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.
# Table of Contents

**About the Qualys VM Integration** ........................................................................ 4
   Additional Qualys VM Documentation ............................................................. 4

**About This Module** ....................................................................................... 4
   Components ................................................................................................. 5
   Considerations .......................................................................................... 5
   What to Do ............................................................................................... 6

**Requirements** ............................................................................................. 6
   Forescout Requirements ............................................................................. 7
   About Support for Dual Stack Environments ............................................. 7
   Forescout eyeExtend (Extended Module) Licensing Requirements .......... 7
      Per-Appliance Licensing Mode ............................................................... 7
      Flexx Licensing Mode ......................................................................... 9
   More License Information ........................................................................ 9
   Qualys Requirements ................................................................................ 9

**Configure the Qualys Environment** ............................................................ 10

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

**Disable Discovery of Qualys Host Properties** .......................................... 18

**Test the Module** ......................................................................................... 19

**Create Qualys VM Policies Using Templates** .............................................. 22
   Create a Basic Qualys VM Scan Trigger Policy ....................................... 23
   Create a Qualys VM Severity Results Policy .......................................... 27

**Create Custom Policies in the Forescout Platform** .................................. 30
   Detect Vulnerabilities – Policy Properties .............................................. 30
   Scan Endpoints - Policy Actions ............................................................. 32
   Launch Qualys Scan ................................................................................ 32

**Display Qualys VM Asset Inventory Information** ...................................... 33

**Additional Forescout Documentation** ....................................................... 35
   Documentation Downloads ..................................................................... 35
   Documentation Portal ............................................................................... 36
   Forescout Help Tools ................................................................................ 36
About the Qualys VM Integration

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

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

Forescout eyeExtend for Qualys VM lets you integrate the Forescout platform with Qualys Cloud Platform vulnerability management tools. Create the Forescout platform policies to monitor, manage, restrict, and remediate endpoints in real-time, based on Qualys scan results.

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

Additional Qualys VM Documentation

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

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

About This Module

The Forescout platform’s bi-directional communication with the Qualys Cloud Platform offers several unique capabilities:

- The Forescout platform can launch a Qualys scan based on detected network activity. For example, scan an endpoint on its admission to the network or if a specific application is installed. See Scan Endpoints - Policy Actions.

- The Forescout platform evaluates Qualys scan results and can trigger actions. For example, if a critical vulnerability severity is detected on an endpoint, the Forescout platform can apply an action that triggers another scan, or one that restricts corporate network access.

- The Forescout Asset Inventory displays the endpoints that have been identified as vulnerable by the module. See Display Qualys VM Asset Inventory Information.

Information detected is also displayed in the Forescout Dashboard and in Forescout reports. Refer to the Online Help for details about these features.
Components

The components of Forescout eyeExtend for Qualys VM include:

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

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

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

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

![Diagram showing the relationship between Qualys Cloud Platform, Connecting CounterACT Device, and devices](image)

Considerations

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

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

If an Option Profile or Scanner Appliance name is changed or added in the Qualys Cloud Platform, the name in the Forescout platform configuration must be set accordingly. See [Add Qualys Option Profiles](#) and [Add Qualys Scanner Appliances](#).
The Qualys operator must ensure that:

- There is a Qualys Report Template named ForeScout Vulnerability Report, which is not limited to any Asset Group or IP range. See Configure the Qualys Environment.
- The Option Profile name selected from the names configured in Forescout eyeExtend for Qualys VM matches the name of a Qualys Option Profile that is not limited to any Asset Group or IP range.
- All endpoints to be scanned are:
  - Included as host assets in the Qualys subscription
  - Within the scope defined in the Forescout platform policy

Consider the following when using Forescout eyeExtend for Qualys VM:

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

**What to Do**

Perform the following steps to set up the integration:

1. Verify that all requirements are met. See Requirements.
2. Configure the Qualys Environment.
3. Install the Module.
4. Configure the Module.
5. Test the Module.

**Requirements**

Verify that the following requirements are met:

- Forescout Requirements
- About Support for Dual Stack Environments
- Forescout eyeExtend (Extended Module) Licensing Requirements
- Qualys Requirements
Forescout Requirements

The module requires the following Forescout releases and components:

- Forescout version 8.2.
- A module license for Forescout eyeExtend for Qualys VM. See Forescout eyeExtend (Extended Module) Licensing Requirements.

About Support for Dual Stack Environments

The Forescout platform 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.

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.

Qualys Requirements

- Qualys VM version 8.x.
- 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.
Configure the Qualys Environment

Configure your Qualys environment for communication with the Forescout platform.

**To configure your Qualys environment:**

1. In the Qualys Enterprise Vulnerability Management window, create a Qualys user for the Forescout platform.
   - a. Assign the user an email address at which status emails can be received.
   - b. Assign the user a **Manager** role.
   - c. Configure the user for **API**.
2. Log in as the newly created user for the Forescout platform.
3. In the Reports Setup, enable **CVSS Scoring**.
4. Create a new Scan Report Template.
   - a. Set the template **Title** to **ForeScout Vulnerability Report**.
   - b. Set the template owner to the user created for the Forescout platform.
   - c. In the Findings tab, select **Host Based Findings**, and set the Asset Groups to **All**. Do not change any other settings in the tab.
   - d. In the Display tab, in the Graphics area, select **Vulnerabilities by Severity** and **Potential Vulnerabilities by Severity**.
   - e. Do not change any other settings in the template.

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

Install the Module

This section describes how to 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 the Module**

After Forescout eyeExtend for Qualys VM is installed, configure the module to ensure that the Forescout platform can communicate with the Qualys VM service.

**To configure the module:**

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

2. Select **Modules**.

3. In the Modules pane, select **Qualys VM**, and select **Configure**.

4. Do the following:
   - **Add Qualys Option Profiles**.
   - **Add Qualys Scanner Appliances**.
   - **Add a Qualys Cloud Platform**.
   - **Define Test Configuration Parameters**.
Add Qualys Option Profiles

Qualys Option Profiles determine which information Qualys gathers during a scan. When the Forescout platform initiates a scan, it must pass the name of a specific Option Profile to Qualys.

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

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

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

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

To add the name of an Option Profile:

1. In the Option Profiles tab, select Add.

2. Enter the name of an Option Profile exactly as it appears in your Qualys Cloud Platform configuration.

3. Select OK. The Option Profile name is displayed in the Option Profiles pane.

Add Qualys Scanner Appliances

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

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

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

If a Scanner Appliance is removed or renamed in the Qualys Cloud Platform, you must update the Forescout platform configuration. Future Qualys scans are not handled correctly if the Scanner Appliance names in Qualys and in the Forescout platform do not match.
To add the name of a Scanner Appliance:
1. In the Scanner Appliances tab, select Add.
2. Enter the name of a Scanner Appliance exactly as it appears in your Qualys Cloud Platform configuration.

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

To add a Qualys Cloud Platform:
1. In the Qualys Cloud Platforms tab, select Add.
2. Configure the following connection parameters:

<table>
<thead>
<tr>
<th>Qualys Username</th>
<th>Enter the login name that has full access to the Qualys Cloud Platform. See step 1 of Configure the Qualys Environment.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Qualys Password</td>
<td>Enter the password.</td>
</tr>
<tr>
<td>Verify Password</td>
<td>Re-enter the password.</td>
</tr>
<tr>
<td>Qualys Cloud Platform</td>
<td>Enter the URL of the Qualys Cloud Platform.</td>
</tr>
<tr>
<td>-----------------------</td>
<td>--------------------------------------------</td>
</tr>
<tr>
<td>Qualys Cloud Platform Description</td>
<td>Enter a description of the Qualys Cloud Platform, or a relevant comment.</td>
</tr>
</tbody>
</table>
| 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. |

Forescout eyeExtend for Qualys VM needs to be restarted after a Certificate Authority (CA) or self-signed server certificate is installed.

3. Select Next.

4. In the CounterACT Devices pane, from the Connecting CounterACT Device drop-down menu, select a Connecting CounterACT Device through which other CounterACT devices will communicate with this Qualys Cloud Platform. Each CounterACT device can be assigned to only one Connecting Device. Each Connecting Device can communicate with only one Qualys Cloud Platform. This CounterACT device manages all communication with the defined Qualys Cloud Platform, including forwarding scan requests submitted to it by other CounterACT devices assigned to this Qualys Cloud Platform, and dispatching received scan results back to the appropriate devices.

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

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

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

<table>
<thead>
<tr>
<th>Use Proxy Server</th>
<th>Select this option to use a proxy server to communicate with the Qualys Cloud Platform.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proxy Server IP Address</td>
<td>The network address of the proxy server.</td>
</tr>
<tr>
<td>Proxy Server Port</td>
<td>The port used to communicate with the proxy server.</td>
</tr>
<tr>
<td>Proxy Username</td>
<td>The login name for an authorized account defined on the proxy server, if required.</td>
</tr>
<tr>
<td>Proxy Password</td>
<td>Enter the password, if required.</td>
</tr>
<tr>
<td>Verify Password</td>
<td>Re-enter the password.</td>
</tr>
</tbody>
</table>

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

**Define Test Configuration Parameters**

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

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host IP Address</td>
<td>Define the IP address of the endpoint to be tested. If Display report details for last scan is selected, the scan status and start time of the last scan requested for this endpoint are displayed. If Launch new scan is selected, the selected endpoint is scanned. The endpoint must be connected to the corporate network when the scan is run. If Launch new scan and Display report details for last scan are not selected, this field can be any valid IP value.</td>
</tr>
<tr>
<td>Option Profile</td>
<td>Select a Qualys Option Profile. If Display report details for last scan is selected, details are displayed of the last scan that used the selected Option Profile. If Launch new scan is selected, the selected Option Profile is used in the scan test. If Launch new scan and Display report details for last scan are not selected, this field is ignored.</td>
</tr>
<tr>
<td>Scanner Appliance</td>
<td>Select a Qualys Scanner Appliance. If Display report details for last scan is selected, details are displayed of the last scan that used the selected Scanner Appliance. If Launch new scan is selected, the selected Scanner Appliance is used in the scan test. If Launch new scan and Display report details for last scan are not selected, this field is ignored.</td>
</tr>
<tr>
<td>Display report details for last scan</td>
<td>If this option is selected, the test retrieves the status and the start time of the last Forescout platform scan request in which: The selected endpoint was requested to be scanned The selected Option Profile was used in the scan request The selected Scanner Appliance was used in the scan request</td>
</tr>
<tr>
<td>Launch new scan</td>
<td>If this option is selected, the test launches a new scan on the test endpoint using the selected Option Profile and Scanner Appliance.</td>
</tr>
</tbody>
</table>

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

To run the test, see Test the Module.

2. Select Finish. The Qualys Cloud Platform information is displayed in the Qualys Cloud Platforms pane.
3. Select **Apply** and **Close**. The module configurations are applied.

---

**Disable Discovery of Qualys Host Properties**

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

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

For more information about discovery features, refer to the *Forescout Administration Guide*.

**To disable background discovery behavior for Qualys host properties:**

1. In the Console, select **Options** from the **Tools** menu. The Options dialog box opens.
2. Select **Discovery**. The Discovery pane opens.
3. In the Discovery table, select the Inventory record.
4. Select **Edit**.
5. Select the Properties tab. This tab lets you select which properties listed in Asset Inventory view are regularly updated in the background.

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

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

Test the Module

The best practice is to perform a test after setting up a connection. Run the module test to:

- Verify that the selected endpoint’s Connecting Device can log in to the specified Qualys Cloud Platform.
- (Optional) Launch a scan to verify that a scan can be run.
  
  A successful scan indicates that:
  - The endpoint is connected.
  - The specified Option Profile name exists in the Qualys environment.
  - The specified Scanner Appliance name exists in the Qualys environment.
- (Optional) Retrieve the status of the selected endpoint’s most recent Forescout platform scan request that used the specified Option Profile and Scanner Appliance.

You can modify the test configuration parameters before running the test.

To run the module test:

1. In the Console, select Options from the Tools menu. The Options dialog box opens.
2. Select **Modules**.

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

4. In the Qualys Cloud Platforms tab, select the Connecting Device to be tested.

5. (Optional) To modify the test parameters:
   a. Select **Edit**. The Edit Qualys Cloud Platform window opens.
   b. Select the Test tab.
   
   ![Edit Qualys Cloud Platform](image)

   c. Set the values. For details, see **Define Test Configuration Parameters**.
   d. Select **OK** and select **Apply**.

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

   The following example shows the results of a test with no options selected:
The following example shows the results of a test with `Display report details for last scan` selected:
The following example shows the results of a test with Launch new scan selected:

7. Select Close.

Create Qualys VM Policies Using Templates

The 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 that match specified policy rules – are included in the templates.

This section describes how to use Qualys VM templates to create policies to detect and manage endpoints. Refer to the following sections:

- Create a Basic Qualys VM Scan Trigger Policy
- Create a Qualys VM Severity Results Policy
Both templates provide baseline capabilities. It is recommended to test the policies on a limited network segment, and then modify and extend them to meet corporate security requirements.

Create a Basic Qualys VM Scan Trigger Policy

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

Use the Basic Qualys VM Scan Trigger's template to create a policy that launches a Qualys scan request for the selected Qualys Option Profile and Scanner Appliance, based on the following default settings:

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

This policy template enables the Forescout platform to launch a basic scan. You can update the defaults as required and can further customize the policy by adding sub-rules that instruct the Forescout platform to launch a scan only when an endpoint is detected with specific properties. For example, instruct the Forescout platform to launch a scan request when it detects specific applications installed on an endpoint or if specific 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 the Policy tab.
2. Select Add from the Policy Manager. The Policy Wizard opens.
3. Expand the **Qualys VM** folder and select **Basic Qualys VM Scan Launch**.

4. Select **Next**.

5. Accept the default name or create a new 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.
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.

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

11. Select Next.

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

- Not scanned within the last 24 hours
- Not currently being scanned

12. Select Finish to create the Qualys VM policy.
Create a Qualys VM Severity Results Policy

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

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

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

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

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

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

These actions are disabled by default.

**To create a policy:**

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

5. Accept the default name or create a new 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.
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.

9. Select **Next**.

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

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

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

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

## Create Custom Policies in the Forescout Platform

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

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

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

**To create a custom policy:**

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

## Detect Vulnerabilities – Policy Properties

Policy properties let you instruct the Forescout platform to detect endpoints with specific attributes. For example, create a policy that instructs the Forescout platform to detect endpoints running a specific operating system or having a specific application installed.
To access Qualys VM properties:

1. Open the policy Conditions dialog box.
2. Expand the Qualys VM folder in the Properties tree. The following properties are available:

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

### Scanner Appliance
The Qualys Scanner Appliance name. If you do not select a Scanner Appliance, the property is resolved for all Scanner Appliances.

### Scan Status
The status of the Qualys scan requested by the Forescout platform.

### Last Start Scan Time
The most recent time that a scan was successfully launched, regardless of its current status.

### Scan Endpoints - Policy Actions
Policy actions let you instruct the Forescout platform how to control detected endpoints. For example, assign potentially compromised endpoints to an isolated VLAN, or send the endpoint user or IT team an email.

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

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

Scans launched automatically by a policy use the Option Profile and the Scanner Appliance set during policy creation.
Manual scans are launched using the Launch Qualys Scan action on one or more endpoints. The action prompts the operator to select an Option Profile and a Scanner Appliance.

As with other actions in the Forescout platform, you can identify successful or failed actions using the Console.

**Display Qualys VM Asset Inventory Information**

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

The Asset Inventory lets you:

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

1. Log in to the Console and select **Asset Inventory**.
2. In the Views pane, expand the **Qualys VM** folder.

The following views are available:

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

- **Qualys Scan Results**: Displays the vulnerability results from the most recent Qualys host-based ForeScout Vulnerability Report for each endpoint.

- **Qualys Scan Status**: Displays the Qualys scan parameters, the status, the start time, the last time the status was reported to the Forescout platform, and the scanned host information of the most recent Qualys scans initiated by the Forescout platform.
For information about how to work with the Asset Inventory, refer to Working in the Console > Working with Inventory Detections in the Forescout Administration Guide or the Console Online Help.

**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 Technical Documentation Page, and 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 Support Portal

Software downloads are also available from these portals.

**To identify your licensing mode:**

- From the Console, select Help > About Forescout.
**Forescout Technical Documentation Page**
The Forescout Technical Documentation Page provides access to a searchable, web-based Documentation Portal as well as PDF links to the full range of technical documentation.

**To access the Technical Documentation Page:**
- Go to https://www.Forescout.com/company/technical-documentation/

**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 Support Portal**
The Downloads page on the Forescout Customer Support 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 Customer Support 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.

**To access the Documentation Portal:**
- Go to https://updates.forescout.com/support/files/counteract/docs_portal/

**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 Administration Guide from the Help menu.
**Plugin Help Files**

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

**Documentation Portal**

- Select **Documentation Portal** from the **Help** menu to access the [Documentation Portal](#).