Contact Information
Forescout Technologies, Inc.
190 West Tasman Drive
San Jose, CA 95134 USA
https://www.forescout.com/support/
Toll-Free (US): 1.866.377.8771
Tel (Intl): 1.408.213.3191
Support: 1.708.237.6591

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

Legal Notice
© 2019 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.
# Table of Contents

**About the Tenable VM Integration** .......................................................... 5  
Compatible Tenable Vulnerability Products .................................................. 5  
About Certification Compliance Mode ......................................................... 6  
About Support for Dual Stack Environments ................................................. 6  
Additional Tenable Documentation ............................................................... 6  

**Concepts, Components, Considerations** .................................................. 6  
  Concepts ........................................................................................................ 6  
  Components .................................................................................................... 9  
  Considerations ............................................................................................... 9  
  Tenable Server Authentication ...................................................................... 11  

**What to Do** .................................................................................................. 11  

**Requirements** ........................................................................................... 11  
  Forescout Requirements .................................................................................. 12  
  Forescout eyeExtend (Extended Module) Licensing Requirements .................. 12  
    Per-Appliance Licensing Mode .................................................................... 12  
    Flexx Licensing Mode ................................................................................ 14  
    More License Information .......................................................................... 14  
    Supported Tenable Versions ...................................................................... 14  

**Install the Module** ..................................................................................... 15  

**Configure the Module** ................................................................................ 15  
  Add a Tenable Server .................................................................................... 16  
  Synchronize Scan Parameters and Select Defaults ...................................... 22  
  Set Auto-Deletion of Scan Results ................................................................ 23  

**Test the Module Configuration** .................................................................. 23  
  Define Test Configuration Parameters ......................................................... 23  
  Run a Module Test ......................................................................................... 25  
  Export the Test Results ................................................................................. 25  

**Create Tenable VM Policies Using Templates** ............................................ 26  
  Forescout Platform Policy Coordination Considerations ............................. 27  
  Create a Basic Tenable Scan Trigger Policy ................................................. 29  
  Create a Risk Factor Results Policy ............................................................ 33  

**Create Custom Tenable VM Policies** ......................................................... 37  
  How Endpoints Are Detected and Handled .................................................. 38  

**Policy Properties – Detect Vulnerabilities** ............................................... 39  
  Tenable Scanner is Reachable ....................................................................... 41  
  Tenable Scan Results .................................................................................... 41
Tenable Scan Status ................................................................. 43
Tenable Server IP ..................................................................... 44
Tenable Vulnerability Summary ............................................. 44

Policy Actions – Scan Endpoints ........................................... 46
Start Tenable Scan ................................................................ 46

Work with the Tenable VM Module ....................................... 47
Display Tenable VM Asset Inventory Events ....................... 47
Start Tenable Scan ............................................................... 48

Additional Forescout Documentation .................................. 49
Documentation Downloads .................................................. 49
Documentation Portal ......................................................... 50
Forescout Help Tools .......................................................... 50
About the Tenable VM Integration

Forescout eyeExtend for Tenable™ Vulnerability Management (VM) integrates the Forescout platform 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 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 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 Forescout platform policies and other basic features work.

Compatible Tenable Vulnerability Products

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

- **Nessus versions 6.0.x through 6.10.x** – A 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 – A 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 Certification Compliance Mode

Forescout eyeExtend for Tenable VM supports Certification Compliance mode. For information about this mode, refer to the Forescout Installation Guide.

About Support for Dual Stack Environments

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

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 the Forescout platform and Tenable VM 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 product is connected to one or more CounterACT devices. When configuring Forescout eyeExtend for Tenable Vulnerability Management, ensure that each product 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 Nessus scanners, Tenable.io products, or SecurityCenter servers. A 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 product, 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**

The key components of a typical deployment include:

- **Connecting CounterACT Device:** This CounterACT device communicates directly with the Nessus scanner, Tenable.io product, 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 servers or Tenable.io products:

- **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 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 products 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**, double-click the device, and select the IP Assignments tab.

- **Synchronization with Scan Policies, Repositories, Zones, and Credentials:** When the Forescout platform triggers a Tenable product scan, it passes information to Tenable including the specific endpoint IP to be scanned, and a Nessus scan policy name. In addition, when triggering a SecurityCenter 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 module configuration tabs of Forescout eyeExtend for Tenable VM. 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 module 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 **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 SecurityCenter, Tenable.io, and Nessus products. By default, the Forescout platform 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 products, or Nessus scanners, and diverse scan compliance policies, see Policy Properties – Detect Vulnerabilities.

Tenable Server Authentication

Forescout eyeExtend for Tenable VM 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 Console. This option is not available for Nessus.

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 the Module.
3. Map CounterACT devices to Nessus, Tenable.io, or SecurityCenter products. See Configure the Module.
4. Test the Module Configuration.
5. Run Forescout platform policies that detect and manage endpoints tracked by a Nessus, Tenable.io, or SecurityCenter product. See Create Tenable VM Policies Using Templates.

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:

- Forescout version 8.1.
- 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 product 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 products. 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 products. 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 products, packaging individual licensed modules are supported. The Open Integration Module is an eyeExtend product 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

- Refer to the Release Notes for the latest supported versions.

Forescout eyeExtend for Tenable VM 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 5.6.1

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

This section 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 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.

Configure the Module

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

After Forescout eyeExtend for Tenable VM is installed on your targeted CounterACT Appliance, you can configure the module for multiple Nessus, Tenable.io, and SecurityCenter products.

To complete configuration of some of these connections, you must perform the following configuration steps on the Tenable.io instance:
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 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 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 SecurityCenter server, Nessus scanner, or Tenable.io cloud.
4. In the General pane, configure the following connection parameters:

<table>
<thead>
<tr>
<th><strong>Server Type</strong></th>
<th>Select the type of Tenable Network Security server. The following options are available:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>- <strong>SecurityCenter</strong> – All fields are active except the Tenable server port.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Tenable.io</strong> – After selecting this option, enter information into the activated Description, User Name, Password and Verify Password fields. All other fields are deactivated.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Nessus Scanner</strong> – When selected, all fields in this pane are active except the Authentication Type and the two SSL fields.</td>
</tr>
</tbody>
</table>

| **Server Domain Name or IP Address** | Enter the server domain name, a Fully Qualified Domain Name (FQDN), or the IPv4 address of Nessus or SecurityCenter that will execute the Forescout platform’s 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** is the selected server type, this field contains a non-editable URL. |
### Server Port
Select the port used to access the SecurityCenter or Nessus scanner. By default, this is port 8834. If **SecurityCenter** or **Tenable** is the selected server type, this field is deactivated.

### Description
(Optional) Enter a description or relevant comment.

### Validate Server Certificate
Select this option to validate the identity of the third-party server before establishing a connection, when the eyeExtend product communicates as a client over SSL/TLS. To validate the server certificate, either of the following certificate(s) must be installed:

- 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

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 Forescout Administration Guide.

### Authentication Type
This option is only available for SecurityCenter servers. 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
- For SecurityCenter servers with **Standard Login** authentication selected, a Security Manager account in SecurityCenter is required.
- For Tenable.io or Nessus servers, enter the User Name.

### Password
Enter the password for the User Name.

### Verify Password
Re-enter the password to verify it.

### SSL Certificate File
For SecurityCenter servers with **Standard Login** authentication 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 the 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.
**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 SecurityCenter, Tenable.io, or Nessus product, 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 product, 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. Only one vulnerability product is designated as the default product.
   - **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**.
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:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum number of seconds a request is in queue</td>
<td>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. 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.</td>
</tr>
<tr>
<td>Number of queued requests to trigger a scan job</td>
<td>The number of queued scan requests that triggers an expedited scan job even before the defined interval elapses.</td>
</tr>
<tr>
<td>Max number of queued requests to trigger a scan job</td>
<td>The number of queued scan requests that triggers an expedited scan job even before the defined interval elapses.</td>
</tr>
<tr>
<td>Max number of scan requests per scan job</td>
<td>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. 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).</td>
</tr>
<tr>
<td>Retrieve results of scans not initiates by CounterACT</td>
<td>When this option is selected, the following policy properties report results from ALL scans, not just Forescout-platform-initiated scans:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Tenable Scan Results</strong></td>
</tr>
<tr>
<td></td>
<td>- <strong>Tenable Scan Status</strong></td>
</tr>
</tbody>
</table>
9. Select **Finish**.

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

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:

<table>
<thead>
<tr>
<th>User Proxy Server</th>
<th>Select this option to use a proxy server to communicate with Tenable.io.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proxy Server Address</td>
<td>Enter the network address of the proxy server.</td>
</tr>
<tr>
<td>Proxy Server Port</td>
<td>Enter the port used to communicate with the proxy server.</td>
</tr>
<tr>
<td>Proxy Username</td>
<td>Enter the login name for an authorized account defined on the proxy server, if required. A management level (or higher) account defined in SecurityCenter is required.</td>
</tr>
<tr>
<td>Proxy Password</td>
<td>Enter the password for the above Proxy User Name.</td>
</tr>
<tr>
<td>Verify Password</td>
<td>Re-enter the password to verify it.</td>
</tr>
</tbody>
</table>

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

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

The best practice is to perform a test after setting up a connection. See **Test the Module Configuration**.
Synchronize Scan Parameters and Select Defaults

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

- **Scan policies** – Specifies which vulnerabilities are tested during the scan. One name per scan.
- **Repositories** – Specifies the location where the scan results are 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 lists 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 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 left pane, select **Tenable VM**. The Tenable VM pane opens.
3. In the Tenable Servers tab, select **Sync**.
   The lists in the Scan Policies, Repositories, Zones, Scanners, and Credentials tabs are updated.
4. 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.
5. For Tenable.io, go to the Scanners tab, select the scanner and then select **Make Default**.
6. For SecurityCenter, select the Repositories tab, select a repository name and then select **Make Default**.
7. 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 are not handled in the Forescout platform if the scan parameter names do not match.*

8. 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.

Test the Module 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 module 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 Nessus, Tenable.io, or SecurityCenter.
- 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 scanner or SecurityCenter to be tested, and select **Edit**.

   ![Edit Tenable Server](image)

   **Edit Tenable Server**

   **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.

<table>
<thead>
<tr>
<th>Endpoint IP Address</th>
<th>Policy Name</th>
<th>Repository</th>
<th>Zone</th>
<th>Scanner</th>
<th>Credential</th>
</tr>
</thead>
<tbody>
<tr>
<td>123.123.123.123</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

2. Select the Test Parameters tab.

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

<table>
<thead>
<tr>
<th><strong>Endpoint IP Address</strong></th>
<th><strong>Enter the IP address of the endpoint on which to carry out the test.</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>▪ If <strong>Display report details for last scan</strong> is selected, the scan status and start time of the last scan requested for this endpoint are displayed.</td>
</tr>
<tr>
<td></td>
<td>▪ If <strong>Trigger a test scan</strong> is not selected, enter any IP value.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Policy Name</strong></th>
<th><strong>Select the Tenable scan policy for which the requested scan test is to be carried out.</strong></th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th><strong>Repository</strong></th>
<th><strong>Select a repository to save the SecurityCenter scan to.</strong></th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th><strong>Zone</strong></th>
<th><strong>If this drop-down menu is populated, select a zone. (It is not an error if this menu is empty.)</strong></th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th><strong>Scanner</strong></th>
<th><strong>If this is a Tenable.io scan, select a scanner.</strong></th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th><strong>Credential</strong></th>
<th><strong>(Optional) Select the credential for the scan test.</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Display status details of the last Tenable scan</td>
<td>Retrieve scan status details of the endpoint to be tested. See Tenable Scan Status for more information.</td>
</tr>
<tr>
<td>------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Trigger a test scan</td>
<td>Trigger a scan on the endpoint to test the scan trigger.</td>
</tr>
</tbody>
</table>

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.

## Run a Module Test

Run the module 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 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 product, or Nessus scanner.
3. Select Test. The test is run.
4. When the tests is complete, 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 and select Export Table....

2. Select a name and the in which format for the information to be exported.
3. Select OK to export the report.

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. Refer to the following sections:

- Forescout Platform Policy Coordination Considerations
- Create a Basic Tenable Scan Trigger Policy
- Create a Risk Factor Results Policy
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.

Working with Tenable VM templates requires you to incorporate Tenable information. See Synchronize Scan Parameters 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 SecurityCenter server, Tenable.io product, or Nessus scanner are connected via the CounterACT Appliance. The CounterACT Appliance determines which endpoints 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 which Scan Policy Name this condition applies to. 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.

   **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, 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 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 Forescout eyeExtend for Tenable VM 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 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, 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**.

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.

Policy names are displayed in the Policy Manager, the Views pane, NAC Reports and in other features. Precise names make working with policies and reports more efficient.

6. Select Next. Both 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.

![IP Address Range dialog box]

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 steps 7 to 8.
9. Select Next.
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 are 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 this menu is empty.)

- **Scanners** – Select the scanner type to use for Tenable.io. (Not applicable 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. (Not applicable for Nessus scans.)
Select **Next**.

The **Sub-Rules** instruct the Forescout platform 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**.

11. 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** 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**.
4. Select **Next**.

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.
Policy names are displayed in the Policy Manager, the Views pane, NAC Reports and in other features. Precise names make working with policies and reports more efficient.

6. Select Next. Both 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.

![IP Address Range dialog box]

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 steps 7 to 8.

9. Select Next.
The Sub-Rules instruct the Forescout platform 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 – 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 Policy Coordination Considerations.

To create a custom policy:
1. Log in to the Console and select Policy. The Policy Manager pane opens.
4. Select Next. The Name pane opens.
5. (Optional) Enter a name and add a description.
6. Select **Next**. Both 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 is displayed in the Scope pane. You can add multiple rows to the scope list by selecting **Add** and repeating steps 7 to 8.

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.

10. Select **Next**. The Main Rule pane opens.

11. In the Conditions section, select **Add**. The Condition dialog box opens.

12. Expand the **Tenable VM** folder in the Properties tree to view the available properties. For details, see:

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

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

13. Configure the rule conditions and actions, and then select **OK** to close the Condition dialog box.

14. In the Group section of the Main Rule pane, select **Add**. The Action dialog box opens.

15. Expand **Audit** in the Actions tree and then select **Start Tenable Scan**.

16. Add conditions and actions based on the expected behavior of the custom policy.

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

18. Sub-Rules are additional condition/action pairs. For definitions, see **Policy Properties – Detect Vulnerabilities**.

19. Select **Finish**.

**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 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**. 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.

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

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

7. Configure the rule conditions and actions, and then select **OK** in the Conditions dialog box. Your new criteria is displayed in the Sub-Rule: New Rule dialog box.

8. To continue, go to **Policy Actions – Scan Endpoints**.
**Tenable Scanner is Reachable**

Configure this property to indicate whether the SecurityCenter server, Tenable.io, or Nessus scanner connected to Forescout eyeExtend for Tenable VM responds to the Forescout platform's 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 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 a property to configure its settings.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Scan Policy Name</strong></td>
<td>The Tenable scan policy name. If you do not select a policy, the values are resolved for all policies.</td>
</tr>
<tr>
<td><strong>Repository Name</strong></td>
<td>The name or ID of the SecurityCenter repository where the scan results are written. This applies to SecurityCenter servers only.</td>
</tr>
<tr>
<td><strong>Endpoint IP</strong></td>
<td>The IP address of the endpoint to be matched.</td>
</tr>
<tr>
<td><strong>Port</strong></td>
<td>The TCP/IP port of the scanned endpoint.</td>
</tr>
<tr>
<td><strong>First Discovery Time</strong></td>
<td>The time when the vulnerability was first discovered in a scan.</td>
</tr>
<tr>
<td><strong>Last Discovery Time</strong></td>
<td>The last time the vulnerability was discovered in a scan.</td>
</tr>
<tr>
<td><strong>Service</strong></td>
<td>The name of the service detected by Tenable.</td>
</tr>
<tr>
<td><strong>Protocol</strong></td>
<td>The protocol used by the scanned endpoint to communicate; for example, TCP, UDP</td>
</tr>
<tr>
<td><strong>Accept Risk</strong></td>
<td>Enter a value to match the SecurityCenter Accept Risk value.</td>
</tr>
<tr>
<td><strong>Severity</strong></td>
<td>Any of the following vulnerability severities detected: None (Nessus scanner only) or Information (SecurityCenter only), Low, Medium, High, Critical.</td>
</tr>
<tr>
<td><strong>Plugin ID</strong></td>
<td>The human-readable ID of the reporting Forescout eyeExtend for Tenable VM.</td>
</tr>
<tr>
<td><strong>Plugin Name</strong></td>
<td>The human-readable name of the reporting Forescout eyeExtend for Tenable VM.</td>
</tr>
<tr>
<td><strong>Plugin Family</strong></td>
<td>The family to which the reporting Forescout eyeExtend for Tenable VM belongs.</td>
</tr>
<tr>
<td><strong>Synopsis</strong></td>
<td>Brief description of the detected vulnerability.</td>
</tr>
<tr>
<td><strong>Risk Factor</strong></td>
<td>The human-readable form of the perceived risk factor of the vulnerability or vulnerabilities reported: None, Low, Medium, High, Critical.</td>
</tr>
<tr>
<td><strong>Vulnerability Publication Date</strong></td>
<td>Date the vulnerability was published.</td>
</tr>
<tr>
<td><strong>Plugin Publication Date</strong></td>
<td>Date the reporting Forescout eyeExtend for Tenable VM was published.</td>
</tr>
<tr>
<td><strong>Plugin Modification Date</strong></td>
<td>Date the reporting Forescout eyeExtend for Tenable VM was last modified.</td>
</tr>
<tr>
<td><strong>CVSS Base Score</strong></td>
<td>CVSSv2 base score.</td>
</tr>
<tr>
<td><strong>CVE</strong></td>
<td>CVE ID.</td>
</tr>
<tr>
<td><strong>BID</strong></td>
<td>Tenable Bugtraq ID (bug identifier).</td>
</tr>
<tr>
<td><strong>Xref</strong></td>
<td>Pointers to other vulnerability databases such as IAVA, MSFT, OSVDB.</td>
</tr>
</tbody>
</table>
If you enabled the **Retrieve results of scans not initiated by CounterACT** option, the Tenable Last Scan condition reports results from **ALL scans**, not just Forescout-platform-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 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.

<table>
<thead>
<tr>
<th><strong>Scan Policy Name</strong></th>
<th>The Tenable scan policy name. If you do not select a policy, the values are resolved for all policies.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Repository Name</strong></td>
<td>The name or ID of the SecurityCenter repository where the scan results are written. This applies to SecurityCenter servers only.</td>
</tr>
</tbody>
</table>
| **Scan Status**      | The status of the scan:  
  - *Completed* – Scan results received  
  - *In Progress* – The scan request was triggered by Forescout eyeExtend for Tenable VM and activated by the SecurityCenter server, Tenable.io, or Nessus scanner |
<table>
<thead>
<tr>
<th><strong>Last Scan Initiation</strong></th>
<th>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.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Last Scan Completed</strong></td>
<td>Enter the values to match the Scan Completed time. If the scan is In Progress, this field contains the same value as the Last Scan Initiation field.</td>
</tr>
</tbody>
</table>

**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 states Tenable Vulnerabilities Found Obsolete.*
<table>
<thead>
<tr>
<th><strong>Scan Policy Name</strong></th>
<th>The name of the Tenable scan policy. If you do not select a policy, the values are resolved for all policies.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Repository Name</strong></td>
<td>The name or ID of the SecurityCenter repository where the scan results are written. This applies to SecurityCenter servers only.</td>
</tr>
<tr>
<td><strong>Vulnerability Score</strong></td>
<td>Enter vulnerability score values to match the SecurityCenter's vulnerability score.</td>
</tr>
<tr>
<td><strong>Information Severity Message Count</strong></td>
<td>Enter Information Severity Message Count values to match the count of Information severity messages.</td>
</tr>
<tr>
<td><strong>Low Severity Defect Count</strong></td>
<td>Enter Low Severity Defect Count values to match the count of Low Severity Defects.</td>
</tr>
</tbody>
</table>
Policy Actions – Scan Endpoints

The Forescout platform policy actions let you instruct the Forescout platform 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 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, 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.
2. Expand the Audit folder in the Actions tree.
3. Select Start Tenable Scan. The Parameters tab is displayed in the right pane.
4. Enter the following:

<table>
<thead>
<tr>
<th>Policy Name</th>
<th>Enter a brief name to represent the policy the Tenable scan uses, for example, DNS Name or IPs.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Repository</td>
<td>Enter the values to match the SecurityCenter repository ID or name.</td>
</tr>
<tr>
<td>Zones</td>
<td>If SecurityCenter is configured in selectable mode, this drop-down menu is populated for selection.</td>
</tr>
<tr>
<td>Scanners</td>
<td>This option is activated for Tenable.io.</td>
</tr>
<tr>
<td>Credentials</td>
<td>(Optional) Select the appropriate credential for this scan.</td>
</tr>
</tbody>
</table>

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 Console Detections pane.

Work with the Tenable VM Module

Now that you have established communication between Forescout eyeExtend for Tenable VM 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 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 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 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 is *Tenable Vulnerabilities Found (Obsolete)*.

Refer to *Working in the Console > Working with Inventory Detections* in the *Forescout Administration Guide* or the Console Online Help for information about how to work with the Asset Inventory.

## Start Tenable Scan

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 triggers the scan when an endpoint meets this condition.

### To manually start a scan:

1. In the Console, select **Home**.
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. Configure the scan as follows:
   - If SecurityCenter is configured to let you select a scan zone, you can select a zone from the **Zones** drop-down menu.
   - If Tenable.io is configured, you can select a scanner from the **Scanner** drop-down menu.
4. Set the scan 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 where 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.
Additional Forescout Documentation

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

- Documentation Downloads
- Documentation Portal
- Forescout Help Tools

Documentation Downloads

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

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

Software downloads are also available from these portals.

To identify your licensing mode:

- From the Console, select Help > About Forescout.

Forescout Resources Page

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

To access the Forescout Resources Page:


Product Updates Portal

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

To access the Product Updates Portal:

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

Customer Portal

The Downloads page on the Forescout Customer Portal provides links to purchased Forescout version releases, Base and Content Modules, and eyeExtend products, as well as related documentation. Software and related documentation will only appear on the Downloads page if you have a license entitlement for the software.
To access documentation on the Forescout Customer Portal:

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

Documentation Portal

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

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

To access the Documentation Portal:

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

Forescout Help Tools

Access information directly from the Console.

Console Help Buttons

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

Forescout Administration Guide

- Select Forescout Help from the Help menu.

Plugin Help Files

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

Online Documentation

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