform the following configuration steps on the Tenable.io instance:

- [Add Tenable Server](#)
- [Synchronize Scan Parameters and Select Defaults](#)
- [Set Auto-Deletion of Scan Results](#)
- [Test eyeExtend for Tenable VM Configuration](#)
- [Create Tenable VM Policies Using Templates](#)

To configure the module:

1. In the Console, select **Options** from the **Tools** menu. The Options dialog box opens.
2. Select the **Modules** folder.
3. In the Modules pane, select **Tenable VM**, and select **Configure**.



Add Tenable Server

Enter basic information about the Tenable.sc server or Tenable.io cloud to be added to the configuration, and select a connecting CounterACT device.

Tenable Server Authentication

Forescout eyeExtend for Tenable VM supports three types of authentication to Tenable servers:

- **Standard Login:** When configuring the eyeExtend module to communicate with a Tenable.sc or Tenable.io server using *Standard Login* authentication, enter the Tenable server username and password.
- **SSL Authentication:** When configuring the eyeExtend module to communicate with a Tenable.sc server using *SSL Authentication*, upload the client certificate and key file to the Console.
- **API Key/Secret:** When configuring the eyeExtend module to communicate with a Tenable.io server using *API Key/Secret* authentication, enter the API access key and secret key.

Using Username/Password

Note the following when using Username/Password:

- To get the token, a *GET /session* API call is made to Tenable.io, which includes the Username and Password, sent in plain-text on a secure HTTPS connection
- The Username/Password is only included in the *GET /session* API call when the token is fetched; for all other API calls, the token is used
- On the Forescout platform, the token is refreshed every 20 minutes by default
- It is recommended to keep **Validate Server Certificate** selected in the Add Tenable Server, General pane

Using API Key/Secret

Note the following when using API Key/Secret:

- All API calls that include the Access Key and Secret are sent in plain-text
- The communication is encrypted using SSL (encrypt on transport)
- The API Key/Secret is static; there is no token as with Username/Password
- It is strongly recommended to keep **Validate Server Certificate** selected in the Add Tenable Server, General pane

For API Key/Secret, refer to the following:

<https://developer.tenable.com/docs/authorization>

<https://docs.tenable.com/tenableio/vulnerabilitymanagement/Content/Settings/GenerateAPIKey.htm>

To add a Tenable server:

1. In the Console, select **Options** from the Tools menu. The Options dialog box opens.
2. Select **Tenable VM**. The Tenable VM is displayed in the right pane.
3. In the Tenable Servers tab, select **Add** to add a Tenable.sc or Tenable.io server.

Add Tenable Server

General

Define the data and login credentials of a Tenable.sc or Tenable.io server that will run scan jobs requested by CounterACT. Define the Connecting CounterACT Device that will handle all communication with this Tenable server.

Server Type: Tenable.sc

Server Name or IP Address:

Description:

Validate Server Certificate: ☒

Use DNS Name (if available): ☐

Data Format: IPv4

Authentication Type: Standard Login

User Name / API Access Key:

Password / API Secret Key:

Verify Password / API Secret Key:

SSL Certificate File: Browse ...

SSL Key File: Browse ...


Connecting CounterACT Device: Enterprise Manager

Help Previous Next Finish Cancel

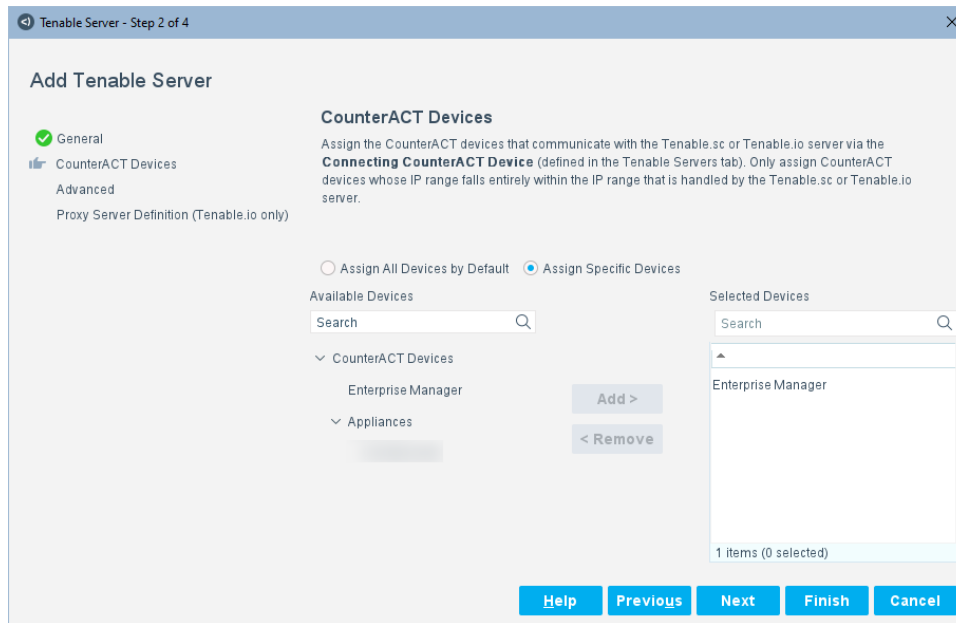
4. In the General pane, configure the following connection parameters:

Server Type	<p>Select the type of Tenable Network Security server:</p> <ul style="list-style-type: none"> ▪ Tenable.sc: All fields on this pane are active. <ul style="list-style-type: none"> - Enter Server Name or IP Address and Description. - Select optional checkboxes for Validate Server Certificate or Use DNS Name (if available). - For Data Format, select IPv4 or IPv6. - For Authentication Type, select Standard Login or SSL Authentication. - Select Connecting CounterACT Device. ▪ Tenable.io: Not all fields on this pane are active. <ul style="list-style-type: none"> - Enter Description. - Select optional checkboxes for Validate Server Certificate or Use DNS Name (if available). - For Data Format, select IPv4 or IPv6. - For Authentication Type, select Standard Login or API Key/Secret. - Select Connecting CounterACT Device.
Server Name or IP Address	<p>For Tenable.sc, enter the server name as a Fully Qualified Domain Name (FQDN) or the IPv4 or IPv6 address of the server that will execute the Forescout platform's scan requests on one or more identified endpoints.</p> <p>FQDNs are used for scanning and resolving. If an FQDN is not available for a scan, the IP address is used.</p> <p>The Tenable.sc must be able to handle the IP ranges of its assigned CounterACT devices.</p> <p>For Tenable.io, this field contains a non-editable URL.</p> <p>If the Validate Server Certificate option is selected, you must enter an FQDN in the Server Name or IP Address field.</p>
Description	(Optional) Enter a description.
Validate Server Certificate	<p>This checkbox is enabled by default.</p> <p>Select this option to validate the identity of the third-party server before establishing a connection, when the eyeExtend product module communicates as a client over SSL/TLS. To validate the server certificate, either of the following certificate(s) must be installed:</p> <ul style="list-style-type: none"> ▪ Self-signed server certificate – the server certificate must be installed on the CounterACT Appliance ▪ Certificate Authority (CA) signed server certificate – the CA certificate chain (root and intermediate CA certificates) must be installed on the CounterACT Appliance <p>Use the Certificates > Trusted Certificates pane to add the server certificate to the Trusted Certificate list. For more information about certificates, refer to the appendix, "Configuring the Certificate Interface" in the <i>Forescout Administration Guide</i>.</p>

Use DNS Name (if available)	Select this option to use a DNS name if one is available for the endpoint, otherwise, use the IP address.
Data Format	Select either IPv4 or IPv6.
Authentication Type	<p>For Tenable.sc servers, select one of the following:</p> <ul style="list-style-type: none"> ▪ Standard Login for username and password authentication. ▪ SSL Authentication for SSL certificate and key authentication. <p>For Tenable.io servers, select one of the following:</p> <ul style="list-style-type: none"> ▪ Standard Login for username and password authentication. ▪ API Key/Secret for API access key and secret key authentication.
User Name /API Access Key	<p>Enter one of the following:</p> <ul style="list-style-type: none"> ▪ For Tenable.sc or Tenable.io with Standard Login authentication, enter the User Name. For Tenable.sc, a Security Manager account in Tenable.sc is required. ▪ For Tenable.io, with API Key/Secret authentication, enter the API access key.
Password /API Secret Key	<p>Enter one of the following:</p> <ul style="list-style-type: none"> ▪ For Tenable.sc or Tenable.io with Standard Login authentication, enter the password for the User Name. ▪ For Tenable.io, with API Key/Secret authentication, enter the API secret key.
Verify Password	Re-enter the password to verify it.
SSL Certificate File	For Tenable.sc servers with SSL Authentication , select the SSL Certificate File . Enter or browse to the full path of the client certificate to be used for Tenable.sc authentication.
SSL Key File	For Tenable.sc servers with SSL Authentication , select the SSL Key File . Enter or browse to the full path of the certificate key to be used for Tenable.sc authentication.
Connecting CounterACT Device	<p>Select the CounterACT device to be assigned to the Tenable vulnerability product.</p> <p>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.</p>


 *Forescout eyeExtend for Tenable VM must be restarted after a Certificate Authority (CA) or self-signed server certificate is installed.*

5. Select **Next**.



6. In the CounterACT Devices pane, assign the CounterACT devices to work with the defined Tenable.sc or Tenable.io server, communicating via the connecting CounterACT device. Only assign CounterACT devices whose IP range falls entirely within the IP range that is handled by the Tenable.sc or Tenable.io server. Each CounterACT device can be assigned to *only* one Tenable.sc or Tenable.io server. Select one of the following options:

- **Assign All Devices by Default:** Automatically assigns all unassigned CounterACT devices to the defined Tenable.sc or Tenable.io server. When selected, it becomes the *default* Tenable vulnerability product. Only one Tenable vulnerability product is designated as the *default*.
- **Assign Specific Devices:** Assigns specific CounterACT devices to work with the defined Tenable.sc or Tenable.io server.

 *If no other Tenable Network Security servers have been added to the eyeExtend 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**.

Tenable Server - Step 3 of 4

Add Tenable Server

☒ General
☒ CounterACT Devices
☒ **Advanced**
 Proxy Server Definition (Tenable.io only)

Advanced

Configure settings to optimize the processing of scan jobs. Scan jobs are sent from CounterACT to this Tenable.sc or Tenable.io server when:

- A pre-defined interval has passed since the previous scan job was sent
- A pre-defined number of scan requests have accumulated in the job queue

Maximum number of seconds a request is in queue: 600

Number of queued requests to trigger a scan job: 100

Maximum number of scan requests per scan job: 100

Retrieve results of scans not initiated by CounterACT: ☒

[Help](#)
[Previous](#)
[Next](#)
[Finish](#)
[Cancel](#)

Endpoint scan requests can be generated by Forescout platform policies and by manual actions. A collection of endpoint scan requests is called a scan job.

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

Maximum number of seconds a request is in queue	<p>The interval, in seconds, in which Forescout eyeExtend for Tenable VM collects endpoint scan requests from assigned devices and adds them to its scan job queue. The default is 600 seconds.</p> <p>When this interval expires, Forescout eyeExtend for Tenable VM sends the collected endpoint scan requests in a scan job to the relevant Tenable vulnerability product.</p>
Number of queued requests to trigger a scan job	<p>The number of queued scan requests that triggers an expedited scan job even before the defined interval elapses. The default is 100.</p> <p>During a collection interval, host scan requests are added by Forescout eyeExtend for Tenable VM to its scan job queue. When the queue reaches the value defined for Number of queued requests to trigger a scan job, Forescout eyeExtend for Tenable VM 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.</p>
Maximum number of scan requests per scan job	<p>The maximum number of hosts that Forescout eyeExtend for Tenable VM can include in any scan job that it sends to the relevant Tenable vulnerability product. The default is 100.</p> <p>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).</p>

Retrieve results of scans not initiated by CounterACT	<p>For Tenable.io, when this option is selected, the following policy properties report results from ALL scans, not just Forescout platform-initiated scans:</p> <ul style="list-style-type: none"> ▪ Tenable Scan Results ▪ Tenable Scan Status <p>If this checkbox is selected, the first time the eyeExtend module starts, it downloads all the scans on Tenable.io. Based on the number of scans, it could take a considerable amount time for the Forescout platform to download them all. During the time the eyeExtend module is busy with the download, it will not respond to Console requests like Sync.</p> <p>This checkbox is not available for Tenable.sc.</p>
--	---

9. Select Finish.

10.(Optional) If a proxy server for Tenable.io needs to be configured, select **Next**.

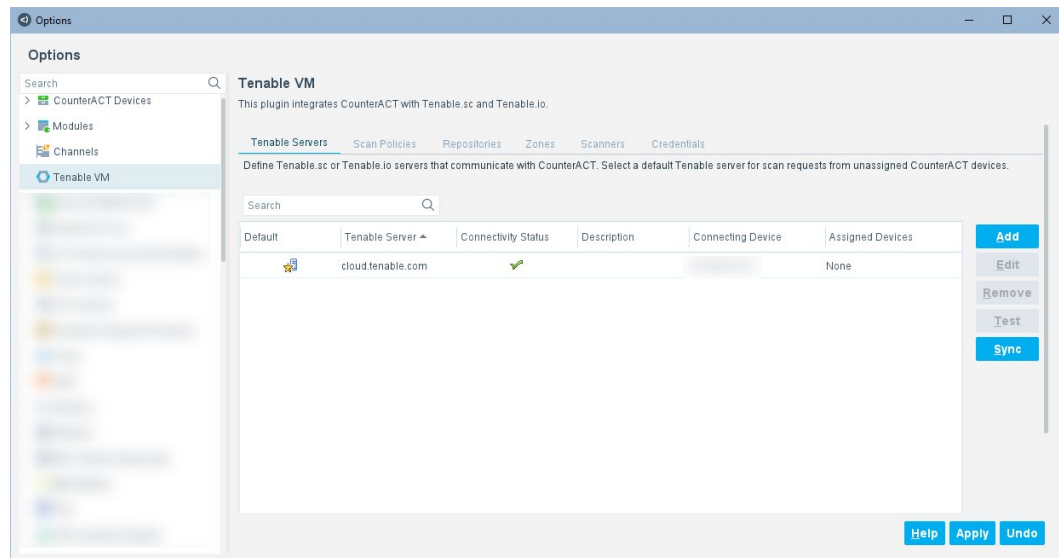
The screenshot shows a configuration window titled 'Tenable Server - Step 4 of 4'. The main heading is 'Add Tenable Server'. On the left, there are three steps: 'General' (checked), 'CounterACT Devices' (checked), and 'Advanced' (checked). Below these is a sub-heading 'Proxy Server Definition (Tenable.io only)' with a small icon. The main content area is titled 'Proxy Server Definition (Tenable.io only)' and contains a paragraph: 'If your environment routes Internet communications through proxy servers, select Use Proxy Server and specify login information for the proxy server that handles communications between Tenable.io and its connecting CounterACT device.' Below this paragraph are several input fields: 'Use Proxy Server' (checkbox), 'Proxy Server' (text box), 'Proxy Server Port' (spin box with '0' selected), 'Proxy Username' (text box), 'Proxy Password' (text box), and 'Verify Password' (text box). At the bottom right, there are five buttons: 'Help' (blue), 'Previous' (blue), 'Next' (disabled, grey), 'Finish' (blue), and 'Cancel' (blue).

11.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:

Use Proxy Server	Select this option to use a proxy server to communicate with Tenable.io.
Proxy Server	Enter the proxy server domain name as an FQDN, IPv4 or IPv6 address.
Proxy Server Port	Enter the port used to communicate with the proxy server.

Proxy Username	Enter the login name for an authorized account defined on the proxy server, if required. A management level (or higher) account is required.
Proxy Password	Enter the password for the Proxy Username .
Verify Password	Re-enter the password to verify it.

12. Select **Finish**. The server is displayed in the Tenable Servers tab.



The Connectivity Status is displayed as a green check mark for a valid connectivity or a red cross mark for an invalid connectivity.

13. In the Tenable VM pane, select **Apply**.

The best practice is to perform a test after setting up a connection. See [Test eyeExtend for Tenable VM Configuration](#).

Synchronize Scan Parameters and Select Defaults

The Forescout platform incorporates the following Tenable information into its scan requests:

- **Scan Policies:** Specifies the vulnerabilities that are tested during the scan. One scan policy name is required for each scan.
- **Repositories:** Specifies the location where the scan results are stored. One repository name is required per scan for Tenable.sc servers.
- **Zones:** The Zones tab is for Tenable.sc only and may or may not be populated, depending on how Tenable.sc is configured. Some Tenable.sc configurations require one or more zones, so performing a **Sync** will populate data for this tab, if configured. Other Tenable.sc configurations do not require multiple zones, and this tab will be empty.

- **Scanners:** The Scanners tab is populated for Tenable.io devices and lists all managed scanners.
- **Credentials:** Enables in-depth endpoint scanning by authorizing access to specific information that would otherwise be protected. You can select one or more credentials per scan for Tenable.sc servers.

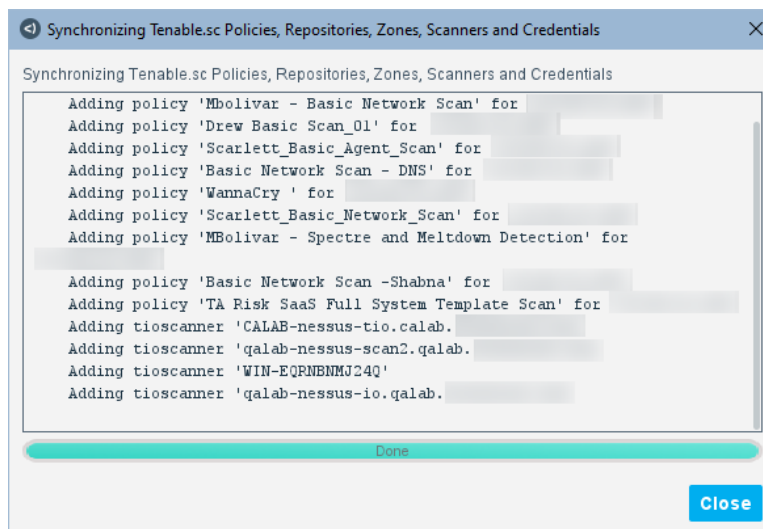
Use the Tenable Servers tab to synchronize the Forescout platform with the up-to-date list of scan parameters. Use the other tabs to view the lists of synchronized parameters.

To synchronize scan parameters and set defaults:

1. In the Console, select **Options** from the Tools menu. The Options dialog box opens.
2. In the Options pane, select **Tenable VM**. The Tenable VM pane opens.

*If **Retrieve Results of Scans not initiated by CounterACT** is selected on the Advanced pane, the first time the eyeExtend module starts, it downloads all the scans on Tenable.io. Based on the number of scans, it could take a considerable amount time for the Forescout platform to download them all. During the time the eyeExtend module is busy with the download, it will not respond to Console requests like **Sync**. The recommendation is to wait or re-try after a few minutes.*

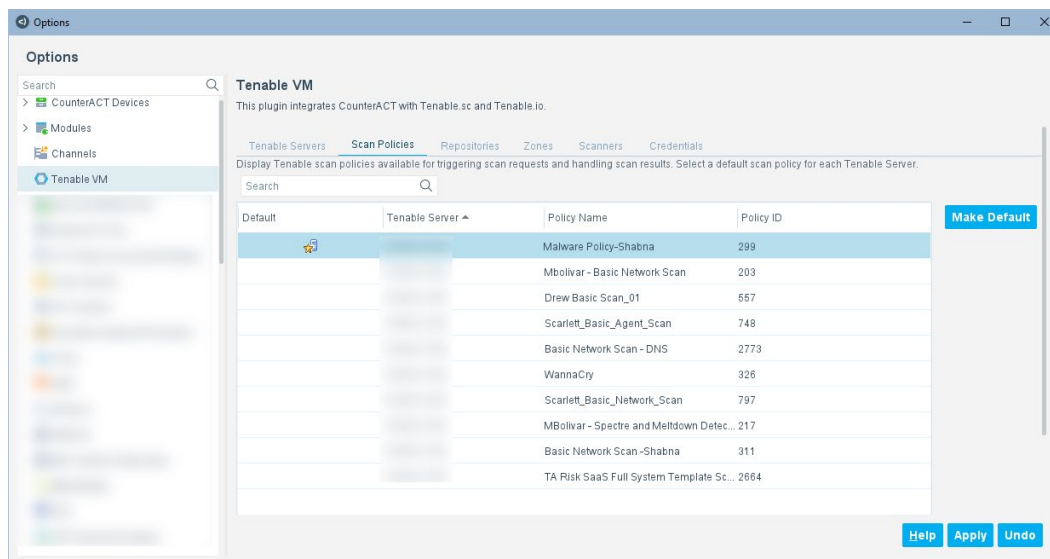
3. In the Tenable Servers tab, select a Tenable server, and then select **Sync**. The synchronization will populate the lists in the Scan Policies, Repositories, Zones, Scanners, and Credentials tabs, if configured.



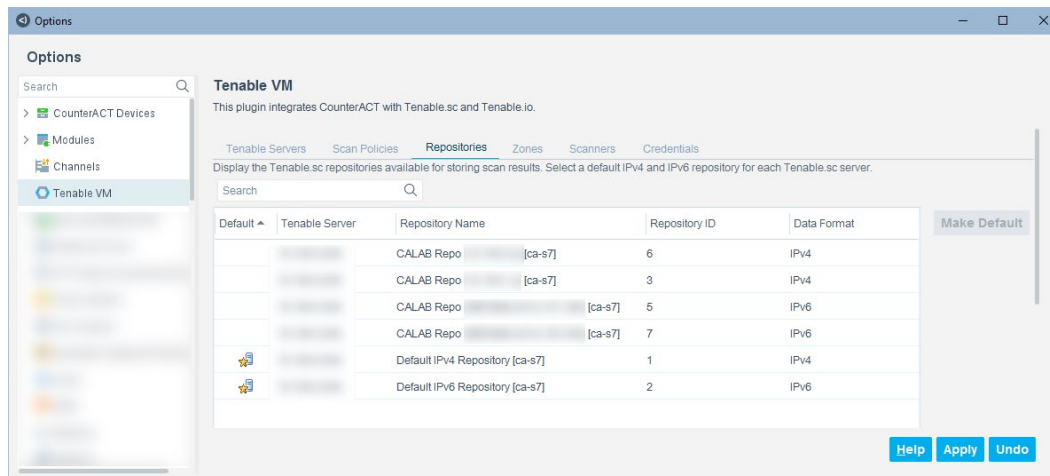
4. After the sync is Done, select **Close**.
5. Select **Apply** in the Tenable VM pane.
6. Select the Scan Policies tab, select a scan policy to be used for scans, and then select **Make Default**.

Note the following:

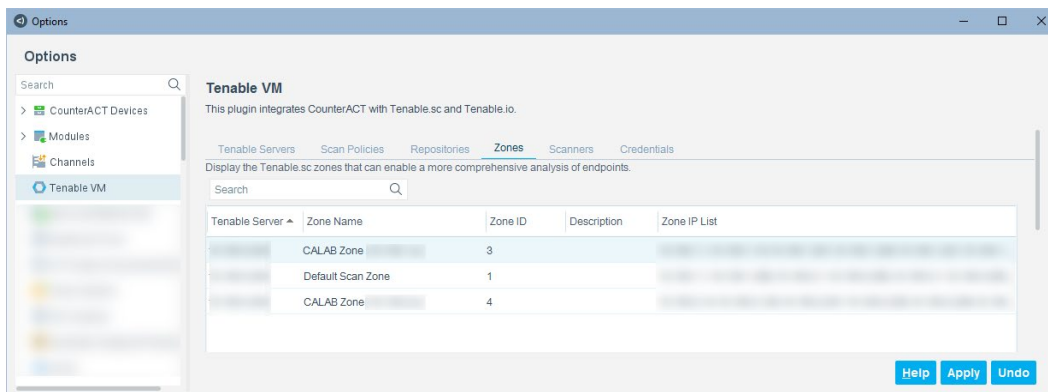
- If more than one Tenable server is defined, each one needs a default policy.
- If a scan policy contains the word *default*, it will become the initial default.



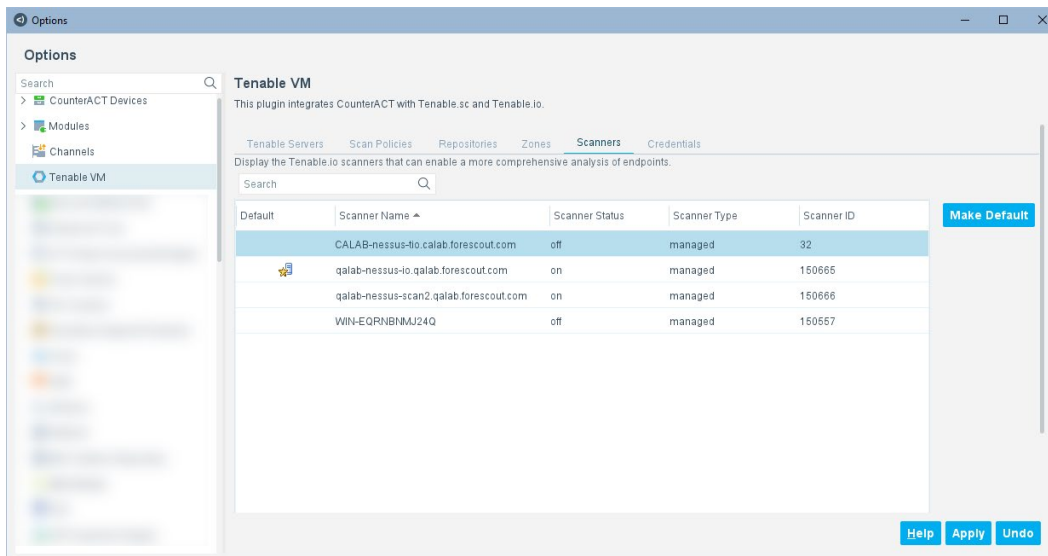
7. For Tenable.sc, select the Repositories tab to display the repositories. To make a default, select a repository, and then select **Make Default**. Both IPv4 and IPv6 are supported and there can be a default for both. If a repository contains the word *default*, it will become the initial default.



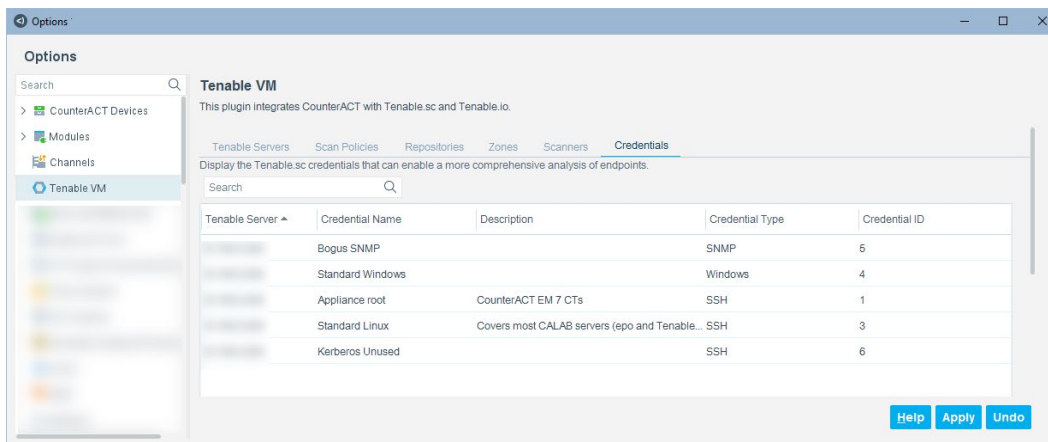
8. For Tenable.sc, select the Zones tab to display the zones.




9. For Tenable.io, select the Scanners tab to display the scanners. To make a default, select a scanner, and then select **Make Default**.



10. For Tenable.sc, select the Credentials tab to display the credentials.



11. Select **Apply.**

 *If a scan policy, repository, zone, scanner, or credential is added, removed, or renamed in the Tenable server, you must re-synchronize the scan parameters. Tenable-related property resolution and actions are not handled in the Forescout platform if the scan parameter names do not match.*

12. 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, Forescout platform-initiated scans are automatically 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** Forescout eyeExtend for Tenable VM using one of the following methods:**

- Start the module from **Tools > Options > Modules**
- Log onto the focal appliance and use the fstool command: `fstool nessus restart`

Edit Tenable Server

You can edit a Tenable server.

To edit a Tenable server:

- 1.** In the Options pane, select **Tenable VM**. The Tenable VM pane opens to the Tenable Servers tab.

2. Select an existing Tenable server and select **Edit**.

Edit Tenable Server

General CounterACT Devices Advanced Proxy Server Definition (Tenable.io only) Test Parameters

General

Define the data and login credentials of a Tenable.sc or Tenable.io server that will run scan jobs requested by CounterACT. Define the Connecting CounterACT Device that will handle all communication with this Tenable server.

Server Type: Tenable.io

Server Name or IP Address: cloud.tenable.com

Description:

Validate Server Certificate: ☐

Use DNS Name (if available): ☐

Data Format: IPv4

Authentication Type: Standard Login

User Name / API Access Key:

Password / API Secret Key: *****

Verify Password / API Secret Key: *****

SSL Certificate File: Browse ...

SSL Key File: Browse ...

Connecting CounterACT Device: Enterprise Manager

Help OK Cancel

3. Edit the parameters in the General, CounterACT Devices, Advanced, Proxy Server Definition (Tenable.io only), and Test Parameters tabs.
4. Select **OK**.
5. In the **Tenable VM** pane, select **Apply**.

Test eyeExtend for Tenable VM Configuration


After you configure Forescout eyeExtend for Tenable VM, it is recommended that you:

- [Define Test Configuration Parameters](#)
- [Run a Module Test](#)

- [Export the Test Results](#)

Define Test Configuration Parameters

Define the test configuration parameters to use when testing the configuration. Setting these parameters does not trigger a test.

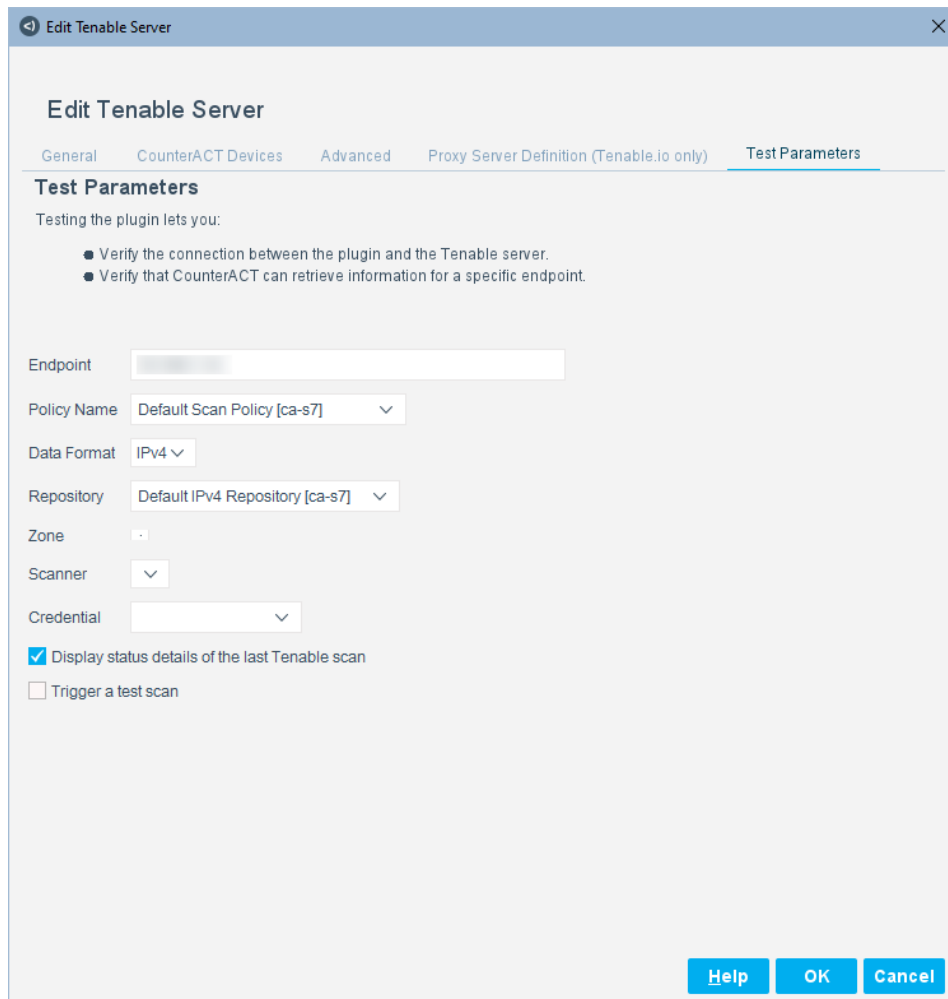
 To run the test, see [Run a Module Test](#).

Use the test to:

- Test the connection between Forescout eyeExtend for Tenable VM and Tenable.io or Tenable.sc.
- Verify that the Forescout platform can retrieve information for a specific endpoint.
- Trigger a scan request.

To set test parameters:

1. In the Tenable Servers tab, select the server to be tested, and select **Edit**.
2. Select the Test Parameters tab.



Edit Tenable Server

General CounterACT Devices Advanced Proxy Server Definition (Tenable.io only) **Test Parameters**

Test Parameters

Testing the plugin lets you:

- Verify the connection between the plugin and the Tenable server.
- Verify that CounterACT can retrieve information for a specific endpoint.

Endpoint

Policy Name

Data Format

Repository

Zone

Scanner

Credential

☒ Display status details of the last Tenable scan

☐ Trigger a test scan

Help OK Cancel

3. Configure the following fields to be used when the test is run:

Endpoint	<p>Enter the endpoint on which to carry out the test as an FQDN, IPv4 or IPv6 address.</p> <p>FQDNs are used for scanning and resolving. If an FQDN is not available for a scan, the IP address is used.</p> <p>Note the following:</p> <ul style="list-style-type: none"> ▪ If Display status details of the last Tenable 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 selected, the endpoint will be started. The Trigger a test scan will fail if the endpoint does not match the data format, for example, if the endpoint is IPv4 and the data format is IPv6.
Policy Name	Select the Tenable scan policy for which the requested scan test is to be carried out.
Data Format	Select either IPv4 or IPv6.
Repository	Select a repository to which to save the Tenable.sc scan.
Zone	(Optional) If this drop-down menu is populated, select a zone. (It is not an error if this menu is empty.)
Scanner	(Optional) If this is a Tenable.io scan, select a scanner. If a Tenable.io server is configured, the Scanner menu will have a default.
Credential	(Optional) Select a credential for the scan test on the selected endpoint.
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.

4. Select **OK**. The scan test parameters are saved.

5. In the Tenable VM pane, select **Apply**.

Run a Module Test

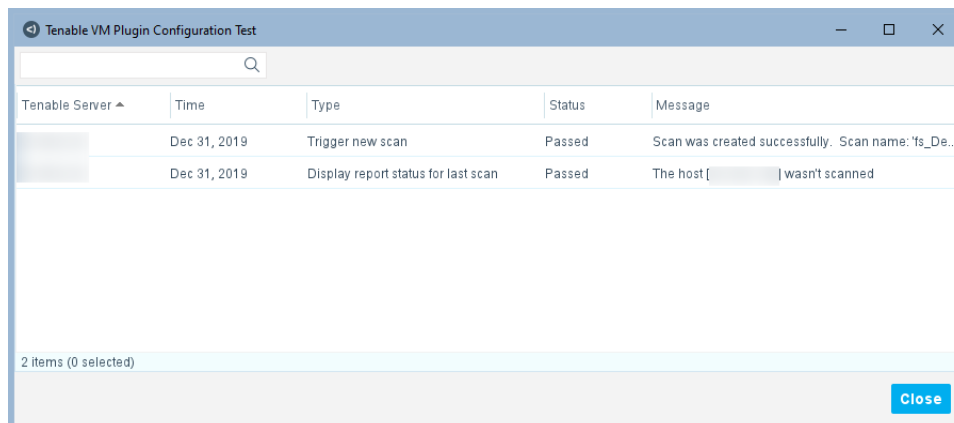
Run the configuration test to test the following:

- The connection of Forescout eyeExtend for Tenable VM to the Tenable server
- The ability of the Forescout platform to retrieve scan results
- That the scan policy name, repository, and credentials selected in the Test Parameters tab of the configuration are synchronized with the Tenable server

To run a 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 **Tenable.io** or **Tenable.sc** to be tested. You can select more than one Tenable.sc or Tenable.io server.

3. Select **Test**. The test is run.



4. Select **Close**.

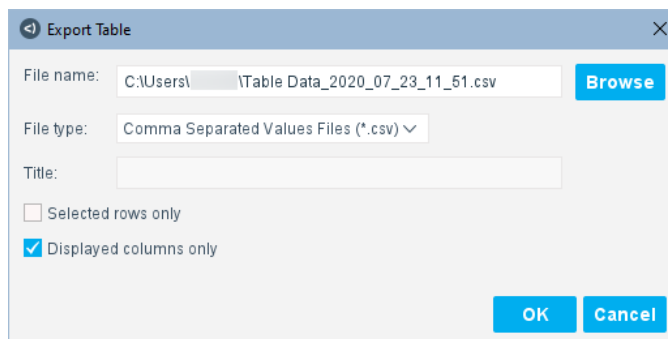
Export the Test Results

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)

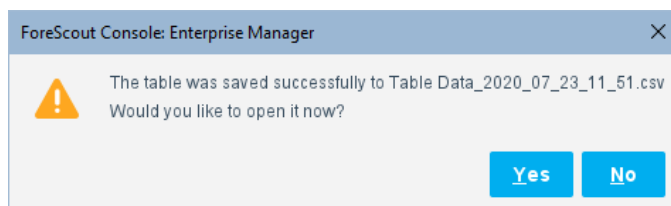
To export the report:

1. Right-click on a configured server and select **Export Table**.



- To change the path for the information to be exported, select **Browse**, select a new path, and then select **Open**.
- To change the File type, select a format. For .pdf files, you can also add a Title.
- Select options for **Selected rows only** or **Displayed columns only**.

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



3. Select **Yes** to open the file.

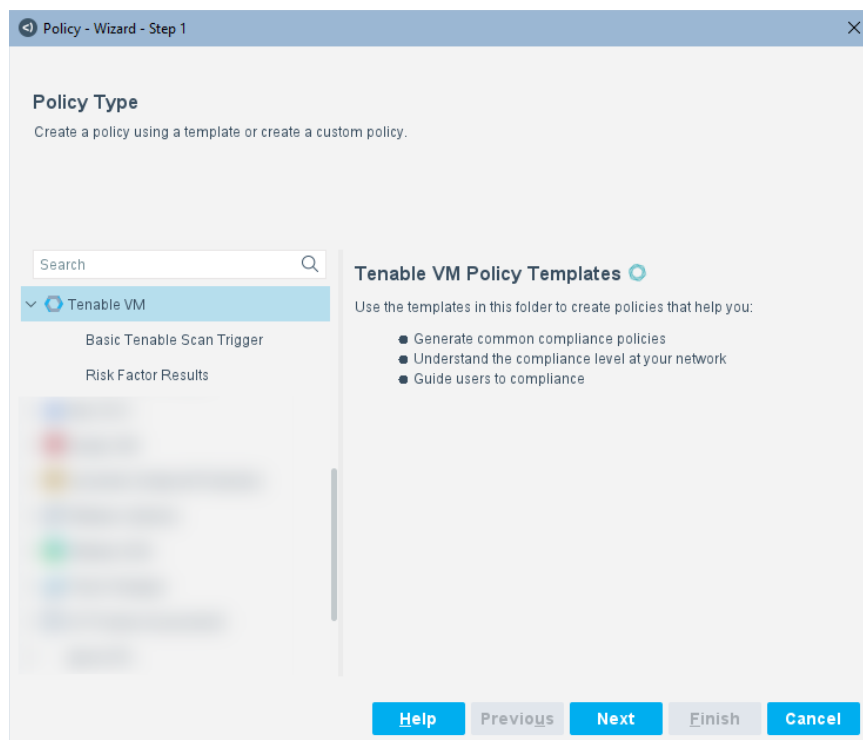
Create Tenable VM Policies Using Templates

Forescout platform 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.

You can use Tenable templates to create policies to detect, manage, and remediate devices. See the following topics:

- [ForeScout Platform Policy Coordination Considerations](#)
- [Create a Basic Tenable Scan Trigger Policy](#)
- [Create a Risk Factor Results Policy](#)



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

Working with Tenable VM templates requires you to incorporate Tenable information. See [Synchronize Scan Parameters and Select Defaults](#) for details.

Forescout Platform Policy Coordination Considerations

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

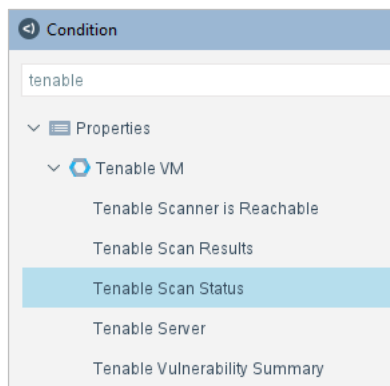
- In large-scale deployments, with multiple scanners and Appliances, the host and Tenable.sc or Tenable.io server are connected via the CounterACT Appliance. The CounterACT Appliance determines the endpoints that connect with it, and to which server the scan requests are sent. This is configured in the configuration settings of Forescout eyeExtend for Tenable VM. This means that the Tenable Server IP may differ between endpoints. Therefore, it is important to add the Tenable Server IP property to any Forescout platform policy condition that checks the scanner status.
- The Forescout platform 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 the Forescout platform 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. Forescout platform 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 Forescout operator to ensure that the necessary changes are made.
- A Forescout platform 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 the *Scan Policy Name* to which this condition applies. For example, assume you have defined the Tenable scan policies N1 & N2 and that the Forescout platform triggers scans using these policies at T1 & T2 respectively.

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)

To define a condition to rescan the host:

1. In the Condition dialog box, select the Tenable Scan Status property.



2. In the **Tenable Scan Status** section, select *For all property values*.
3. In the **Scan Policy Name** section, set the parameters to:

Tenable Scan Status: Indicates the scan status details on an endpoint for specific scan policies or for all policies if none are selected.

For all property values

☒ **Scan Policy Name**
Enter a value to match the scan policy name.

☒ Meets the following criteria
☐ Does not meet the following criteria

Matches Scan_Production

☐ Match case

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

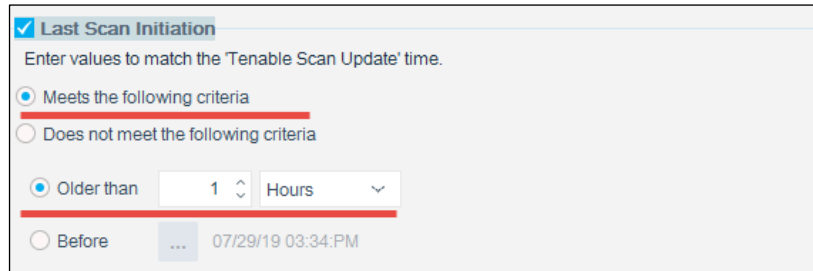
☒ **Scan Status**
Enter values to match the Tenable scan status.

☒ Meets the following criteria
☐ Does not meet the following criteria

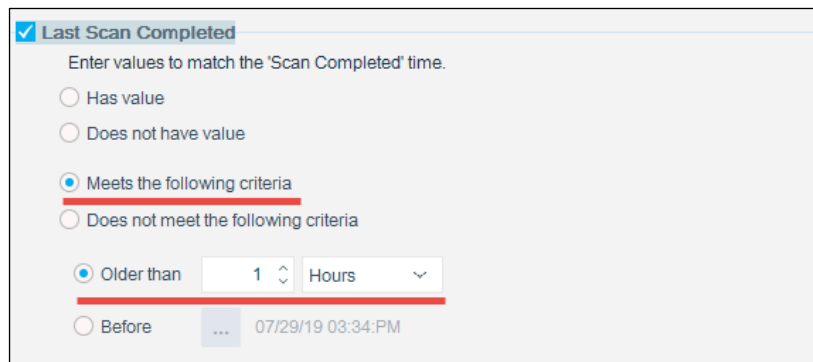
Search

<input checked="" type="checkbox"/> Name ▲	<input type="button" value="Select All"/> <input type="button" value="Clear All"/>
<input checked="" type="checkbox"/> Completed	
<input type="checkbox"/> In Progress	

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



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



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

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

Create a Basic Tenable Scan Trigger Policy

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

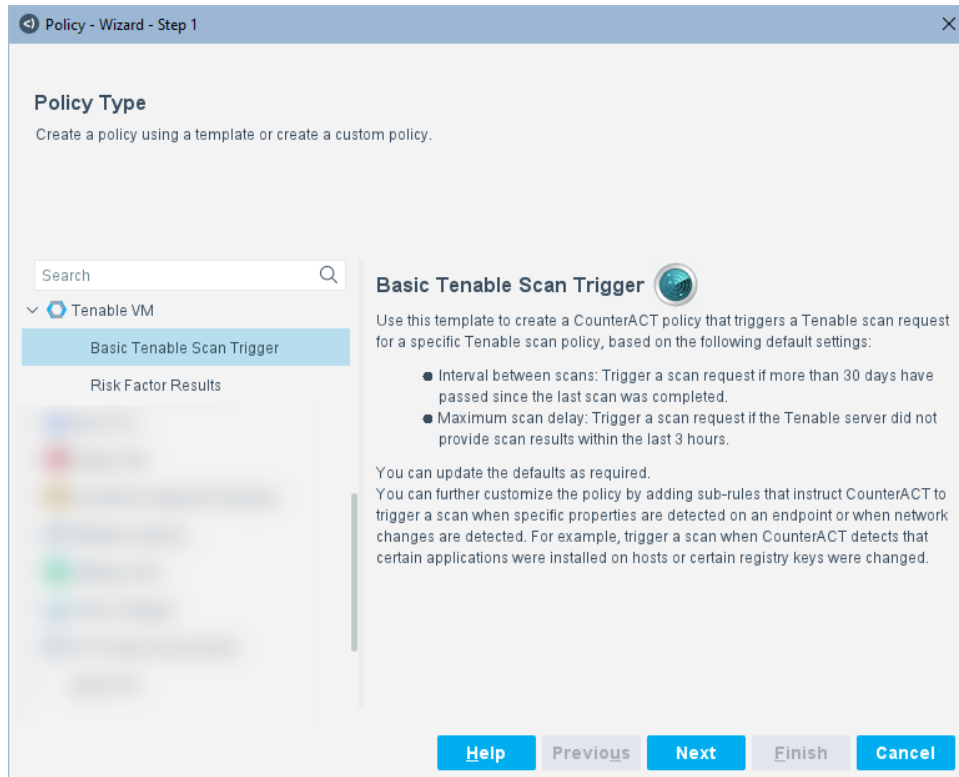
- Interval between scans: Trigger a scan request if more than 30 days have passed since the last scan was completed.
- Maximum scan delay: Trigger a scan request if the Tenable.sc or Tenable.io server did not provide scan results within the last 3 hours.

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

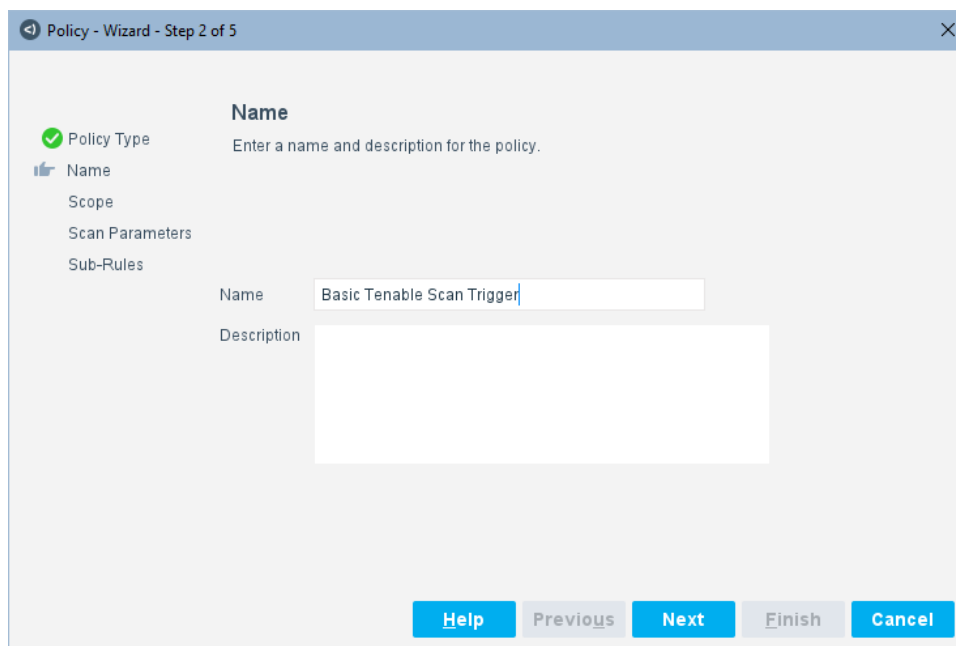
This policy template provides basic triggering capacity. You can update the defaults as required and further customize the Forescout platform policy by adding sub-rules that instruct the Forescout platform to only trigger a scan when an endpoint is detected with specific properties. For example, you can instruct the Forescout platform 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 Forescout platform policies to carry out these changes.

To create a policy:

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



4. Select **Next**.



Policy - Wizard - Step 2 of 5

☒ Policy Type

☐ Name

Scope

Scan Parameters

Sub-Rules

Name: Basic Tenable Scan Trigger

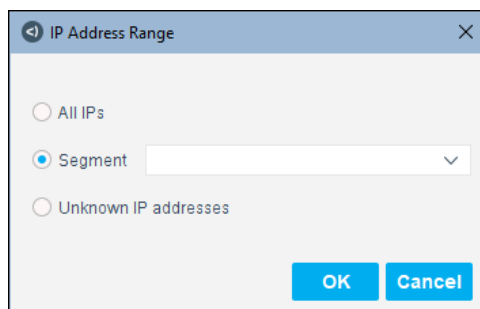
Description:

Help Previous Next Finish Cancel

5. Enter a name and optionally add a description.

6. Select **Next**. Both the IP Address Range dialog box and the Scope pane open.

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



IP Address Range

☐ All IPs

☒ Segment

☐ Unknown IP addresses

OK Cancel

The following options are available:

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

8. Select **OK**. The added range is displayed in the Scope pane. You can add multiple rows to the scope list by selecting **Add** and repeating the previous step.

Policy - Wizard - Step 3 of 5

Scope
Define the range of Hosts to be inspected for this policy.

Policy Type
Name
Scope
Scan Parameters
Sub-Rules

Hosts inspected by the policy

Segment	IP Addresses
No Name Assigned	All IPv4, All IPv6

Add
Remove
Segments

Help Previous Next Finish Cancel

9. Select **Next**.

Policy - Wizard - Step 4 of 5

Scan Parameters
Select the scan parameters you want to use for the scan. You must define a Tenable server and sync with it before you can create this policy.

Policy Type
Name
Scope
Scan Parameters
Sub-Rules

Policy Name: Default

Data Format: ☒ IPv4 ☐ IPv6

Repository: Default IPv4

Zones:

Scanners: Default

Credentials:

Help Previous Next Finish Cancel

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

- **Policy Name:** Specifies the vulnerabilities that are tested during the scan. One scan policy name is required for each scan.
- **Data Format:** Specifies the data format. Select either IPv4 or IPv6. If you select a **Data Format** of **IPv4**, the **Repository** list is populated with IPv4 repositories. If you select a **Data Format** of **IPv6**, the **Repository** list is populated with IPv6 repositories.
- **Repository:** Specifies the location where the scan results are stored. One repository name is required per scan for Tenable.sc servers.
- **Zones:** (Optional) Specify the scan zone to use in some cases. (This menu can be empty.)
- **Scanners:** (Optional) Select the scanners to use for Tenable.io. (Not applicable to Tenable.sc.)
- **Credentials:** (Optional) Enables in-depth endpoint scanning by authorizing access to specific information that would otherwise be protected. You can select one or more credentials per scan for Tenable.sc servers. To select multiple credentials, hold down the Ctrl key or the Shift key.

11.Select **Next**.

Sub-Rules

Use this screen to review policy sub-rule definitions.
Hosts are inspected by each sub-rule in the order shown. When a match is found, the action defined is applied. If no match is found, the host is inspected against the next sub-rule.

	Name	Conditions	Exceptions	Actions
1	Verify scanner is reachable	NOT Tenable Scanner is Reachable:		
2	Verify time since host last scan	Tenable Scan Status: Last Scan Completed NOT: Older than 30 days, Scan Status: Completed		
3	Assert scan status	Tenable Scan Status: Last Scan Initiation NOT: Older than 3 hours, Scan Status: In Progress		
4	Request a host scan	No Conditions		

Buttons: Add, Edit, Remove, Duplicate, Up, Down

Navigation: Help, Previous, Next, Finish, Cancel

The Sub-Rules instruct the Forescout platform how to detect and handle endpoints. They also define how often the connectivity to the scanner 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.

Double-click on a Sub-Rule to view or change the condition or action. See [Tenable VM Policy Properties – Detect Vulnerabilities](#).

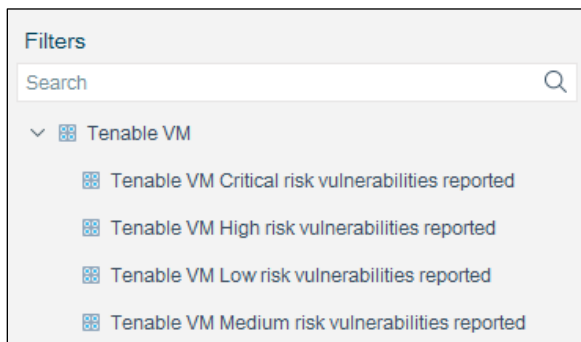
12.Select **Finish**.

Create a Risk Factor Results Policy

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

Risk factor results are based on all Tenable scan policies synchronized with Forescout eyeExtend for Tenable VM. See [Synchronize Scan Parameters and Select Defaults](#) for details.

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



You can later use these groups in Forescout platform 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 Forescout administrator that vulnerabilities were detected
- Send a Syslog message indicating that vulnerabilities were detected

These actions are disabled by default.

To create a policy:

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

Policy - Wizard - Step 1

Policy Type
Create a policy using a template or create a custom policy.

Search

▼ Tenable VM

- Basic Tenable Scan Trigger
- Risk Factor Results**

Risk Factor Results

Use this template to create a CounterACT policy that detects the most current Tenable Risk Factor results assigned to network hosts. The policy organizes hosts into CounterACT groups with Critical, High, Medium, Low or no risk factors. You can later use these groups in CounterACT policies to control hosts. For example, you can assign hosts having Critical risks to an isolated VLAN. Additional information about hosts is also provided, such as the scan policy name, port scanned and protocol.

Optional remediation actions 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.

Help **Previous** **Next** **Finish** **Cancel**

4. Select **Next**.

Policy - Wizard - Step 2 of 4

Name
Enter a name and description for the policy.

✔ Policy Type

▢ Name

▢ Scope

▢ Sub-Rules

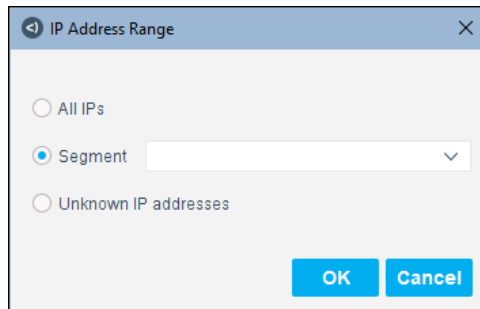
Name: Risk Factor Results

Description:

Help **Previous** **Next** **Finish** **Cancel**

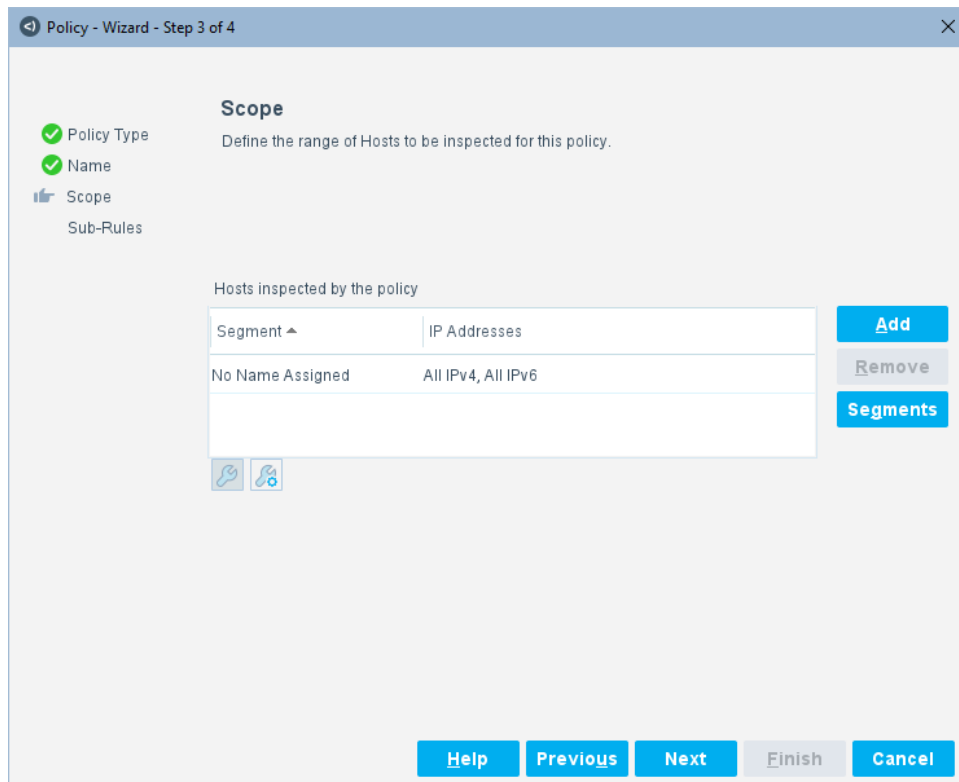
5. Enter a name and optionally add a description.

6. Select **Next**. Both the IP Address Range dialog box and the Scope pane 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 pane.
 - **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 is displayed in the Scope pane. You can add multiple rows to the scope list by selecting **Add** and repeating the previous step.



9. Select **Next**.

Policy - Wizard - Step 4 of 4

✓ Policy Type
✓ Name
✓ Scope
✗ Sub-Rules

Sub-Rules

Use this screen to review policy sub-rule definitions.
Hosts are inspected by each sub-rule in the order shown. When a match is found, the action defined is applied. If no match is found, the host is inspected against the next sub-rule.

	Name	Conditions	Exceptions	Actions
1	Retry if scanner is not responsive	Tenable Scan Results: Repository Name NOT: Any Value		
2	Critical risk vulnerabilities reported	Tenable Scan Results: Risk Factor: Critical, CVE: Any Value		
3	High risk vulnerabilities reported	Tenable Scan Results: Risk Factor: High, CVE: Any Value		
4	Medium risk vulnerabilities reported	Tenable Scan Results: Risk Factor: Medium, CVE: Any Value		
5	Low risk vulnerabilities reported	Tenable Scan Results: Risk Factor: Low, CVE: Any Value		
6	No vulnerabilities reported	Tenable Scan Results: Risk Factor: None, CVE: Any Value		

[Add](#)
[Edit](#)
[Remove](#)
[Duplicate](#)
[Up](#)
[Down](#)

[Help](#) [Previous](#) [Next](#) [Finish](#) [Cancel](#)

The Sub-Rules instruct the Forescout platform how to detect and handle endpoints. They also define how often the connectivity to the scanner 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 [Tenable VM Policy Properties – Detect Vulnerabilities](#).

10. Select **Finish**.

Create Custom Tenable VM Policies

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

For more information, see [Forescout Platform Policy Coordination Considerations](#).

To create a custom policy:

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

3. Select **Custom**.

Policy - Wizard - Step 1

Policy Type
Create a policy using a template or create a custom policy.

Search

Custom

The custom policy wizard allows you to define policies for which no template exists.

When defining a policy, you need to consider the following:

- What hosts are subject to the policy
- What conditions should be tested against these hosts
- What actions should be applied if the conditions are met

As an example, consider a simple policy requiring all corporate Windows machines to run an antivirus. In this case, the condition would be

OS is Windows AND Machine is Managed AND NOT Antivirus is running

The actions associated with hosts matching this condition can be "HTTP Notifications" and "Send email to the Help desk".

Sometimes the policy is more complex, and divides the network into multiple categories, each requiring a different set of actions. You can use a compound policy combining multiple sub-rules to cope with such cases.

Custom

Help Previous Next Finish Cancel

4. Select **Next**.

Policy - Wizard - Step 2 of 5

Name
Enter a name and description for the policy.

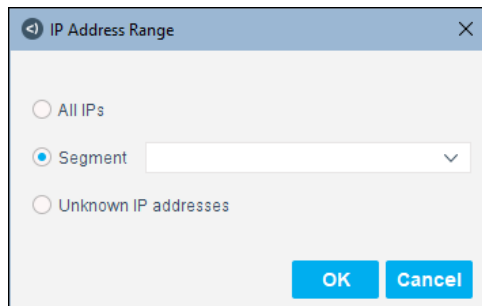
Policy Type
Name
Scope
Main Rule
Sub-Rules

Name

Description

Help Previous Next Finish Cancel

5. Enter a name and optionally add a description.
6. Select **Next**. Both the IP Address Range dialog box and the Scope pane 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 pane.
- **Unknown IP addresses**: Apply the policy to endpoints whose IP addresses are not known. Endpoint detection is based on the endpoint MAC address.

By default, the template excludes network printers from the scope.

8. Select **OK**. The new host address is displayed in the Scope pane. You can add multiple rows to the scope list by selecting **Add** and repeating the previous step.

Policy - Wizard - Step 3 of 5

Scope
Define the range of Hosts to be inspected for this policy.

✓ Policy Type
✓ Name
☷ Scope
Main Rule
Sub-Rules

Hosts inspected by the policy

Segment ▲	IP Addresses
No Name Assigned	All IPv4, All IPv6

Add
Remove
Segments

Help **Previous** **Next** **Finish** **Cancel**

9. (Optional) Select the wrench icon. The Advanced fields are displayed. It is recommended to select **Add** from the Filter by Group section to include only Windows, Linux/Unix and Macintosh machines.



Policy - Wizard - Step 3 of 5

Scope
Define the range of Hosts to be inspected for this policy.

Policy Type
Name
Scope
Main Rule
Sub-Rules

Hosts inspected by the policy

Segment ▲	IP Addresses	
No Name Assigned	All IPv4, All IPv6	Add Remove Segments

Filter by Group - Only inspect hosts from the following groups

Group	Description	
No Group Filter applied		Add Remove

Exceptions - Do not inspect the following

Type	Values	
No items to display		Add Edit Remove

Help **Previous** **Next** **Finish** **Cancel**

10. Select **Next**.

Policy - Wizard - Step 4 of 5

✓ Policy Type
✓ Name
✓ Scope
Main Rule
Sub-Rules

Main Rule
Define a condition and actions

The condition defines a set of tests to be checked against the hosts.
Actions are applied to hosts matching the condition.
Only hosts matching the main rule condition are subject to further inspection by sub-rules.

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

All criteria are True

Criteria

No items to display

Add Edit Remove

Actions
Actions are applied to hosts matching the above condition.

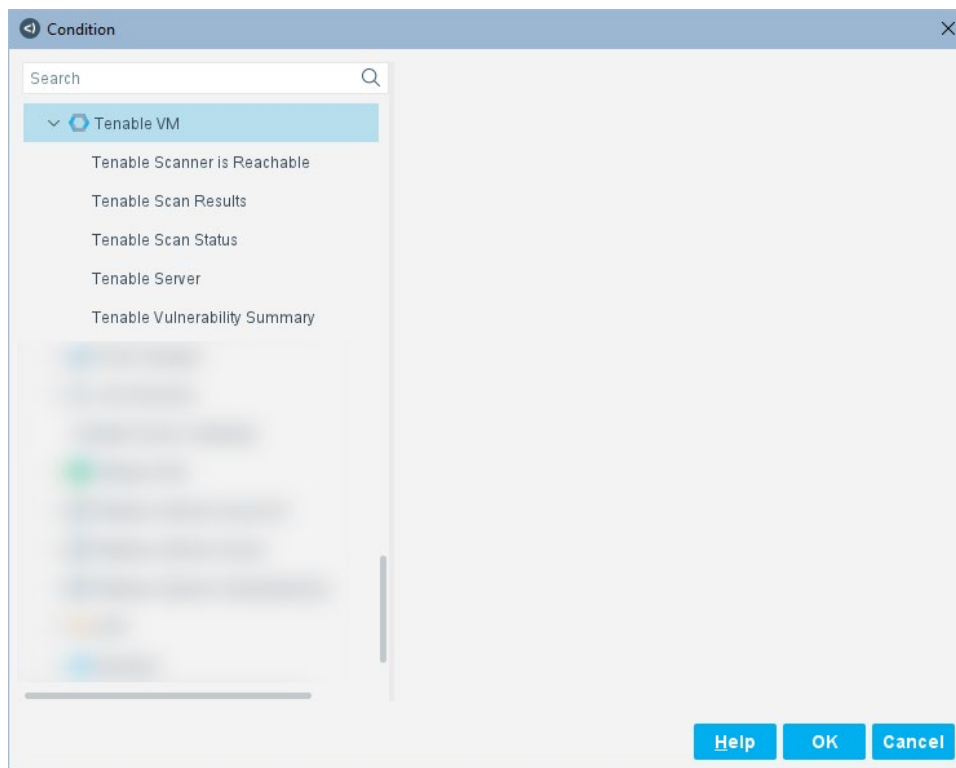
Enable	Action	Details
No items to display		

Add Edit Remove

Help Previous Next Finish Cancel


Policy rules instruct the Forescout platform 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.

- 11.** In the Condition section of the Main Rule pane, select **Add** and then expand the **Tenable VM** folder in the Properties Tree.



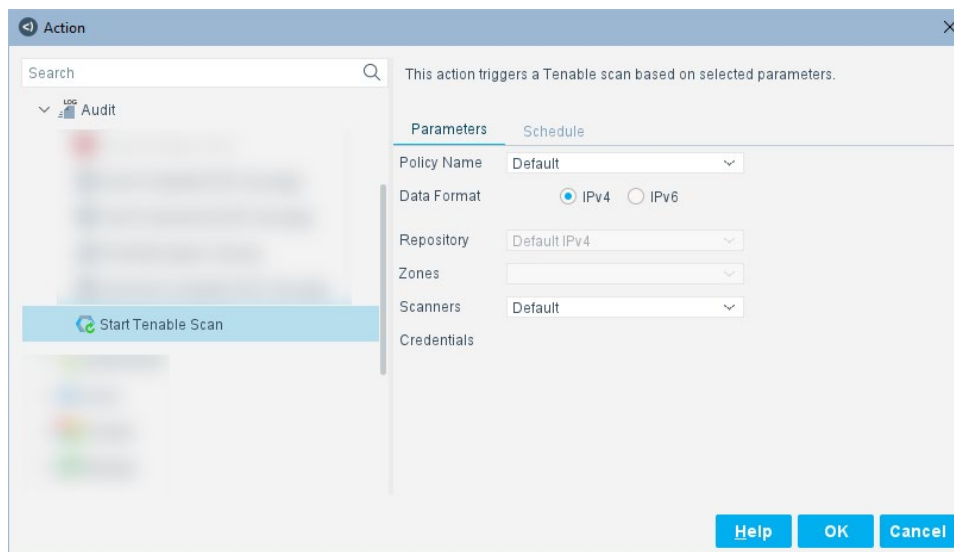
- 12.** Add conditions based on the expected behavior of the custom policy. For details, see:

- [Tenable Scanner is Reachable](#)
- [Tenable Scan Results](#)
- [Tenable Scan Status](#)
- [Tenable Server](#)
- [Tenable Vulnerability Summary](#)

 *For each property, you can set the evaluation of irresolvable criteria as True/False.*

- 13.** Configure the properties, and then select **OK** to close the Condition dialog box.

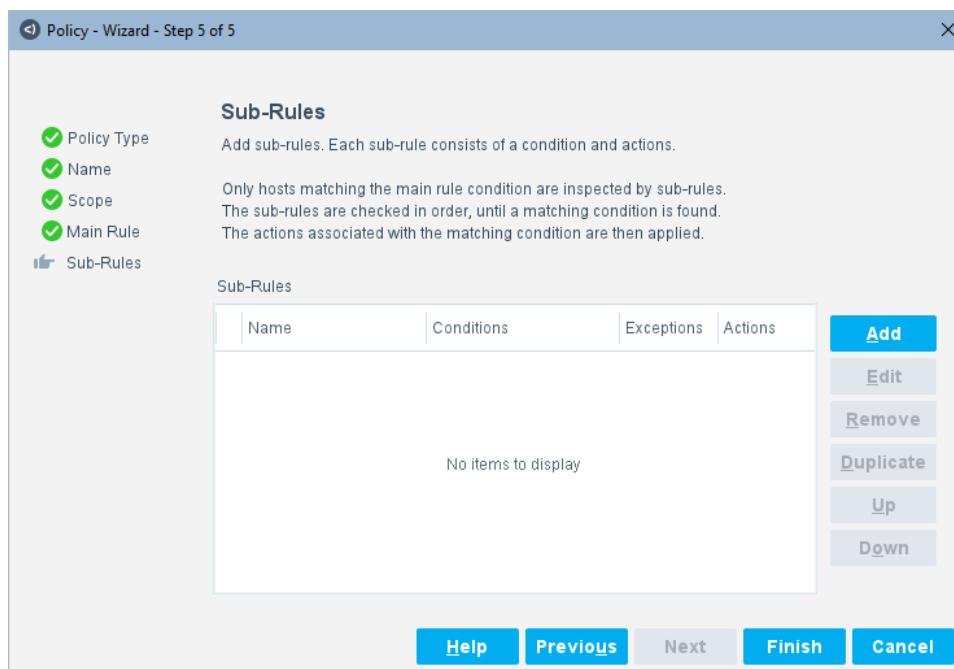
- 14.** In the Actions section of the Main Rule pane, select **Add** and then expand the Audit folder in the Actions tree.



- 15.** Select **Start Tenable Scan**.

- 16.** Add actions based on the expected behavior of the custom policy, then select **OK** to close the Action dialog box.

- 17.** Select **Next**.



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.

18. Define sub-rules, which are additional condition/action pairs. For definitions, see [Tenable VM Policy Properties – Detect Vulnerabilities](#).

19. Select **Finish**.

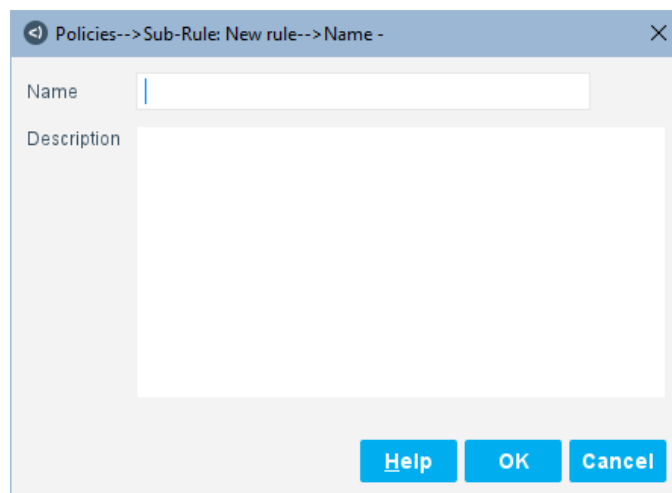
Tenable VM Policy Properties – Detect Vulnerabilities

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

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

To access Tenable VM properties:

1. In the Sub-Rules pane of the Policy Wizard, select **Add**.



2. Enter a name and description of the sub-rule.

3. Select OK.

Policies-->Sub-Rule: New rule -

Name

Tenable Advanced

Edit

Description

None.

Condition

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

All criteria are True

Criteria

No items to display

Add

Edit

Remove

Actions

Actions are applied to hosts matching the above condition.

Enable	Action	Details
No items to display		

Add

Edit

Remove

Advanced

Recheck match

Every 8 hours, All admissions

Edit

Exceptions

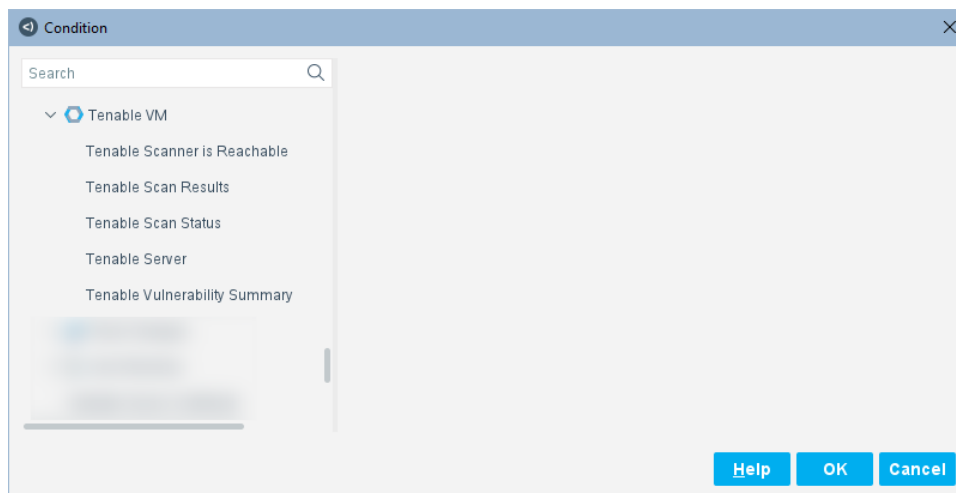
None.

Help

OK


Cancel

4. In the Condition section of the Sub-Rule pane, select **Add** and then expand the **Tenable VM** folder in the Properties Tree.



5. Add conditions based on the expected behavior of the policy. For details, see:

- [Tenable Scanner is Reachable](#)
- [Tenable Scan Results](#)
- [Tenable Scan Status](#)
- [Tenable Server](#)
- [Tenable Vulnerability Summary](#)

 *For each property, you can set the evaluation of irrisolvable criteria as True/False.*

6. Configure the rule conditions, and then select **OK** in the Conditions dialog box. Your new criteria is displayed in the Sub-Rules pane.
7. To configure the rule actions, go to [Tenable VM Policy Actions – Scan Endpoints](#).

Tenable Scanner is Reachable

This property indicates whether the Tenable.sc or Tenable.io server connected to the plugin responds to requests from the Forescout platform.

The screenshot shows the 'Condition' dialog box with the title 'Condition'. On the left, a search bar is above a list of conditions under the 'Tenable VM' category. 'Tenable Scanner is Reachable' is selected and highlighted in blue. The main area on the right displays the description: 'Tenable Scanner is Reachable: The Tenable server connected to the plugin and responded to CounterACT requests.' Below this, there are two radio buttons: 'Meets the following criteria' (which is selected) and 'Does not meet the following criteria'. At the bottom, there is a checkbox 'Evaluate irresolveable criteria as' followed by a dropdown menu set to 'False'. At the bottom right are three buttons: 'Help', 'OK', and 'Cancel'.


Tenable Scan Results

This property indicates specific scan results on an endpoint for a selected Tenable scan policy. If none of the items are selected, the scan results apply to all Tenable scan policies.

The screenshot shows the 'Condition' dialog box with the title 'Condition'. On the left, the same search bar and list of conditions are shown, but 'Tenable Scan Results' is now selected and highlighted in blue. The main area on the right displays the description: 'Tenable Scan Results: Indicates specific scan results for an endpoint based on specific scan policies or all scan policies if none is selected.' Below this is a dropdown menu set to 'For one or more property values'. There are three sections, each with a checkbox and a description: 'Scan Policy Name' (description: 'Enter a value to match the Tenable scan policy name.'), 'Repository Name' (description: 'Enter values to match the Tenable.sc repository name or ID.'), and 'DNS Name' (description: 'Enter values to match the fully qualified domain name of the endpoint on which the vulnerat eected.'). Each section has a radio button for 'Meets the following criteria' (all three are selected) and a radio button for 'Does not meet the following criteria'. Below each section is a dropdown menu set to 'Any Value' and a text input field. There is also a checkbox 'Match case' for each section. At the bottom, there are two checkboxes: 'Evaluate irresolveable criteria as' (set to 'False') and 'Evaluate empty list value as' (set to 'False'). At the bottom right are three buttons: 'Help', 'OK', and 'Cancel'.

Select a property to configure its settings.

Scan Policy Name	The Tenable scan policy name. If you do not select a policy, the values are resolved for all policies.
Repository Name	The name or ID of the Tenable.sc repository to which the scan results are written. This applies to Tenable.sc servers only.
DNS Name	The FQDN of the endpoint on which the vulnerability was detected.
Endpoint IP	The IP address of the endpoint on which the vulnerability was detected.
Port	The TCP/IP port of the scanned endpoint.
First Discovered	The time when the vulnerability was first discovered in a scan.
Last Observed	The last time the vulnerability was observed in a scan.
Service	The name of the service detected by the Tenable server.
Protocol	The protocol used by the scanned endpoint to communicate, such as TCP or UDP.
Accept Risk	The Tenable.sc Accept Risk field.
Severity	The vulnerability severity detected by the Tenable.sc or Tenable.io plugin: None (Tenable.io only) or Information (Tenable.sc only), Low, Medium, High, Critical.
Plugin ID	The Tenable.sc or Tenable.io plugin ID.
Plugin Name	The Tenable.sc or Tenable.io plugin name.
Plugin Family	The Tenable.sc or Tenable.io plugin family.
Synopsis	The Tenable brief description of the detected vulnerability.
Risk Factor	The Tenable risk factor of the detected vulnerability or vulnerabilities: None, Low, Medium, High, or Critical.
Vulnerability Publication Date	The date the vulnerability was published.
Plugin Publication Date	The Tenable.sc or Tenable.io plugin publication date.
Plugin Modification Date	The Tenable.sc or Tenable.io plugin modification date.
CVSS Base Score	The Tenable.sc or Tenable.io plugin CVSSv2 base score.
CVE	The Tenable.sc or Tenable.io plugin CVE.
BID	The Tenable Bugtraq ID (bug identifier).
Xref	The pointers to other vulnerability databases, such as IAVA, MSFT, OSVDB.

 If you enabled the **Retrieve results of scans not initiated by CounterACT** option in the Advanced pane, the Tenable Last Scan condition reports results from ALL scans, not just Forescout platform-initiated scans.

Tenable Scan Status

This property indicates the scan status details on an endpoint for a selected Tenable scan policy. If none of the items are selected, the scan status details apply to all Tenable scan policies.

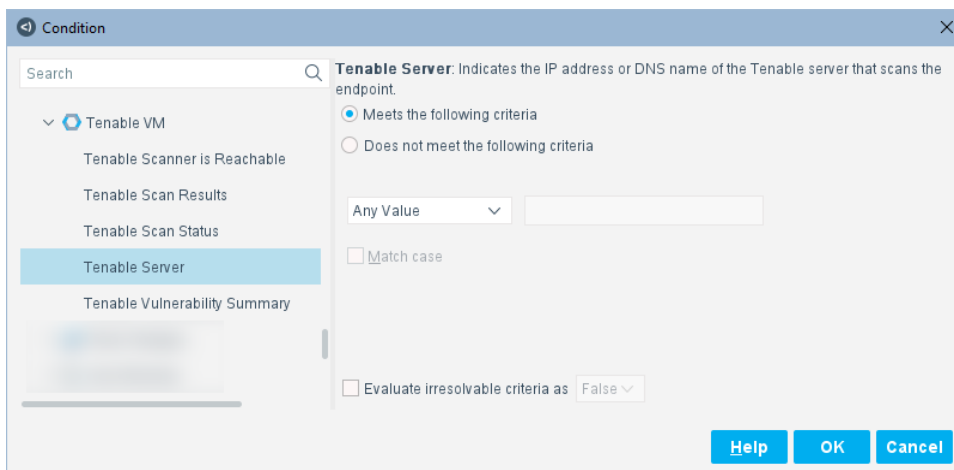
The screenshot shows the 'Condition' configuration window for 'Tenable Scan Status'. The left sidebar lists several properties: 'Tenable VM', 'Tenable Scanner is Reachable', 'Tenable Scan Results', 'Tenable Scan Status' (selected), 'Tenable Server', and 'Tenable Vulnerability Summary'. The main area displays the configuration for 'Tenable Scan Status', which is described as: 'Indicates the scan status details on an endpoint for specific scan policies or for all policies if none are selected.' Below this, there are three sections for configuration: 'Scan Policy Name', 'Repository Name', and 'Scan Status'. Each section has a checkbox to enable it, a text input field, and radio buttons for 'Meets the following criteria' (selected) and 'Does not meet the following criteria'. There are also dropdown menus for 'Any Value' and checkboxes for 'Match case'. At the bottom, there are two checkboxes: 'Evaluate irresolvable criteria as' (set to 'False') and 'Evaluate empty list value as' (set to 'False'). The window has 'Help', 'OK', and 'Cancel' buttons at the bottom right.

Select a property to configure its settings.

Scan Policy Name	The Tenable scan policy name. If you do not select a policy, the values are resolved for all policies.
Repository Name	The name or ID of the Tenable.sc repository to which the scan results are written. This applies to Tenable.sc servers only.
Scan Status	The Tenable scan status: <ul style="list-style-type: none"> ▪ <i>Completed</i>: The scan results were received ▪ <i>In Progress</i>: The scan request was triggered by Forescout eyeExtend for Tenable VM and activated by the Tenable.sc or Tenable.io server
Last Scan Initiation	If the scan is in progress, the time the last scan request was made is reported. Otherwise, the time the last scan was initiated by the Tenable vulnerability product is reported.
Last Scan Completed	The time the last scan completed. If the scan is In Progress, this field contains the same value as the Last Scan Initiation field.

Tenable Server

This property indicates the IP address or DNS name of the Tenable server that scans the endpoint.



Tenable Vulnerability Summary

This property indicates a summary of the vulnerabilities found during scans performed by Tenable.sc on a specific endpoint.

If you are using Tenable.sc, set the parameters. If you are using Tenable.io, this property does not apply.

- 📄 *The Tenable.sc Vulnerabilities Found property was made obsolete in release 2.6. If you migrated from Tenable VM version 2.5 or earlier, the scan title states Tenable Vulnerabilities Found Obsolete.*

Condition

Search

Tenable VM

- Tenable Scanner is Reachable
- Tenable Scan Results
- Tenable Scan Status
- Tenable Server
- Tenable Vulnerability Summary**

Tenable Vulnerability Summary: Indicates a summary of the vulnerabilities found during scans performed by Tenable.sc. (Tenable.sc only)

For one or more property values

☐ Scan Policy Name
Enter a value to match the Tenable scan policy name.

☒ Meets the following criteria
☐ Does not meet the following criteria

Any Value

☐ Match case

☐ Repository Name
Enter values to match the Tenable.sc repository name or ID.

☒ Meets the following criteria
☐ Does not meet the following criteria

Any Value

☐ Match case

☐ Vulnerability Score
Enter values to match the Tenable.sc vulnerability score.

☒ Meets the following criteria

☐ Evaluate irresolvable criteria as False Evaluate empty list value as False

Help OK Cancel

Select a property to configure its settings.

Scan Policy Name	The name of the Tenable scan policy. If you do not select a policy, the values are resolved for all policies.
Repository Name	The name or ID of the Tenable.sc repository to which the scan results are written.
Vulnerability Score	The Tenable.sc vulnerability score.
Information Severity Message Count	The count of Information severity messages.
Low Severity Defect Count	The count of Low severity defects.
Medium Severity Defect Count	The count of Medium severity defects.
High Severity Defect Count	The count of High severity defects.
Critical Severity Defect Count	The count of Critical severity defects.
All Severity Counts	The comma-separated list of the counts of the five severity levels, from Critical to Information.

Tenable VM Policy Actions – Scan Endpoints

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

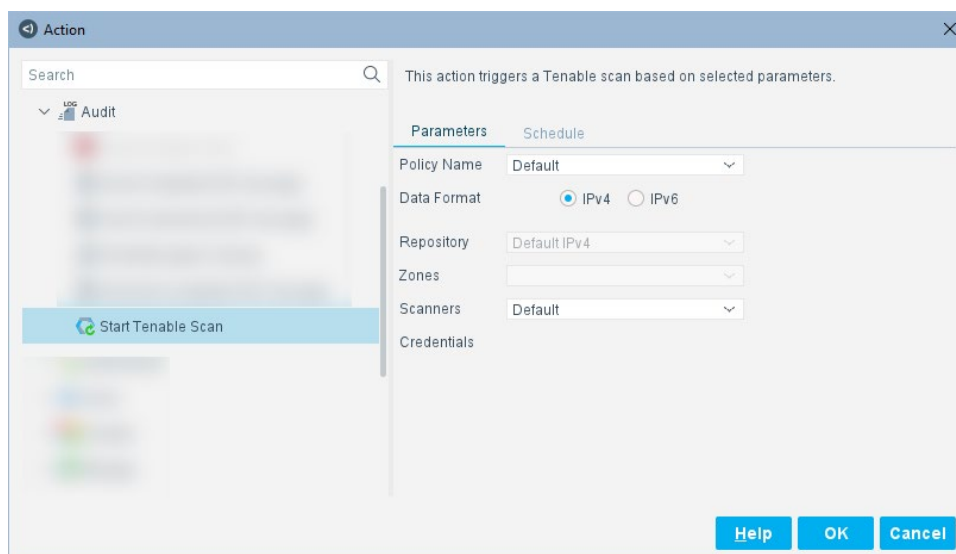
In addition to the bundled Forescout actions available for handling endpoints, you can work with the Tenable-related actions to create custom Forescout platform policies. This action is available when you install Forescout eyeExtend for Tenable VM.

Start Tenable Scan

Use the Start Tenable Scan action in Forescout platform policies to run a scan when certain policy conditions are met. For example, you can create a policy that runs a Tenable scan when the Forescout platform 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 and expand the **Audit** folder in the Actions tree.



2. Select **Start Tenable Scan**. The dialog box opens to the Parameters tab.

3. Enter the following parameters.

Policy Name	The brief name of the policy the Tenable scan uses.
Data Format	The data format. Select either IPv4 or IPv6 .
Repository	The repository ID or name. If you select a Data Format of IPv4 , the list is populated with IPv4 repositories. If you select a Data Format of IPv6 , the list is populated with IPv6 repositories.
Zones	The zones for this scan. If Tenable.sc is configured for you to select a scan zone, you can select a zone from the Zones menu.
Scanners	The scanners for this scan. If Tenable.io is configured, you can select a scanner from the Scanners menu.
Credentials	(Optional) The credentials for this scan. You can select one or more credentials for Tenable.sc servers. To select multiple credentials, hold down the Ctrl key or the Shift key.

4. Select the Schedule tab and select one of the following schedules:

- **Start action when the endpoint matches a 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 after a condition sub-rule match on the Action Scheduler. Select **OK**.

5. Select **OK**.

You can identify action success or failure in the Console Detections pane. See [Start Tenable Scan Action](#).

Tenable VM – Asset Inventory and Scan Results

Now that you have established communication between Forescout eyeExtend for Tenable VM and a Tenable server, you can launch scans and create policies based on scan results.

Display Tenable VM Asset Inventory Events

Use the 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 you can acquire information about endpoints with similar findings.

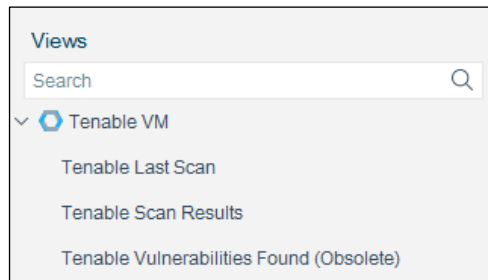
The Asset Inventory lets you:

- 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 Forescout platform policies.

To access the Asset Inventory:

1. Log in to the Console and select **Asset Inventory**.
2. In the Views pane, expand the **Tenable** folder or enter **Tenable** in the **Search** field.



The following information is available:

- **Tenable Last Scan:** Displays the time of the last scan initiated by Forescout eyeExtend for Tenable VM.
- **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 Tenable.sc Vulnerabilities Found property was made obsolete in release 2.6. If you migrated from Tenable VM version 2.5 or earlier, the scan title is *Tenable Vulnerabilities Found (Obsolete)*.

Plugin Name	Plugin Family	Risk Factor	CVSS Base Score	CVE	Xref	LL	No.	L.	L.
MS16-077: Security Update for WPAD (3165191)	Windows : Microsoft Bulletins	Critical	10.0	CVE-2016-3299	1	7L...	10...		
MS16-077: Security Update for WPAD (3165191)	Windows : Microsoft Bulletins	Critical	10.0	CVE-2016-3213	1	7L...	10...		
MS16-077: Security Update for WPAD (3165191)	Windows : Microsoft Bulletins	Critical	10.0	CVE-2016-3236	1	7L...	10...		
MS16-076: Security Update for Netlogon (3167691)	Windows : Microsoft Bulletins	High	9.0	CVE-2016-3228	1	7L...	10...		
MS16-076: Security Update for Windows SMB Server...	Windows : Microsoft Bulletins	Medium	6.9	CVE-2016-3225	1	7L...	10...		
MS16-074: Security Update for Microsoft Graphics Co...	Windows : Microsoft Bulletins	Medium	6.9	CVE-2016-3216	1	7L...	10...		

Hosts

Scan Policy Name:
Repository Name:
DNS Name:
Endpoint IP:
Port:
First Discovered:
Last Observed:
Service:
Protocol:
Accept Risk:
Severity:

Tenable Scan Results: Plugin ID: Plugin Name: MS16-077: Security Update for WPAD (3165191)

1 OF 382 HOSTS

There is a warning in the Asset Inventory when you select *Tenable Scan Results*: Note that the data in this view is collected from endpoints based only on policies. Select **OK**.

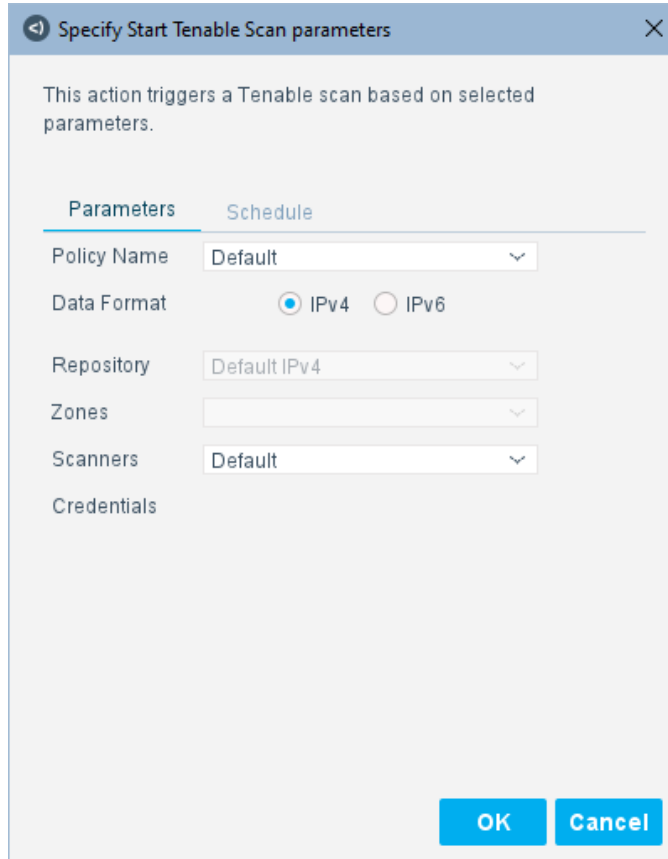
Refer to [Working with Asset Inventory Detections](#) in the *Forescout Administration Guide* for information about how to work with the Asset Inventory.

Start Tenable Scan Action

Use the **Start Tenable Scan** action in the Forescout platform to launch a scan after selected parameters are set. For example, create a Forescout platform 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 Console, select **Home**.
2. Right-click on a host, select **Audit** and then select **Start Tenable Scan**.



The dialog box titled "Specify Start Tenable Scan parameters" contains a description: "This action triggers a Tenable scan based on selected parameters." It features two tabs: "Parameters" (active) and "Schedule". Under the "Parameters" tab, there are several fields: "Policy Name" (a dropdown menu showing "Default"), "Data Format" (radio buttons for "IPv4" (selected) and "IPv6"), "Repository" (a dropdown menu showing "Default IPv4"), "Zones" (a dropdown menu), "Scanners" (a dropdown menu showing "Default"), and "Credentials" (a text input field). At the bottom right, there are "OK" and "Cancel" buttons.

3. Enter the following parameters:

Policy Name	The brief name of the policy the Tenable scan uses.
Data Format	The data format. Select either IPv4 or IPv6 .

Repository	The Tenable.sc repository ID or name. If you select a Data Format of IPv4 , the list is populated with IPv4 repositories. If you select a Data Format of IPv6 , the list is populated with IPv6 repositories.
Zones	The zones for this scan. If Tenable.sc is configured for you to select a scan zone, you can select a zone from the Zones menu.
Scanners	The scanners for this scan. If Tenable.io is configured, you can select a scanner from the Scanners menu.
Credentials	(Optional) The credentials for this scan. You can select one or more credentials for Tenable.sc servers. To select multiple credentials, hold down the Ctrl key or the Shift key.

4. Select the Schedule tab and select one of the following schedules:
 - **Start action when the endpoint matches a 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 after a condition sub-rule match on the Action Scheduler. Select **OK**.
5. Select **OK**.

To view the results of a scan:

1. In the Detections pane of the **Home** tab, select the endpoint on which you ran the scan.
2. In the **Actions** column, an icon indicates the status of the scan.
3. Hold your cursor over the icon. The scan results are displayed.

