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 Rapid7 Nexpose Integration .......................................................... 5
- Use Cases ........................................................................................................ 5
  - Initiate Nexpose Scan of Suspect Endpoints Identified by the Forescout Platform ................................................. 5
  - Enriched Endpoint Data Context .................................................................. 5
  - Leverage Nexpose Risk Scoring Expertise .................................................... 6
  - Automated Response to Nexpose Scan Results with Forescout Actions ............ 6
  - Additional Rapid7 Nexpose Documentation .................................................. 6

## About the Rapid7 Integration ....................................................................... 6
- Concepts, Components, Considerations ........................................................... 7
- Concepts ......................................................................................................... 7
- Components ................................................................................................. 8
- Considerations ............................................................................................... 9

## What to Do ................................................................................................. 10

## Requirements ............................................................................................. 10
- Forescout Requirements .................................................................................. 10
- About Support for Dual Stack Environments ................................................ 11
- Supported Vendor Requirements .................................................................... 11
- Forescout eyeExtend (Extended Module) Licensing Requirements ................. 11
  - Per-Appliance Licensing Mode ..................................................................... 11
  - Flexx Licensing Mode .................................................................................. 13
  - More License Information ........................................................................... 13

## Install the Module ...................................................................................... 13

## Configure the Module .................................................................................. 14
- Add a Nexpose Security Console .................................................................... 15

## Test the Module Configuration .................................................................... 18
- Export the Test Results .................................................................................. 20

## Create Rapid7 Nexpose Policies Using Templates ....................................... 20
- Create a Nexpose Basic Scan Trigger Policy ................................................ 21
- Create a Nexpose Risk Score Ranking Policy ................................................ 24
- Create a CVSS Severity Ranking Policy ......................................................... 27

## Create Custom Forescout Platform Policies ................................................. 30
- Detect Vulnerabilities - Policy Properties ..................................................... 31
  - Nexpose Connection Is Up ........................................................................... 31
  - Nexpose Risk Score ..................................................................................... 31
  - Nexpose Scan Results ............................................................................... 32
  - Nexpose Scan Status .................................................................................. 34
- Scan Endpoints - Policy Actions ..................................................................... 35
Scan Initiation Fields ................................................................. 35
Start Nexpose Scan ................................................................. 35

Use Rapid7 Nexpose................................................................. 36
   Display Nexpose Inventory Events........................................ 37
   Use the Nexpose Site Deletion Tool ...................................... 39

Additional Forescout Documentation....................................... 39
   Documentation Downloads ................................................ 40
   Documentation Portal ........................................................ 40
   Forescout Help Tools ......................................................... 41
About the Rapid7 Nexpose 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.

Rapid7’s vulnerability management solution, Nexpose, helps you reduce your threat exposure by enabling you to assess and respond in real-time to changes in your environment. The Forescout eyeExtend for Rapid7 Nexpose integration lets you harness real-time network visibility and control capabilities in the Forescout platform to improve the timeliness and efficacy of your vulnerability assessments. The integration lets you leverage real-time information about the risks and vulnerabilities on your network, and enables you to automate response workflows for endpoint remediation and risk mitigation.

Use Cases

This section describes important use cases supported by this integration. To understand how this module helps you achieve these goals, see About the Rapid7 Integration.

- Initiate Nexpose Scan of Suspect Endpoints Identified by the Forescout Platform
- Enriched Endpoint Data Context
- Leverage Nexpose Risk Scoring Expertise
- Automated Response to Nexpose Scan Results with Forescout Actions

Initiate Nexpose Scan of Suspect Endpoints Identified by the Forescout Platform

The Forescout platform policies can launch a Nexpose scan based on:

- Network events or detected activity
- Endpoint posture assessment based on a wealth of host properties
- Nexpose-specific metrics such as time of last scan.

For example, the Forescout platform can scan an endpoint on its admission to the network or if a specific application is installed.

Enriched Endpoint Data Context

Integration brings vulnerability and risk information detected by Nexpose into the rich Forescout platform environment. Forescout policy-based management combines information from several sources synergistically – yielding more rapid, accurate risk detection and mitigation.
Leverage Nexpose Risk Scoring Expertise

Integration makes Nexpose’s strength in risk assessment available within the Forescout platform. In particular, Nexpose Risk Scores refine vulnerability assessment, allowing security managers to quantify the potential threat in security exposures, and prioritize actions and resources devoted to mitigation. Integration lets the Forescout platform detect endpoints based on the severity of their Nexpose Risk Scores, and automatically apply corresponding mitigation/interrogation actions.

Automated Response to Nexpose Scan Results with Forescout Actions

The Forescout platform evaluates Nexpose scan results and can trigger actions based on detected vulnerabilities. For example, if a Nexpose scan reports a critical vulnerability or a high Nexpose Risk Score on an endpoint, the Forescout platform can apply notification, restriction, or isolation actions such as Assign to VLAN or Switch Block to the endpoint.

Additional Rapid7 Nexpose Documentation

Refer to Rapid7 Nexpose documentation for more information:
http://www.rapid7.com/products/Nexpose/

About the Rapid7 Integration

Forescout eyeExtend for Rapid7 Nexpose integrates the Forescout platform with Nexpose Security Consoles so you can:

- Trigger Nexpose endpoint scan requests based on network activity detected by the Forescout platform. For example, delay a scan if the host is offline, or push a scan if a specific application is installed or if the previous scan was not run within a specific time frame. See Create a Nexpose Basic Scan Trigger Policy.

- Organize endpoints into Forescout groups based on the Nexpose risk scores or severity rankings of their detected vulnerabilities. See Create a Nexpose Risk Score Ranking Policy and Create a CVSS Severity Ranking Policy. You can create policies that detect endpoints that are members of these groups, and apply actions to them. For example, apply the Assign to VLAN action to endpoints in the Nexpose Critical Vulnerabilities group.

- Use the Forescout Asset Inventory to see which endpoints the module has identified as vulnerable. Use standard Forescout platform policies to leverage the rich information about hosts detected by Nexpose scans. See Display Nexpose Inventory Events.
To use the module, you should have a solid understanding of Nexpose concepts, functionality and terminology, and understand how the Forescout platform’s policies and other basic features work.

**Concepts, Components, Considerations**

This section provides a basic overview of the architecture of Rapid7 Nexpose and the Forescout platform:

- **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 work with this module.

> In this integration, the terms **asset** and **endpoint** are used interchangeably.

**Concepts**

The module deployment supports one or more CounterACT® devices and one or more Nexpose Security Console scan engine interfaces. Each CounterACT device is associated with a specific Security Console. The Security Console's scan engines must have access to the IP addresses for which the CounterACT device requests a scan.

This integration lets you map one or more CounterACT Appliances or Enterprise Managers to a Nexpose Security Console.

You can assign only one Security Console to a single Connecting CounterACT Device.
Deployment Options

There are two topologies that can be used to integrate multiple CounterACT devices with multiple Nexpose Security Consoles:

- **Peer-to-Peer**: Each CounterACT device communicates directly with a unique Nexpose Security Console. This is a basic one-to-one relationship, where each CounterACT Appliance prompts its connected Security Console to initiate scans when required. This is the typical topology for remote sites where a remote Security Console and remote CounterACT device are deployed.

- **Appliance Proxy**: A Connecting CounterACT Device serves as a proxy to a Nexpose Security Console. The connecting device queues all scan requests from its Assigned CounterACT Devices, and controls the number of scan requests as well as the number of hosts per single scan request, to ensure more efficient traffic control and to avoid overloading the scan engines.

  Deployments can be designed to combine both topologies to meet particular network requirements.

Components

The components of Forescout eyeExtend for Rapid7 Nexpose include:

**Connecting CounterACT Device**: The CounterACT device that communicates directly with the Nexpose Security Console. In an environment where more than one CounterACT device is assigned to a Security Console, the connecting device functions as a proxy between the Nexpose Security Console and all the CounterACT devices assigned to it, handling all queries and requests submitted by the assigned devices. The Connecting CounterACT Device is its own Assigned CounterACT Device.

**Assigned CounterACT Device**: The CounterACT device that communicates with a Nexpose Security Console through a Connecting CounterACT Device. When scans are requested by these devices, the IP addresses to be scanned must be accessible to the scan engines of the Security Console to which the devices are assigned.
**Default Security Console:** The Security Console that handles requests of all CounterACT devices not explicitly assigned to another Security Console. This may happen, for example, if new Appliances are registered with an Enterprise Manager, but are not yet assigned to a specific Security Console.

**Considerations**

Consider the following when mapping CounterACT devices to Nexpose Security Consoles:

- **Firewalls** Ensure that your firewall configurations allow connections between each Nexpose Security Console and its selected Connecting CounterACT Device.

- **Multiple Time Zones:** In situations where there are multiple CounterACT devices and Security Consoles deployed across multiple time zones, all devices and Security Consoles should use the same NTP server, and regularly synchronize their clocks. Proper synchronization is required when resolving scanner attributes.

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

- **IP Address Ranges:** Verify that the Nexpose Security Console handles at least the same IP addresses as the CounterACT devices assigned to it. To see IP address assignments to CounterACT devices, in the Console, select **Tools > Options** and then select **CounterACT Devices**. Double-click the device and select the IP Assignments tab.
• **Scan Engine Assignments:** For efficient use of scan resources, use the Nexpose Security Console interface to assign a scan engine to each endpoint, taking into consideration load balance and network partitioning implications.

• **Sites:** A unique scan site is created for every scan the Forescout platform initiates. These sites can be identified on the Nexpose Security Console interface by a unique prefix. See step 6 in Add a Nexpose Security Console. Sites for Forescout-platform-initiated scans are deleted by default when the scan completes. You can change the default behavior when the scan is launched. See Start Nexpose Scan.

• **Vulnerability Tracking:** For proper Risk Score comparison, all scans reported to the Forescout platform must use Nexpose scan policies that assess the same vulnerabilities. By default, the Forescout platform looks at results of scans that only it triggered. If other scans are reported to the Forescout platform, ensure that they use compatible scan templates.

**What to Do**

Perform the following steps to set up the integration:

- Verify that all requirements are met. See Requirements.
- Download and install the module. See Install the Module.
- Map CounterACT devices to Nexpose Security Consoles. See Configure the Module.
- Run the Forescout platform policies that detect and manage endpoints managed by a Nexpose Security Console. See Create Rapid7 Nexpose Policies Using Templates.

**Requirements**

Verify that the following requirements are met:

- Forescout Requirements
- Supported Vendor Requirements
- Forescout eyeExtend (Extended Module) Licensing Requirements

**Forescout Requirements**

The following Forescout releases can work with this module:

- Forescout version 8.2.
- A module license for Forescout eyeExtend for Rapid7 Nexpose. 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.

Supported Vendor Requirements

- Nexpose Security Console version 6.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](#).

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.

![Example Module License Request - Step 3 of 4](image)

**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.

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

Configure the module to:

− Map CounterACT Appliances and Enterprise Managers to specific Nexpose Security Consoles.

− Define settings, such as how frequently the Forescout platform polls the Security Consoles for new scan results.

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

To configure the module:

1. In the Console, select Options from the Tools menu.

2. Select Rapid7 Nexpose in the Options tree.
3. In the Rapid7 Nexpose pane, select **Add**, **Edit**, or **Remove** to add, edit, or remove a Nexpose Security Console.

### Add a Nexpose Security Console

Enter the basic information about the Nexpose Security Console and select a Connecting CounterACT Device. You can repeat the process to add multiple Security Consoles.

**To add a Nexpose Security Console:**

1. In the Rapid7 Nexpose pane, select **Add**.
2. In the Security Console Definition pane, configure the following connection parameters:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Console Domain Name or IP Address</strong></td>
<td>Enter the Console Domain Name, a Fully Qualified Domain Name (FQDN), or the IPv4 address of the Nexpose Security Console responsible for the Forescout platform scan requests on one or more identified endpoints. The Security Console must be able to handle the IP ranges of its Connecting CounterACT Device and the Assigned CounterACT Devices.</td>
</tr>
<tr>
<td><strong>Console Communication Port</strong></td>
<td>Enter the port to use for Nexpose Security Console access. The default port is 3780.</td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td>(Optional) Enter a description of the Nexpose Security Console or a relevant comment.</td>
</tr>
<tr>
<td><strong>Nexpose User Name</strong></td>
<td>Enter the username for accessing the Nexpose Security Console. This user must have Global Administrator or Security Manager permissions for the Security Console.</td>
</tr>
<tr>
<td><strong>Nexpose Password</strong></td>
<td>Enter the password.</td>
</tr>
<tr>
<td><strong>Verify Password</strong></td>
<td>Re-enter the password to verify it.</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. |
| **Connecting CounterACT Device**  | Select the CounterACT device to communicate with the defined Nexpose Security Console. This CounterACT device manages all communication with the Security Console, including forwarding scan requests submitted to it by other CounterACT devices assigned to this Security Console, and dispatching received scan results back to the appropriate devices. |

Forescout eyeExtend for Rapid7 Nexpose 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, assign the CounterACT devices that use the defined Nexpose Security Console, communicating with it via the Connecting CounterACT Device selected in the Security Console Definition pane. Only assign CounterACT devices whose IP ranges fall entirely within the IP range that is handled by the Security Console. Each CounterACT device can be assigned to only one Security Console.

If other Security Consoles are already defined, select one of the following:

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

- **Assign specific devices**: Assign specific CounterACT devices to communicate with the Security Console through this connecting device.

If no other Security Consoles have been added to Forescout eyeExtend for Rapid7 Nexpose, all devices are assigned to this Connecting CounterACT Device by default.

5. Select **Next**.
6. In the Advanced pane, configure the following settings:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interval between scan polling results (seconds)</td>
<td>Set how frequently (in seconds) the module polls the Security Console for new scan results. The default is every 30 seconds.</td>
</tr>
<tr>
<td>Prefix for sites created by CounterACT</td>
<td>Enter the site name created for each Forescout-platform-initiated scan, based on the following format: &lt;prefix&gt;-&lt;scan template&gt;-&lt;unique ID number&gt;</td>
</tr>
<tr>
<td>Retrieve results of scans not initiated by CounterACT</td>
<td>Select this option if you want the module to periodically retrieve and evaluate the results of all scans, not just those initiated by the module. If the results of Forescout-platform-initiated scans are more recent, the results of other scans are ignored.</td>
</tr>
</tbody>
</table>

7. Select Finish.

8. Select Apply to save the configuration.

The best practice is to perform a Test after setting up a connection. See Test the Module Configuration.

Test the Module Configuration

Test the module configuration to:

- Verify connection between the module and a Nexpose Security Console.
- Verify that the Forescout platform has permissions to create and delete sites in the selected Nexpose Security Console.

If the module is started or restarted, the test is not available until the module finishes initializing. This can take up to one minute.
To test the connection:

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

2. Select **Modules**.

3. In the Modules pane, select **Rapid7 Nexpose**. If the module is not running on the required Connecting CounterACT Device, select **Start**, and start the module on the device.

4. Select **Configure**.

5. Select the IP address of the Nexpose Security Console you want to test. You can select multiple Security Consoles.

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

- The test results are not always displayed in chronological order.
Export the Test Results

Test results can be exported to an external viewer in a user-friendly report 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. Enter the file name to which to export the table. For a PDF file, enter a title.

3. Control which information is exported by selecting Selected rows only or Displayed columns only.

4. Select OK. The table creation confirmation dialog box opens with the file location and a prompt to open the table.

5. To open the table, select Yes. The table is opened in a Microsoft® Office Excel® spreadsheet or PDF document.

Create Rapid7 Nexpose Policies Using Templates

Forescout eyeExtend for Rapid7 Nexpose provides policy templates that you can use to detect, manage and remediate endpoints in a Nexpose environment.

This section describes how to use Rapid7 Nexpose templates to create policies to detect and manage endpoints. Refer to the following sections:

- Create a Nexpose Basic Scan Trigger Policy, which triggers a Nexpose scan request.
- Create a Nexpose Risk Score Ranking Policy, which organizes endpoints into groups based on the Nexpose risk scores of their detected vulnerabilities.
- Create a CVSS Severity Ranking Policy, which organizes endpoints into groups based on the Nexpose severity rankings of their detected vulnerabilities.
It is recommended that you have a basic understanding of the Forescout platform policies before working with the templates. See the Forescout Templates and Policy Management chapters of the Forescout Administration Guide.

Create a Nexpose Basic Scan Trigger Policy

A Nexpose Basic Scan Trigger Policy triggers a Nexpose scan request using 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 Nexpose did not provide results for the last scan, and that scan was run more than 3 hours ago.
- Scan template to be launched: Asset Configuration Export

Before determining if a scan request will be triggered, the policy sub-rules verify that:

- The module and the Nexpose Security Console are connected.
- A Nexpose scan of the endpoint is not currently running.
- A Nexpose scan of the endpoint has not finished within the last 30 minutes.
The Nexpose Basic Scan Trigger policy template provides basic scan triggering capacity. You can update the defaults as required and can further customize the 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 for an endpoint when it detects that specific applications were installed or specific registry keys were changed. You should have a basic understanding of the Forescout platform polices to carry out these changes.

**To create a policy:**

1. Log in to the Console and select **Policy**.
2. Select **Add** from the Policy Manager. The Policy Wizard opens.
3. Expand the **Rapid7 Nexpose** folder and select **Nexpose Basic Scan Trigger**.
4. Select **Next**.
5. Accept the default name or create a new name, and add a description (optional).

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.
The sub-rules are predefined to detect if there is a connection to the Security Console, the time elapsed since the last scan and receipt of scan results, and the maximum scan delay on endpoints within the policy scope. A scan request is triggered on any endpoint that meets the default requirements.

10. Select Finish to add the policy.

Create a Nexpose Risk Score Ranking Policy

Use the Nexpose Risk Score Ranking policy template to create a policy that organizes endpoints into the following groups based on the Nexpose risk scores of their detected vulnerabilities:

- Risk Score: above 10000
- Risk Score: 7001-10000
- Risk Score: 3001-7000
- Risk Score: 1-3000
- Risk Score: 0
You can later use these groups in the Forescout platform policies to control hosts. For example, assign endpoints in the Nexpose Risk Score: above 10000 group to an isolated VLAN.

Optional remediation 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 **Policy**.
2. Select **Add** from the Policy Manager. The Policy Wizard opens.
3. Expand the **Rapid7 Nexpose** folder and select **Nexpose Risk Score Ranking**.
4. Select **Next**.
5. Accept the default name or create a new name, and add a description (optional).

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. The sub-rules instruct the Forescout platform how to detect and handle endpoints. The sub-rules are predefined to detect risk levels on endpoints within the policy scope, and assign them to the appropriate group.

The policy wizard includes optional actions that are disabled by default. These optional actions instruct the Forescout platform to notify the Forescout administrator that vulnerabilities were found and send a Syslog message indicating that vulnerabilities were found. Double-click a sub-rule to enable these actions.

11. Select Finish to add the policy.

Create a CVSS Severity Ranking Policy

Use the CVSS Severity Ranking policy template to create a policy that organizes endpoints into groups of Critical, Severe, Moderate, or No Vulnerabilities, based on the CVSS severity rankings of their detected vulnerabilities.
You can later use these groups in the Forescout platform policies to control hosts. For example, assign endpoints in the CVSS Severity Critical group to an isolated VLAN.

Optional remediation 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 **Policy**.
2. Select **Add** from the Policy Manager. The Policy Wizard opens.
3. Expand the **Rapid7 Nexpose** folder and select **CVSS Severity Ranking**.
4. Select **Next**.
5. Accept the default name or create a new name, and add a description (optional).

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**.
The sub-rules instruct the Forescout platform how to detect and handle endpoints. The sub-rules are predefined to detect severity rankings on endpoints within the policy scope, and assign them to the appropriate group.

10. The policy wizard includes optional actions that are disabled by default. These optional actions instruct the Forescout platform to notify the Forescout administrator that vulnerabilities were found, and send a Syslog message indicating that vulnerabilities were found. Double-click a sub-rule to enable these actions.

11. Select Finish to add the policy.

Create Custom Forescout Platform Policies

In addition to the bundled Forescout properties and actions available for detecting and handling endpoints, you can work with Rapid7 Nexpose related properties to create custom policies. These items are available when you install the module.

Custom Forescout platform policy tools provide you with an extensive range of options for detecting and handling endpoints. Specifically, use the policy tools to instruct the Forescout platform to apply a policy action to hosts that match (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 and select Policy.
2. Add or edit a policy.
Detect Vulnerabilities - Policy Properties

The Forescout platform policy properties let you detect hosts 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 Rapid7 Nexpose properties:

1. Open the policy Conditions dialog box.
2. Expand the Rapid7 Nexpose folder in the Properties tree. The following properties are available:
   - Nexpose Connection Is Up
   - Nexpose Risk Score
   - Nexpose Scan Results
   - Nexpose Scan Status

Nexpose Connection Is Up

This property indicates whether the Nexpose Security Console is connected to the module and responded to the Forescout platform's requests.

Nexpose Risk Score

This property indicates the vulnerability risk score calculated by Nexpose for the endpoint. Use this property to detect endpoints with specific risk score value(s).

The Nexpose Risk Score adjusts the CVSS score based on contextual elements such as time factors and governance parameters. This provides greater insight into overall risk posture. The Nexpose Risk Score lets you more accurately compare risks against one another when you prioritize deployment of resources for risk reduction.

The Nexpose Risk Score is calculated using CVSS metrics and Exposure and Exploit data from other Rapid7 Nexpose components. Refer to the following:
Nexpose Scan Results
This property indicates the results of the latest successful scan of an endpoint.
<table>
<thead>
<tr>
<th><strong>Vulnerability Title</strong></th>
<th>Indicates the descriptive name assigned by Nexpose to the specific vulnerability.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Vulnerability ID</strong></td>
<td>Indicates the ID of the detected vulnerability.</td>
</tr>
<tr>
<td><strong>Port</strong></td>
<td>Indicates the TCP/UDP port of the scanned host.</td>
</tr>
<tr>
<td><strong>Nexpose PCIv1.1 Severity Ranking</strong></td>
<td>Indicates the severity of the vulnerability as estimated by version 1.1. of the PCI protocol:</td>
</tr>
<tr>
<td><strong>Level</strong></td>
<td><strong>Severity</strong></td>
</tr>
<tr>
<td>5</td>
<td>Urgent</td>
</tr>
<tr>
<td>4</td>
<td>Critical</td>
</tr>
<tr>
<td>3</td>
<td>High</td>
</tr>
<tr>
<td>2</td>
<td>Medium</td>
</tr>
<tr>
<td>1</td>
<td>Low</td>
</tr>
<tr>
<td><strong>CVE ID</strong></td>
<td>Indicates the CVE ID associated with the detected vulnerability.</td>
</tr>
<tr>
<td><strong>CVSS Score</strong></td>
<td>Indicates the CVSS base score of the detected vulnerability, rounded to the nearest whole number.</td>
</tr>
<tr>
<td><strong>CVSS Severity</strong></td>
<td>Indicates the severity of the vulnerability, based on the CVSS score which ranges from 0 to 10:</td>
</tr>
<tr>
<td></td>
<td>▪ Moderate: CVSS score less than 4</td>
</tr>
<tr>
<td></td>
<td>▪ Severe: CVSS score of 4 or greater, but less than 8</td>
</tr>
<tr>
<td></td>
<td>▪ Critical: CVSS score of 8-10</td>
</tr>
<tr>
<td><strong>PCI Compliance</strong></td>
<td>Indicates whether the detected vulnerability does or does not affect Payment Card Industry (PCI) compliance.</td>
</tr>
<tr>
<td><strong>Scan Template Name</strong></td>
<td>Indicates the Nexpose template name used for the scan.</td>
</tr>
<tr>
<td><strong>Scan Completion Time</strong></td>
<td>Indicates the time the last Nexpose scan was completed.</td>
</tr>
</tbody>
</table>
Nexpose Scan Status

This property indicates the status of scans initiated by the Forescout platform on an endpoint.

<table>
<thead>
<tr>
<th>Scan Template Name</th>
<th>The name of the Nexpose template used for the scan.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scan Status</td>
<td>The scan status reported by Nexpose:</td>
</tr>
<tr>
<td></td>
<td>• Aborted</td>
</tr>
<tr>
<td></td>
<td>• Disposed</td>
</tr>
<tr>
<td></td>
<td>• Error</td>
</tr>
<tr>
<td></td>
<td>• Finished</td>
</tr>
<tr>
<td></td>
<td>• Integrating</td>
</tr>
<tr>
<td></td>
<td>• Paused</td>
</tr>
<tr>
<td></td>
<td>• Running</td>
</tr>
<tr>
<td></td>
<td>• Stopped</td>
</tr>
<tr>
<td></td>
<td>• Unknown</td>
</tr>
</tbody>
</table>
The most recent time that a scan was successfully launched, regardless of its current status.

- The Scan Template Name is available for Forescout-platform-initiated scans only.

Scan Endpoints - Policy Actions

The Forescout platform 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 Forescout actions available for handling endpoints, you can work with the Nexpose related action to create custom policies. This action is available when you install the module.

Scan Initiation Fields

The following information is used for Forescout-platform-initiated scans:

<table>
<thead>
<tr>
<th>Information for Scan</th>
<th>Information Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asset(s) to Be Scanned</td>
<td>Determined by the Forescout platform.</td>
</tr>
<tr>
<td>Security Console IP and user credentials</td>
<td>User-defined in the Forescout platform for the CounterACT device to which the asset is assigned. If none is defined for the CounterACT device, the default set in the Forescout platform is used.</td>
</tr>
<tr>
<td>Scan Engine Name</td>
<td>User-selected in the Security Console interface for the asset to be scanned. A default is set in the Security Console if none is defined for the asset.</td>
</tr>
<tr>
<td>Scan Template Name</td>
<td>User-selected in the Forescout platform for each scan request.</td>
</tr>
<tr>
<td>Scan Schedule</td>
<td>User-defined in the Forescout platform.</td>
</tr>
</tbody>
</table>

Start Nexpose Scan

In the Action dialog box, expand Audit and select **Start Nexpose Scan** to trigger a scan when specified policy conditions are met. For example, create a policy that detects if specific applications were installed on an endpoint or if specific registry keys were changed, and launch a scan when an endpoint meets the condition.
To set the Start Nexpose Scan action parameters:

1. In the Parameters tab, select the Nexpose template to be used for the scan. The selected option indicates that the site created by the Forescout platform for the scan will be removed from the Security Console when the scan completes.

2. In the Schedule tab, define when the scan will start.

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

Use Rapid7 Nexpose

This section covers how to use Forescout eyeExtend for Rapid7 Nexpose.
Display Nexpose Inventory Events

Use the Forescout Asset Inventory to view aggregate information for each of the Rapid7 Nexpose properties, such as vulnerability ID, risk factor, and CVE information. You can browse the inventory to learn which vulnerability information was detected on each endpoint, and on how many endpoints a specific vulnerability 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.

*The Scan Template Name is displayed as N/A if the scan was not originated by the Forescout platform.*

**To access the Asset Inventory:**

1. Log in to the Console and select **Asset Inventory**.
2. In the Views pane, navigate to the **Rapid7 Nexpose** entries.
The following views are available:

- **Nexpose Scan Results** - Displays specific results from the most recent scans for each endpoint.

- **Nexpose Scan Status** - Displays 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 Nexpose scans initiated by the Forescout platform.

In addition, you can filter the display based on the groups into which Nexpose policies sort endpoints.
For information about how to work with the Asset Inventory, refer to *Working on the Console > Working with Inventory Detections* in the Forescout Administration Guide or the Console Online Help.

### Use the Nexpose Site Deletion Tool

Forescout eyeExtend for Rapid7 Nexpose provides a new CLI that lets users delete sites that the Forescout platform created in bulk in Nexpose Security Console.

To use the Nexpose site deletion CLI tool:
- Run the following command:
  
  \[ \text{fstool r7nexpose_delete_sites [number\{m|h|d\}]} \]
  
  [Where \( m \) stands for minutes, \( h \) for hours and \( d \) for days.]

  If no \([\text{number}\{m|h|d\}]\) parameter is provided, the module deletes all sites created in the last 24 hours.

<table>
<thead>
<tr>
<th>Example</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>\text{fstool r7nexpose_delete_sites 7d}</td>
<td>Deletes sites created by the Forescout platform since the last 7 days.</td>
</tr>
<tr>
<td>\text{fstool r7nexpose_delete_sites}</td>
<td>Deletes sites created by the Forescout platform within the last 24 hours (default).</td>
</tr>
</tbody>
</table>

The commands can be run on any CounterACT Appliance that has Forescout eyeExtend for Rapid7 Nexpose installed, and are executed according to the configuration of the corresponding Connecting CounterACT Appliance.

This tool only deletes sites whose name has the same prefix as defined in the device configuration.

### Additional Forescout Documentation

For information about other Forescout features and modules, refer to the following resources:
- [Documentation Downloads](#)
- [Documentation Portal](#)
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.