ForeScout® Extended Module for Rapid7 Nexpose

Configuration Guide

Version 1.2
**Table of Contents**

**About the Rapid7 Nexpose Integration** ............................................................... 4
  Use Cases ........................................................................................................... 4
  Initiate Nexpose Scan of Suspect Endpoints Identified by CounterACT ............ 4
  Enriched Endpoint Data Context ..................................................................... 4
  Leverage Nexpose Risk Scoring Expertise ....................................................... 5
  Automated Response to Nexpose Scan Results with CounterACT Actions ........ 5
  Additional Rapid7 Nexpose Documentation ..................................................... 5

**About the Rapid7 Module** .............................................................................. 5
  Concepts, Components, Considerations .......................................................... 6
    Concepts ........................................................................................................... 6
    Components ..................................................................................................... 7
    Considerations ................................................................................................. 8

**What to Do** ..................................................................................................... 9

**Requirements** ................................................................................................ 9
  CounterACT Software Requirements ............................................................... 9
  About Support for Dual Stack Environments .................................................. 9
  Supported Vendor Requirements ..................................................................... 10
  ForeScout Extended Module License Requirements ....................................... 10
    Per-Appliance Licensing Mode ...................................................................... 10
    Centralized Licensing Mode ......................................................................... 12
    More License Information ............................................................................ 12

**Install the Module** ......................................................................................... 12

**Configure the Module** .................................................................................. 13
  Add a Nexpose Security Console .................................................................... 14

**Test the Module Configuration** ..................................................................... 17
  Exporting the Test Results .............................................................................. 19

**Run Rapid7 Nexpose Policy Templates** .......................................................... 19
  Nexpose Basic Scan Trigger Policy Template ............................................... 20
  Nexpose Risk Score Ranking Policy Template .............................................. 23
  CVSS Severity Ranking Policy Template ......................................................... 26

**Create Custom CounterACT Policies** ............................................................ 29
  Detect Vulnerabilities - Policy Properties ...................................................... 30
  Nexpose Connection Is Up .............................................................................. 30
  Nexpose Risk Score ......................................................................................... 30
  Nexpose Scan Results ..................................................................................... 31
  Nexpose Scan Status ....................................................................................... 33
  Scan Endpoints - Policy Actions ..................................................................... 34
Scan Initiation Fields ................................................................. 34
Start Nexpose Scan ................................................................. 34

Using Rapid7 Nexpose ............................................................... 35
Display Nexpose Inventory Events .............................................. 35
Using the Nexpose Site Deletion Tool ........................................ 37

Additional CounterACT Documentation .................................... 38
Documentation Downloads ....................................................... 38
Documentation Portal .............................................................. 39
CounterACT Help Tools ............................................................ 39
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.

ForeScout® 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 Extended Module for Rapid7 Nexpose integration lets you harness real-time network visibility and control capabilities in CounterACT® 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 Module.

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

Initiate Nexpose Scan of Suspect Endpoints Identified by CounterACT

CounterACT 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, CounterACT 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 CounterACT environment. CounterACT 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 CounterACT. 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 CounterACT 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 CounterACT Actions

CounterACT 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, CounterACT 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 Module

The ForeScout CounterACT® Rapid7 Nexpose Module lets you integrate CounterACT with Nexpose Security Consoles so you can:

- Trigger Nexpose endpoint scan requests based on network activity detected by CounterACT. 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 certain time frame. See Nexpose Basic Scan Trigger Policy Template.
- Organize endpoints into CounterACT groups based on the Nexpose risk scores or severity rankings of their detected vulnerabilities. See Nexpose Risk Score Ranking Policy Template and CVSS Severity Ranking Policy Template. 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 CounterACT Asset Inventory to see which endpoints have been identified as vulnerable by the module. Use standard CounterACT 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 CounterACT policies and other basic features work.

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

## Concepts, Components, Considerations

This section provides a basic overview of Rapid7 Nexpose / CounterACT architecture:

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

### 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 any one 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

**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, on the CounterACT Console select **Tools**, select **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 CounterACT 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 CounterACT-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 CounterACT must use Nexpose scan templates that assess the same vulnerabilities. By default, CounterACT looks at results of scans that only it triggered. If other scans are reported to CounterACT, ensure that they use compatible scan templates.

What to Do

- Verify that 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 CounterACT policies that detect and manage endpoints managed by a Nexpose Security Console. See Run Rapid7 Nexpose Policy Templates.

Requirements

This section describes:

- CounterACT Software Requirements
- Supported Vendor Requirements
- ForeScout Module License Requirements

CounterACT Software Requirements

The following CounterACT releases can work with this module:

- CounterACT version 8.0.

About Support for Dual Stack Environments

CounterACT version 8.0 detects endpoints and interacts with network devices based on both IPv4 and IPv6 addresses. However, IPv6 addresses are not yet supported by this component. The functionality described in this document is
based only on IPv4 addresses. IPv6-only endpoints are typically ignored or not detected by the properties, actions, and policies provided by this component.

**Supported Vendor Requirements**

Nexpose Security Console version 6.x.

**ForeScout Extended Module License Requirements**

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

- **Per-Appliance Licensing Mode**
- **Centralized Licensing Mode**

**Identifying Your Licensing Mode in the Console**

If your Enterprise Manager has a ForeScout CounterACT license listed in the Console, your deployment is operating in Centralized Licensing Mode. If not, your deployment is operating in Per-Appliance Licensing Mode.

Select Options > Licenses to see whether you have a ForeScout CounterACT license listed in the table.

Contact your ForeScout representative if you have any questions about identifying your licensing mode.

**Per-Appliance Licensing Mode**

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

If you would like to continue exploring the module before purchasing a permanent license, you can request a demo license extension. Consult with your ForeScout representative before requesting the extension. You will receive email notification and alerts at the Console before the demo period expires.
When the demo period expires, you will be required to purchase a permanent module license. In order to continue working with the module, you must purchase the license.

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

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

**Requesting a License**

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

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

To view the number of currently detected devices:

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

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

- No demo license is automatically installed during system installation.

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

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

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

More License Information

Refer to the CounterACT Administration Guide for information on Extended Module licenses. You can also contact your ForeScout representative or license@forescout.com for more information.

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 - Centralized Licensing Mode

   To find out which licensing mode your deployment is working with, see Identifying Your Licensing Mode in the Console.

2. Download the module .fpi file.

3. Save the file to the machine where the CounterACT Console is installed.

4. Log into the CounterACT Console and select Options from the Tools menu.

5. Select Modules. The Modules pane opens.
6. Select **Install**. The Open dialog box opens.
7. Browse to and select the saved module .fpi file.
8. Select **Install**. The Installation screen opens.
9. Select **I agree to the License Agreement** to confirm that you have read and agree to the terms of the License Agreement, and select **Install**. The installation will not proceed if you do not agree to the license agreement.

   - **The installation will begin immediately after selecting Install, and cannot be interrupted or canceled.**

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

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

   - **Some components are not automatically started following installation.**

### Identifying Your Licensing Mode in the Console

If your Enterprise Manager has a **ForeScout CounterACT** license listed in the Console, your deployment is operating in Centralized Licensing Mode. If not, your deployment is operating in Per-Appliance Licensing Mode.

Select **Options > Licenses** to see whether you have a **ForeScout CounterACT** license listed in the table.

![License Table](image)

Contact your ForeScout representative if you have any questions about identifying your licensing mode.

### Configure the Module

Configure the module to:

- Map CounterACT Appliances and Enterprise Managers to specific Nexpose Security Consoles.
• Define module settings, such as the frequency with which CounterACT polls the Security Consoles for new scan results.

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

To configure the module:
1. Select Options from the Console 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 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. The Add Nexpose Security Console wizard opens.
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>Nexpose Security Console IP Address</td>
<td>The IP address of the Nexpose Security Console responsible for CounterACT 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>Nexpose Security Console Communication Port</td>
<td>The port to use for Nexpose Security Console access. The default port is 3780.</td>
</tr>
<tr>
<td>Description</td>
<td>Description of the Nexpose Security Console or a relevant comment. (Optional)</td>
</tr>
<tr>
<td>Nexpose User Name</td>
<td>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>Nexpose Password</td>
<td>Password for the above user.</td>
</tr>
<tr>
<td>Verify Password</td>
<td>Retype the password to confirm it.</td>
</tr>
<tr>
<td>Connecting CounterACT Device</td>
<td>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.</td>
</tr>
</tbody>
</table>

3. Select **Next**. The **CounterACT Devices** pane opens.
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 the module, all devices are assigned to this Connecting CounterACT Device by default.

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

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Interval between scan polling results (seconds)</strong></td>
<td>How often the module polls the Security Console for new scan results. The default is every 30 seconds.</td>
</tr>
<tr>
<td><strong>Prefix for sites created by CounterACT</strong></td>
<td>A site name is created for each CounterACT-initiated scan. It takes the form: &lt;prefix&gt;-&lt;scan template&gt;-&lt;unique ID number&gt;</td>
</tr>
<tr>
<td><strong>Retrieve results of scans not initiated by CounterACT</strong></td>
<td>If selected, the module periodically retrieves and evaluates the results of all scans, not just those initiated by the module. If results of CounterACT-initiated scans are more recent, results of other scans are ignored.</td>
</tr>
</tbody>
</table>

7. Select **Finish**.
8. Select **Apply** to save the configuration.

**Test the Module Configuration**

Test the module configuration to:
- Verify connection between the module and a Nexpose Security Console.
- Verify that CounterACT has permissions to create and delete sites in the selected Nexpose Security Console.

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

1. In the CounterACT Console, select **Options** from the **Tools** menu. The Options dialog box opens.
2. Navigate to and select the **Modules** folder.
3. In the **Modules** pane, select **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**. The Rapid7 Nexpose pane opens.

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 will not always display in chronological order.
Exporting 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. A popup menu opens.
2. Select **Export Table**. The Export Table dialog box opens.
3. Enter the file name to which to export the table. For a PDF file, enter a title.
4. Control which information is exported by selecting **Selected rows only** or **Displayed columns only**.
5. Select **OK**. The table creation confirmation dialog box opens with the file location and a prompt to open the table.
6. To open the table, select **Yes**. The table is opened in a Microsoft® Office Excel® spreadsheet or PDF document.

Run Rapid7 Nexpose Policy Templates

This module provides the following policy templates that you can use to detect, manage and remediate endpoints in a Nexpose environment:

- The [Nexpose Basic Scan Trigger Policy Template](#) generates policies that trigger a Nexpose scan request.
- The [Nexpose Risk Score Ranking Policy Template](#) generates policies that organize endpoints into groups based on the Nexpose risk scores of their detected vulnerabilities.
- The [CVSS Severity Ranking Policy Template](#) generates policies that organize endpoints into groups based on the Nexpose severity rankings of their detected vulnerabilities.
It is recommended that you have a basic understanding of CounterACT policies before working with the templates. See the CounterACT Templates and Policy Management chapters of the Console User Guide.

Nexpose Basic Scan Trigger Policy Template

Use this policy to trigger 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.

This 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 CounterACT to only trigger a scan when an endpoint is detected with specific properties. For example, instruct CounterACT to trigger a scan request for an endpoint when it detects that certain applications were installed or certain registry keys were changed. You should have a basic understanding of CounterACT polices to carry out these changes.
To use the Nexpose Basic Scan Trigger policy template:

1. Log in to the CounterACT Console and select the Policy tab.
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. The Name pane opens.
5. Accept the default name or create a new name, and add a description (optional).

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

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

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 appears in the Scope pane.

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

**Nexpose Risk Score Ranking Policy Template**

Use this policy to organize endpoints into the following CounterACT 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 CounterACT 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 CounterACT administrator that vulnerabilities were found.
- Send a Syslog message indicating that vulnerabilities were found.

These actions are disabled by default.

**To use the Risk Score Ranking policy template:**

1. Log in to the CounterACT Console and select the **Policy** tab.
2. Select **Add** from the Policy Manager. The Policy Wizard opens.
3. Expand the **Rapid7 Nexpose** folder and select **Nexpose Risk Score Ranking**. The Policy Type window opens.

   - **Nexpose Risk Score Ranking**
     
     Use this template to create a CounterACT policy that ranks the most current Nexpose Plugin Risk Scores assigned to network endpoints. The policy organizes endpoints into categories based on their Nexpose Plugin Risk Scores. You can change the policy's default categories.
     
     Optional remediation actions can be used to:
     - Notify the CounterACT administrator of high-risk scores.
     - Send a Syslog message indicating high-risk scores.
     
     These actions are disabled by default.

4. Select **Next**. The Name pane opens.
5. Accept the default name or create a new name, and add a description (optional).

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

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

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 appears in the Scope pane.

9. Select **Next**. The Sub-Rules pane opens.
10. The sub-rules instruct CounterACT 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 CounterACT to notify the CounterACT 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.

**CVSS Severity Ranking Policy Template**

Use this policy to organize endpoints into CounterACT 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 CounterACT 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 CounterACT administrator that vulnerabilities were found.
- Send a Syslog message indicating that vulnerabilities were found.

These actions are disabled by default.

**To use the CVSS Severity Ranking policy template:**

1. Log in to the CounterACT Console and select the **Policy** tab.
2. Select **Add** from the Policy Manager. The Policy Wizard opens.
3. Expand the Rapid7 Nexpose folder and select **CVSS Severity Ranking**. The Policy Type window opens.

4. Select **Next**. The Name pane opens.
5. Accept the default name or create a new name, and add a description (optional).

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

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

![IP Address Range dialog box](image)

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 appears in the Scope pane.

9. Select **Next**. The Sub-Rules pane opens.
The sub-rules instruct CounterACT 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 CounterACT to notify the CounterACT 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 CounterACT Policies

In addition to the bundled CounterACT 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 CounterACT policy tools provide you with an extensive range of options for detecting and handling endpoints. Specifically, use the policy tools to instruct CounterACT 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 CounterACT Console and select the Policy tab.
2. Add or edit a policy.
Detect Vulnerabilities - Policy Properties

CounterACT policy properties let you detect hosts with specific attributes. For example, create a policy that instructs CounterACT to detect endpoints running a certain operating system or having a certain 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 CounterACT 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. See https://help.rapid7.com/nexpose/en-us/Files/Risk_scoring_FAQ.html

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>Nexpose PCIv1.1 Severity Ranking</td>
<td>Indicates the severity of the vulnerability as estimated by version 1.1. of the PCI protocol:</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>-----------------------------------------------------------------------------------------------</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>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CVE ID</th>
<th>Indicates the CVE ID associated with the detected vulnerability</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>CVSS Score</th>
<th>Indicates the CVSS base score of the detected vulnerability, rounded to the nearest whole number</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>CVSS Severity</th>
<th>Indicates the severity of the vulnerability, based on the CVSS score which ranges from 0 to 10:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Moderate: CVSS score less than 4</td>
<td></td>
</tr>
<tr>
<td>Severe: CVSS score of 4 or greater, but less than 8</td>
<td></td>
</tr>
<tr>
<td>Critical: CVSS score of 8-10</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>PCI Compliance</th>
<th>Indicates whether the detected vulnerability does or does not affect Payment Card Industry (PCI) compliance</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Scan Template Name</th>
<th>Indicates the Nexpose template name used for the scan</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Scan Completion Time</th>
<th>Indicates the time the last Nexpose scan was completed</th>
</tr>
</thead>
</table>
Nexpose Scan Status
This property indicates the status of scans initiated by CounterACT on an endpoint.

<table>
<thead>
<tr>
<th>Scan Template Name</th>
<th>The Nexpose template name 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>Dispatched</td>
</tr>
<tr>
<td></td>
<td>Error</td>
</tr>
<tr>
<td>Last Scan Start Time</td>
<td>The most recent time that a scan was successfully launched, regardless of its current status.</td>
</tr>
</tbody>
</table>

- The Scan Template Name is available for CounterACT-initiated scans only.
Scan Endpoints - Policy Actions

CounterACT policy actions let you instruct CounterACT 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 CounterACT 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 CounterACT-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 CounterACT.</td>
</tr>
</tbody>
</table>
| Security Console IP and user credentials | User-defined in the CounterACT interface for the CounterACT device to which the asset is assigned.  
                                        | If none is defined for the CounterACT device, the default set in the CounterACT interface is used. |
| Scan Engine Name                      | 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.           |
| Scan Template Name                    | User-selected in the CounterACT interface for each scan request.                    |
| Scan Schedule                         | User-defined in the CounterACT interface.                                           |

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 certain applications were installed on an endpoint or if certain 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 checkbox indicates that the site created by CounterACT 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.

<table>
<thead>
<tr>
<th>Host</th>
<th>Actions</th>
<th>HostIP</th>
<th>MAC Address</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><img src="image" alt="Start Nexpose Scan" /></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Action triggered by: CounterACT operator</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Action Status: Unknown - Rapid7 Nexpose plugin(s) not running</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><img src="image" alt="Add to Group" /></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Action triggered by: policy Asset Classification (Mobile Devices)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Action Status: Success - Group 'Mobile devices'</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><img src="image" alt="Add to Group" /></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Action triggered by: policy Corporate/Guest Control (Guest Hosts)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Action Status: Success - Group 'Guest Hosts'</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><img src="image" alt="N/A" /></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Press 'F2' for focus</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

As with other actions in CounterACT, you can identify successful or failed actions using the CounterACT console.

Using Rapid7 Nexpose

This section covers how to use the ForeScout Extended Module for Rapid7 Nexpose.

Display Nexpose Inventory Events

Use the CounterACT 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 CounterACT.*
To access the Asset Inventory:

1. Log in to the CounterACT Console and select the **Asset Inventory** tab.
2. 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 CounterACT, and the scanned host information of the most recent Nexpose scans initiated by CounterACT.

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 CounterACT Asset Inventory, refer to *Working on the Console > Working with Inventory Detections* in the [CounterACT Administration Guide](#) or the Console Online Help.

### Using the Nexpose Site Deletion Tool

The Rapid7 Nexpose Module provides a new CLI that allows users to delete sites that CounterACT created in bulk in Nexpose Security Console.

To use the Nexpose site deletion CLI tool:

```
fstool r7nexpose_delete_sites [number{m|h|d}]
```

[Where m stands for minutes, h for hours and d for days.]

If no `[number{m|h|d}]` parameter is provided, the module will delete all sites created since the last 24 hours.

<table>
<thead>
<tr>
<th>Example</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>fstool r7nexpose_delete_sites 7d</code></td>
<td>Will delete sites created by CounterACT since the last 7 days.</td>
</tr>
<tr>
<td><code>fstool r7nexpose_delete_sites</code></td>
<td>Will delete sites created by CounterACT within the last 24 hours (default).</td>
</tr>
</tbody>
</table>

The commands can be run on any CounterACT appliance that has the Rapid7 Nexpose module installed, and will be executed according to the configuration of the corresponding Connecting CounterACT appliance.

This tool will only delete sites whose name has the same prefix as defined in the device configuration panel:
Additional CounterACT Documentation

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

- Documentation Downloads
- Documentation Portal
- CounterACT Help Tools

Documentation Downloads

Documentation downloads can be accessed from one of two ForeScout portals, depending on which licensing mode your deployment is using.

- **Per-Appliance Licensing Mode** - Product Updates Portal
- **Centralized Licensing Mode** - Customer Portal

Software downloads are also available from these portals.

To learn which licensing mode your deployment is using, see Identifying Your Licensing Mode in the Console.

Product Updates Portal

The Product Updates Portal provides links to CounterACT version releases, Base and Content Modules, and Extended Modules, as well as related documentation. The portal also provides a variety of additional documentation.
To access the Product Updates Portal:
2. Select the CounterACT version you want to discover.

Customer Portal
The Downloads page on the ForeScout Customer Portal provides links to purchased CounterACT version releases, Base and Content Modules, and Extended Modules, as well as related documentation. Software and related documentation will only appear on the Downloads page if you have a license entitlement for the software. The Documentation page on the portal provides a variety of additional documentation.

To access documentation on the ForeScout Customer Portal:
2. Select Downloads or Documentation.

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

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

To access the Documentation Portal:
2. Use your customer support credentials to log in.
3. Select the CounterACT version you want to discover.

CounterACT Help Tools
Access information directly from the CounterACT Console.

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

CounterACT Administration Guide
Select CounterACT Help from the Help menu.

Plugin Help Files
1. After the plugin is installed, select Options from the Tools menu and then select Modules.
2. Select the plugin and then select Help.

Documentation Portal
Select Documentation Portal from the Help menu.
Identifying Your Licensing Mode in the Console

If your Enterprise Manager has a *ForeScout CounterACT See* license listed in the Console, your deployment is operating in Centralized Licensing Mode. If not, your deployment is operating in Per-Appliance Licensing Mode.

Select **Options > Licenses** to see whether you have a *ForeScout CounterACT See* license listed in the table.

Contact your ForeScout representative if you have any questions about identifying your licensing mode.
Legal Notice

© 2018 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.

2018-04-10 09:21