ForeScout® Extended Module for IBM® QRadar®
Configuration Guide

Version 2.1
# Table of Contents

## About IBM QRadar Integration

- Use Cases ................................................................. 4
  - Visualization of CounterACT Endpoint Compliance Status & Connectivity .... 4
  - Agent Health and Compliance for Windows ........................................... 4
  - Generate IBM QRadar Offense to Drive CounterACT Action .................... 4
  - Right-click to Trigger CounterACT Action .............................................. 5
  - Continuous Posture Tracking ................................................................. 5

## About this Module ........................................................ 5

- How It Works ...................................................................... 6
  - Communicate Host and Policy Status .................................................... 6
  - What to Do ........................................................................... 6

## Requirements .................................................................... 7

- CounterACT Software Requirements ........................................... 7
- About Support for Dual Stack Environments ................................. 7
- ForeScout Extended Module License Requirements ....................... 7
  - Per-Appliance Licensing Mode ........................................................... 8
  - Centralized Licensing Mode ............................................................... 9
  - More License Information ................................................................. 10
- 3rd-Party Vendor Requirements .................................................. 10

## Install the Module ............................................................ 10

- Configure the Module ................................................................ 12
- Define Target IBM QRadar SIEM Servers .................................... 12
  - Edit Server Target ........................................................................ 15
  - Delete Server Targets .................................................................... 15
- Include Syslog Message Header .................................................. 15
- Install the ForeScout App for IBM QRadar into IBM QRadar ........... 16
- Create a Service .......................................................................... 18
- Insert the Authorized Service Token .......................................... 19
- Send Data from CounterACT to IBM QRadar ............................. 20
- Verify Configurations .................................................................. 22

## Run IBM QRadar Policy Templates ....................................... 22

- Action on Disposition Policy Template .......................................... 23
- Action on Offense by Credibility and Severity Policy Template ........ 28
- Action on Offense by Description Policy Template .......................... 32
- Send SIEM Updates Policy Template ............................................. 35
- WinCollect Agent Compliance Policy Template ............................ 37
Create Custom IBM QRadar Policies ......................................................... 42
  Policy Properties .................................................................................. 43
  Policy Actions ...................................................................................... 44
  Send Data from CounterACT to IBM QRadar ........................................ 45

Using the ForeScout Extended Module for QRadar .............................. 47
  Integrate the ForeScout Functionalities into IBM QRadar ................. 47
  View Widget Details ............................................................................ 48
  Customize the Display of the Dashboard ............................................ 49
  Display Inventory Data ........................................................................ 49

Additional CounterACT Documentation .............................................. 50
  Documentation Downloads ................................................................. 50
  Documentation Portal ......................................................................... 50
  CounterACT Help Tools ...................................................................... 51
About IBM QRadar Integration

ForeScout CounterACT® integrates with IBM QRadar SIEM servers to provide complete visibility of network endpoints, including unmanaged endpoints. QRadar integration lets you send policy status and selected host information from CounterACT to QRadar SIEM servers and trigger CounterACT actions based on SIEM messages.

Use Cases

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

- Visualization of CounterACT Endpoint Compliance Status & Connectivity
- Agent Health and Compliance for Windows
- Generate IBM QRadar Offense to Drive CounterACT Action
- Right-click to Trigger CounterACT Action
- Continuous Posture Tracking

Visualization of CounterACT Endpoint Compliance Status & Connectivity

An IBM QRadar security administrator can monitor the current security posture on the IBM QRadar dashboard as per the configurations of different security solutions deployed. The security administrator can add CounterACT widgets to the dashboard. These widgets cover the following visualization scenarios:

- Endpoint compliance status summaries
- Registered corporate users vs. guests
- Device types in the network
- Patterns of network access over time

Agent Health and Compliance for Windows

An IBM QRadar security administrator can ensure that the IBM QRadar WinCollect agent is installed and functioning properly on Windows endpoints within the network. An IBM QRadar WinCollect agent is a Windows Log Collection Agent, a stand-alone Windows application that is installed on both the IBM QRadar machine and the Windows host to allow IBM QRadar to collect Windows-based events.

Generate IBM QRadar Offense to Drive CounterACT Action

An organization uses a network firewall to detect targeted Denial of Service (DOS) attacks on their web applications. The same organization also has IBM QRadar SIEM to collect and aggregate logs from ForeScout CounterACT, firewall, and web applications. When IBM QRadar detects a targeted DOS attack via firewall log correlation, an Offense is generated. The security administrator would then have the
source of the attack automatically blocked by the firewall to prevent further disruption of service to the application(s) on the network.

**Right-click to Trigger CounterACT Action**

In QRadar, you can right-click on any IP address/MAC field to send action type to CounterACT. CounterACT sets properties and triggers policies to take action. For more information, see the *ForeScout App for IBM QRadar How-To-Guide*.

**Continuous Posture Tracking**

In the ForeScout Extended Module for IBM QRadar, the operator can add widgets into the QRadar Dashboard. This gives an overall, big-picture view of device types, compliance status, registered corporate/guest status and network patterns on the network. For more information, see the *ForeScout App for IBM QRadar How-To-Guide*.

**Connecting Appliance Option added to Configuration Setup**

When adding a QRadar SIEM server, the operator can select the CounterACT appliance to communicate between the IBM QRadar SIEM server and the assigned CounterACT devices. For more information, see *Define Target IBM QRadar SIEM Servers*.

**Additional IBM QRadar Documentation**

Refer to online documentation for more information about the IBM QRadar solution:


**About this Module**

CounterACT integrates with IBM QRadar SIEM servers to provide complete visibility of network endpoints, including unmanaged endpoints. IBM QRadar integration lets you send policy status and selected host information from CounterACT to IBM QRadar SIEM servers and trigger CounterACT actions based on SIEM messages.

The ForeScout Extended Module for IBM QRadar integrates CounterACT and IBM QRadar so that you can:

- Use policies and actions provided by the IBM QRadar Module to regularly push endpoint data to IBM QRadar. See details of the *Send SIEM Updates* policy template.
- View CounterACT data in a dedicated, customizable IBM QRadar dashboard. See *Integrate the ForeScout Functionalities into IBM QRadar*.
- Define CounterACT policies that respond to IBM QRadar offenses. See *Action on Offense by Description* and *Action on Offense by Credibility and Severity*. 
Configure IBM QRadar to send offenses to CounterACT based on custom search or report results. Offenses can combine data from multiple sources. See Send Data from CounterACT to IBM QRadar.

It is suggested you install and configure both CounterACT and IBM QRadar to work with the features described in this document. For example, CounterACT policies and actions provided by the IBM QRadar module are used to populate IBM QRadar with CounterACT data.

How It Works

Two components are installed to support this integration:

- The ForeScout Extended Module for IBM QRadar is installed in CounterACT.
- The ForeScout App for IBM QRadar is installed within IBM QRadar.

The result is full bi-directional integration – CounterACT can send a dynamic list of property, policy, and event information to IBM QRadar, and IBM QRadar can send offenses and other messages to CounterACT.

IBM QRadar search uses data from CounterACT and other sources to detect patterns that indicate threats.

The ForeScout Extended Module for IBM QRadar submits offenses generated by IBM QRadar to CounterACT, where it parses the offenses into host properties.

CounterACT policies examine these properties to identify endpoints in need of remediation.

Communicate Host and Policy Status

- **Policy-triggered reporting**: CounterACT sends data to IBM QRadar when the conditions of a policy are met.
- **Update-triggered reporting**: CounterACT sends data to IBM QRadar when there is a change in policy or host status.
- **Scheduled reporting**: CounterACT sends data to IBM QRadar at regular intervals, independent of management policies.

What to Do

Perform the following to carry out the integration:

- Verify that requirements are met. See Requirements for details.
- Download and install the ForeScout Extended Module for IBM QRadar from the ForeScout website: www.forescout.com/support. See Install the Module for details.
- Define target IBM QRadar SIEM servers, and assign CounterACT devices to them. See Define Target IBM QRadar SIEM Servers for details.
- Define actions in CounterACT policies that report data to IBM QRadar servers. See Policy Actions.
Requirements

This section describes:

- CounterACT Software Requirements
- ForeScout Extended Module License Requirements
- 3rd-Party Vendor Requirements

CounterACT Software Requirements

The ForeScout IBM QRadar Extended Module requires the following CounterACT releases and other CounterACT components:

- CounterACT version 8.0
- A module license for the IBM QRadar Module.
- An active Maintenance Contract for the licensed module is required.
- Core Extensions Module version 1.0 or above with the Syslog Plugin running.

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.

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.

3rd-Party Vendor Requirements

- IBM QRadar version 7.2.8
- Verify connectivity between CounterACT and target IBM QRadar servers on the configured TCP or UDP port. The default port is 514.
- ForeScout Extended Module for IBM QRadar has been tested using the following browsers:

<table>
<thead>
<tr>
<th>Web browser</th>
<th>Supported versions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mozilla Firefox</td>
<td>45.2 Extended Support Release</td>
</tr>
<tr>
<td>64-bit Microsoft Internet Explorer with Microsoft Edge mode enabled.</td>
<td>11.0</td>
</tr>
<tr>
<td>Google Chrome</td>
<td>Latest</td>
</tr>
</tbody>
</table>

- For updates or changes to QRadar-supported browsers reference, see https://www.ibm.com/support/knowledgecenter/SS42VS_7.2.8/com.ibm.qradar.doc/c_shi_browser_support_gs.html

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.

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

- *This module interacts with the ForeScout Extended Module for IBM QRadar. If you install only this module, you can send CounterACT information to IBM QRadar. However, you will need to install and configure both components to work with all the features described in this document, including bidirectional interaction with IBM QRadar.*
Configure the Module

Configure the module to ensure that CounterACT can communicate with IBM QRadar. Perform this procedure after the ForeScout Extended Module for IBM QRadar is installed on your IBM QRadar SIEM server. To complete configuration of some of these connections, you need to perform the following configuration steps on the IBM QRadar server:

- Define Target IBM QRadar SIEM Servers
- Include Syslog Message Header
- Install the ForeScout App for IBM QRadar into IBM QRadar
- Create a Service
- Insert the Authorized Service Token
- Send Data from CounterACT to IBM QRadar
- Verify Configurations

Define Target IBM QRadar SIEM Servers

For IBM QRadar reporting purposes, you will need to map CounterACT Appliances to an IBM QRadar server. Each CounterACT device communicates with a single IBM QRadar server. If you define more than one IBM QRadar server, you can assign individual CounterACT appliances to each IBM QRadar server.

To add QRadar SIEM server targets for CounterACT:

1. In the CounterACT Console’s toolbar, select Options.
2. In the left pane, select the Modules folder.
3. In the Modules pane, select QRadar SIEM Server and then select the Configure button.
4. In the QRadar SIEM pane, select Add. The Add QRadar SIEM server wizard opens.
Server Address
Specify the server address of the QRadar SIEM server. If a single SIEM server is selected, then all other CounterACT devices will proxy their endpoint updates through the selected Connecting Appliance. If multiple SIEM servers are specified, utilize the Assigned CounterACT Devices tab to assign each CounterACT device. The assigned CounterACT devices will send their managed endpoints' updates to the SIEM server through the selected Connecting Appliance.

Port
Specify the port number of the QRadar SIEM server. The default port is 514.

Server Protocol
Specify UDP or TCP as your QRadar SIEM server protocol.

Comment
(Optional) Insert text, for example, the name of the QRadar SIEM server.

Connecting Appliance
Select the CounterACT appliance to communicate between the IBM QRadar SIEM server and the assigned CounterACT devices.

5. Select Next. The Assigned CounterACT devices pane opens.

6. Choose one of the following options:
   a. Select Default Server to make this server the target for all CounterACT devices not assigned to another IBM QRadar SIEM server. Until you define more than one server, this is the only option available.
   b. Select Assign CounterACT devices and then select one or more items in the device list. The selected devices will send its managed endpoints' update to the editing SIEM server through the connecting appliance.
7. Select **Finish**. The server appears in the QRadar SIEM pane.
8. (Optional) Repeat Steps 4 through 7 to add additional QRadar servers.

For IBM QRadar High Availability (HA) deployments, add each server IP by repeating the steps above for each QRadar appliance:

- **Primary Appliance IP**
- **Secondary Appliance IP**
Virtual IP of the HA Cluster

Edit Server Target
If you need to reassign CounterACT devices to a different server, use the Edit option:

To edit a QRadar SIEM server target:
1. In the Modules pane, select the QRadar SIEM server. The QRadar SIEM pane opens.
2. Select the server then select Edit.
3. Make your edits and select OK.

Delete Server Targets

To delete a QRadar SIEM server target:
1. In the Modules pane, select the QRadar SIEM server. The QRadar SIEM pane opens.
2. Select the server and then select Remove.

Include Syslog Message Header
You can add a syslog header to all CEF messages delivered to the SIEM servers. This option may require additional configuration on the SIEM servers.

To include syslog message headers in CEF messages:
1. Select Options. The Edit General Parameters dialog box opens.
2. Select **Use Syslog transport for message delivery** and define the following fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Identity</strong></td>
<td>A string to identify the source of the syslog message (default: CounterACT)</td>
</tr>
<tr>
<td><strong>Facility</strong></td>
<td>Syslog message facility (default: local1)</td>
</tr>
<tr>
<td><strong>Priority</strong></td>
<td>Syslog message priority (default: info)</td>
</tr>
</tbody>
</table>

**Install the ForeScout App for IBM QRadar into IBM QRadar**

For greater functionality, the ForeScout App for IBM QRadar needs to be installed.

**To install the ForeScout App for IBM QRadar:**

1. Navigate to [https://exchange.xforce.ibmcloud.com/hub](https://exchange.xforce.ibmcloud.com/hub)
2. Find the ForeScout square and select it to download the zip file attachment to the local drive.
3. In IBM QRadar, select the **Admin** tab and then select **Extension Management**.

4. Select **Add**.

5. Browse to the zip file and select it.

6. You have the option to select **Install immediately** or you can install according to your company’s change policy.

7. The ForeScout Integration for IBM QRadar dialog box opens.

8. Accept the default settings and select the **Install** button. Select **OK** when finished.

9. In the **Admin** tab, the newly installed module displays as **Installed**.

10. IBM QRadar automatically runs a check for any changes.
11. If there are changes that need to be made, select the **Deploy Change** button.

12. Confirm the installation by refreshing the page and scrolling down. The ForeScout icon should display.

---

**Create a Service**

This section addresses how to create a Service for the newly-installed ForeScout Extended Module for IBM QRadar.

1. In QRadar, select **Authorized Services** in the Admin tab. The Authorized Services dialog box displays.

2. Select the **Add Authorized Services** button. The Add Authorized Service dialog box displays.

3. Enter information into the **Service Name**, **User Role**, and **Security Profile** fields.

4. It is recommended that the **No Expiry** field is checked.
5. Select **Create Service**. The new service displays in the Authorized Services list the information, including the Authorization Token.

6. **Close** the Authorized Services dialog box. QRadar automatically checks for un-deployed changes.

7. As you just added a Service, there will be un-deployed changes. Select the **Deploy Changes** button. (Note: It is required do this before proceeding.)

**Insert the Authorized Service Token**

1. You will need the token for the service you just created. In the **Admin** tab, User Management section and then select **Authorized Services**.

2. Select the newly-created service and copy the Authentication Token.

3. Close the Authorized Services dialog box.

4. In the **Admin** tab, scroll down to and select the ForeScout icon. The Authorized Service Token dialog box displays.

5. Paste the Authentication Token into the field and then select **Save**.

6. You will need to communicate with CounterACT the new Authorized Service. In the ForeScout CounterACT section, select **Add**.

7. Enter the IP address of the Connected CounterACT device, protocol, default syslog port number and any comments and then select **Save**. QRadar checks for changes that need to be deployed.

    - **Make sure this CounterACT device is set as connecting device in CounterACT configuration and the protocol setting is the same.**
8. Verify the Authorized Token(s) were saved by returning to the Admin tab and selecting the ForeScout icon.

**Send Data from CounterACT to IBM QRadar**

CounterACT can send policy and host information to IBM QRadar based on set CounterACT policy conditions, or on a regular schedule.

CounterACT policies use a wide range of host conditions to trigger various management and remediation actions. When the conditions of the policy are met, the actions are implemented. With the IBM QRadar module, CounterACT policies can include notification messages to IBM QRadar SIEM servers as an action.

To implement IBM QRadar reporting, define a CounterACT policy that includes the IBM QRadar update action. When the conditions of this policy are met, IBM QRadar notification is implemented in one of several modes:

- **One-time report** - current policy/host information is sent once when the conditions of the policy are met.
- **Update reporting** - a message is sent whenever the host information or policy status changes.
- **Periodic reporting** - a message is sent at regularly defined intervals.

The policy conditions needs to be met at least once to initiate update reporting or periodic reporting. Similarly, CounterACT stops change reporting and periodic reporting when the conditions of the policy are no longer met.

You can further modify notification behavior using standard action scheduling options.

**To create an IBM QRadar reporting action in a CounterACT policy:**

1. In the CounterACT Console, navigate to the Actions pane, select **Audit** and then select **Send Updates to QRadar SIEM Server**. The Contents tab opens in the right pane. Use this tab to determine the information that is reported to IBM QRadar for hosts in the scope of the policy.
2. To send host property values to the QRadar server, select **Send host property results**.

When new host properties are added to CounterACT plugins, Extended Module or future release of the core CounterACT software; it might be necessary use the QRadar DSM Editor to solve parsing problems and add your own custom parsing. You use the DSM Editor to extract fields, define custom properties, categorize events, and define new QID definition. For example: When ForeScout releases a new extended module, ForeScout may also introduce new host properties within that module. To utilize these new properties in the QRadar offense rules, building blocks, or widgets – users need to parse the new host property from the **Send SIEM Updates** event. See processing event data in QRadar for more information on QRadar event processing and creating custom DSMs: [https://www.ibm.com/support/knowledgecenter/en/SS42VS_7.2.8/com.ibm.qradar.doc/c_qradar_admin_data_ingestion.html](https://www.ibm.com/support/knowledgecenter/en/SS42VS_7.2.8/com.ibm.qradar.doc/c_qradar_admin_data_ingestion.html)

3. Choose an option:
   - Select **Send all** to include all properties discovered.
   - Select **Send specific** to send the values of specific properties. Choose the properties to report from the list.

4. Select **Send policy status** to send the CounterACT policy status (Match/Unmatch/Pending/Irresolvable).
   Select the **Trigger** tab. Use this tab to determine reporting behavior.

5. In the Action dialog box, choose an option(s):
   - Select **Send when the action starts** to send information once when the conditions of the policy are met.
   - Select **Send when information is updated** to send information when there is a change in the host properties you specified in the Content tab.
Select **Send periodically every** to send information at fixed intervals.

6. Select the **Schedule** tab. You can use these standard action scheduling options to further customize message delivery. For example, you can choose the **Customize action start time** option to delay message delivery, or to limit the duration of repeated or regularly scheduled messages.

7. Select **OK**.

**Verify Configurations**

1. In the CounterACT Console, select the **Asset Inventory** tab. The Views pane displays on the left.

2. In the left pane, select the **IBM QRadar icon** to expand it and then select any of the items in the list to view its properties.

| QRadar Last Offense | QRadar Last Offense lists the most recent offense that needs addressing by the QRadar user. The offense will show up in both QRadar Last Offense and QRadar Offenses. The last offense will not change until a new offense comes in or CounterACT purges it after a specific time. |
| QRadar Last Policy Trigger | “Policy Trigger” in the CounterACT Console is the same as “Disposition” in the QRadar console. Each time a disposition is selected from a QRadar user, the selected disposition triggers a policy event. |
| QRadar Offenses | QRadar Offenses lists all remediated offenses. |
| QRadar Policy Triggers | QRadar Policy Triggers lists all remediated policies / dispositions. |

3. Check that the properties match the configuration requirements.

The configuration of IBM QRadar is now complete. To use the IBM QRadar application, refer to **QRadar Documentation**. To use the ForeScout Extended Module for IBM QRadar, refer to the **ForeScout App for IBM QRadar How-To-Guide**.

**Run IBM QRadar Policy Templates**

CounterACT templates help you quickly create important, widely-used policies that easily control endpoints and can guide users to compliance. These policies can be viewed in the CounterACT Console’s Policy Manager.

CounterACT policies use a wide range of host conditions to trigger various management and remediation actions. When the conditions of the policy are met, the actions are implemented. With the ForeScout Extended Module for IBM QRadar, CounterACT policies can include notification messages to IBM QRadar SIEM servers as an action.

Predefined actions – instructions regarding how to handle endpoints – are generally disabled by default when working with templates. You should only enable actions after testing and fine-tuning the policy.
The following default policy templates are available within the ForeScout Extended Module for IBM QRadar:

- **Action on Disposition**
- **Action on Offense by Credibility and Severity**
- **Action on Offense by Description**
- **Send SIEM Updates**
- **WinCollect Agent Compliance**

**Action on Disposition Policy Template**

Use the IBM QRadar Action on Disposition policy template to apply actions to an endpoint for which CounterACT received a disposition event message from IBM QRadar. Sub-rules of the policy apply specific actions depending upon the disposition of the most recent IBM QRadar event received for the endpoint.

The sub-rules will indicate that an IBM QRadar operator or administrator has requested the following actions be taken on an endpoint identified by the disposition.

**To use the IBM QRadar Action on Disposition 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 IBM QRadar folder and select **IBM QRadar Action on Disposition**. The **IBM QRadar Action on Disposition** pane opens.

4. Select **Next**. The Name pane opens.

**Name the Policy**

The Name pane lets you define a unique policy name and useful policy description. Policy names appear in the Policy Manager, the Views pane, NAC Reports and in other features. Precise names make working with policies and reports more efficient.

5. Define a unique name for the policy you are creating based on this template, and enter a description.

   - Make sure names are accurate and clearly reflect what the policy does. For example, do not use a generic name such as My_Compliance_Policy.
   - Use a descriptive name that indicates what your policy is verifying and which actions will be taken.
   - Ensure that the name indicates whether the policy criteria is to be met or not.
   - Avoid having another policy with a similar name.

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

**Define which Endpoints will be Inspected - Policy Scope**

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 Main Rule pane opens. See [How Endpoints are Detected and Handled](#) for details of default policy logic.

### How Endpoints are Detected and Handled

This section describes the main rule and sub-rules of the policy created by this template. Policy rules instruct CounterACT how to detect and handle endpoints defined in the policy scope.

Endpoints that match the Main Rule are included in the policy inspection. *Endpoints that do not match this rule are not inspected for this policy*. Sub-rules automatically follow up with endpoints after initial detection and handling, streamlining separate detection and actions into one automated sequence.

Sub-rules are performed in order until a match is found. When a match is found, the corresponding action is applied to the endpoint. If the endpoint does not match the requirements of the sub-rule, it is inspected by the next rule.

### Main Rule

The main rule of this policy detects the last disposition sent from IBM QRadar Action to CounterACT.
10. The Condition Criteria section is populated by default.

Sub-Rules

The sub-rules of the IBM QRadar Action on Disposition policy detect threats based on their reported severity.

The Sub Rules pane displays all the Sub-Rules associated with the IBM QRadar Action on Disposition policy. Below is a list of all the icons used in the Actions column. These are used for threats with Critical and High severity:

- An optional Send Updates to QRadar SIEM Server action is enabled for each sub-rule.

- See the CounterACT Administration Guide to understand the symbols listed in the Actions column.

12. Select Finish

13. In the CounterACT Policy Manager, select Apply to save the policy. The Policy Manager refreshes with the IBM QRadar Action on Disposition rule and all the sub-rules.

14. Select the Start button to execute the policy.

For information on how to use the IBM QRadar Action on Disposition feature, see the ForeScout App for IBM QRadar How-to-Guide.
Action on Offense by Credibility and Severity Policy Template

Use the IBM QRadar Action on Offense by Credibility and Severity policy template to apply action to an endpoint for which CounterACT received an offense alert from QRadar. Sub-rules of the policy will apply specific action depending upon the severity and credibility of the offense event.

To use the IBM QRadar Action on Offense by Credibility and Severity 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 IBM QRadar folder and select IBM QRadar Action on Offense by Credibility and Severity. The IBM QRadar Action on Offense by Credibility and Severity pane opens.
4. Select Next. The Name pane opens.

Name the Policy

The Name pane lets you define a unique policy name and useful policy description. Policy names appear in the Policy Manager, the Views pane, NAC Reports and in other features. Precise names make working with policies and reports more efficient.

5. Define a unique name for the policy you are creating based on this template, and enter a description.
   - Make sure names are accurate and clearly reflect what the policy does. For example, do not use a generic name such as My_Compliance_Policy.
   - Use a descriptive name that indicates what your policy is verifying and which actions will be taken.
   - Ensure that the name indicates whether the policy criteria needs to be met or not.
   - Avoid having another policy with a similar name.
6. Select **Next**. The Scope pane and IP Address Range dialog box opens.

**Define Which Endpoints Will Be Inspected - Policy Scope**

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 Main Rule pane opens. See [How Endpoints Are Detected and Handled](#) for details of default policy logic.

**How Endpoints Are Detected and Handled**

This section describes the main rule and sub-rules of the policy created by this template. Policy rules instruct CounterACT how to detect and handle endpoints defined in the policy scope.

Endpoints that match the Main Rule are included in the policy inspection. *Endpoints that do not match this rule are not inspected for this policy*. Sub-rules automatically follow up with endpoints after initial detection and handling, streamlining separate detection and actions into one automated sequence.

Sub-rules are performed in order until a match is found. When a match is found, the corresponding action is applied to the endpoint. If the endpoint does not match the requirements of the sub-rule, it is inspected by the next rule.

**Main Rule**

The main rule of this policy applies no filtering conditions: it includes all endpoints detected by CounterACT within the specified policy scope.
10. The Condition Criteria section is populated by default.

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

**Sub-Rules**

Sub-rules include default action to be taken on:

- High Credibility and (High) Severity events – By default the sub-rule for last offense credibility is set to 8, 9, and 10.
- Medium Credibility and (Medium) Severity events - By default the sub-rule for last offense credibility is set to 4, 5, 6, and 7.
- Low Credibility and (Low) Severity events - By default the sub-rule for last offense credibility is set to 1, 2, and 3.
The Sub Rules pane displays all the Sub-Rules associated with the IBM QRadar Action on Offenses by Credibility and Severity policy. Below is a list of all the icons used in the Actions column. These are used for threats with Critical and High severity:

- An optional Send Updates to QRadar SIEM Server action is enabled for each sub-rule.

- See the CounterACT Administration Guide to understand the symbols listed in the Actions column.

12. Select Finish.

13. In the CounterACT Policy Manager, select Apply to save the policy. The Policy Manager refreshes with the IBM QRadar Action on Offenses by Credibility and Severity rule and all the sub-rules.

14. Select the Start button to execute the policy.

15. On the Policy Manager, select Apply to save the policy.

For information on how to use the IBM QRadar Action on Offense by Credibility and Severity feature, see the ForeScout App for IBM QRadar How-to-Guide.
Action on Offense by Description Policy Template

Use the IBM QRadar Action on Offense by Description policy template to apply action to an endpoint for which CounterACT received an offense alert from IBM QRadar. Sub-rules of the policy will apply specific action depending upon the description of the offense alert.

To use the IBM QRadar Action on Offense by Description 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 IBM QRadar folder and select IBM QRadar Action on Offense by Description. The IBM QRadar Action on Offense by Description pane opens.
4. Select Next. The Name pane opens.

Name the Policy

The Name pane lets you define a unique policy name and useful policy description. Policy names appear in the Policy Manager, the Views pane, NAC Reports and in other features. Precise names make working with policies and reports more efficient.

5. Define a unique name for the policy you are creating based on this template, and enter a description.
   – Make sure names are accurate and clearly reflect what the policy does. For example, do not use a generic name such as My_Compliance_Policy.
   – Use a descriptive name that indicates what your policy is verifying and which actions will be taken.
   – Ensure that the name indicates whether the policy criteria needs to be met or not.
   – Avoid having another policy with a similar name.
Define Which Endpoints Will Be Inspected - Policy Scope

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 Main Rule pane opens.

How Endpoints Are Detected and Handled

This section describes the main rule and sub-rules of the policy created by this template. Policy rules instruct CounterACT how to detect and handle endpoints defined in the policy scope.

Endpoints that match the Main Rule are included in the policy inspection. *Endpoints that do not match this rule are not inspected for this policy.* Sub-rules automatically follow up with endpoints after initial detection and handling, streamlining separate detection and actions into one automated sequence.

Sub-rules are performed in order until a match is found. When a match is found, the corresponding action is applied to the endpoint. If the endpoint does not match the requirements of the sub-rule, it is inspected by the next rule.

**Main Rule**

The main rule of this policy detects all Offenses detected by IBM QRadar Action by Offense by Description reported to CounterACT in the last week.
The Condition Criteria section is populated by default.

Select Next. The Sub-Rules pane opens.

Sub-Rules

The Sub Rules pane displays all the Sub-Rules associated with the IBM QRadar Action on Offense by Description policy. Sub-rules include default action to be taken on:

- Quarantine endpoints that access honeypots
- Quarantine endpoints that are subject to an attack and then respond to malicious activity
- Notify users when their endpoint has stopped sending events to IBM QRadar
- Quarantine endpoints with excessive firewall denies
- Quarantine endpoints that are executing a TCP flood attack
- Quarantine endpoints that are actively scanning for SSH servers
- Notify CounterACT when a new endpoint is discovered by IBM QRadar

Below is a list of all the icons used in the Actions column. These are used for threats with Critical and High severity:

1. An optional Send Updates to QRadar SIEM Server action is enabled for each sub-rule.

2. See the CounterACT Administration Guide to understand the symbols listed in the Actions column.
12. Select Finish.

13. In the CounterACT Policy Manager, select Apply to save the policy. The Policy Manager refreshes with the IBM QRadar Action on Disposition rule and all the sub-rules.

14. Select the Start button to execute the policy.

For information on how to use the IBM QRadar Action on Offense by Description feature, see the ForeScout App for IBM QRadar How-to Guide.

Send SIEM Updates Policy Template

Use the IBM QRadar Send SIEM Update policy template to periodically send host information to IBM QRadar. By default, this policy sends all property and policy information, for all endpoints, using all syslog as a communication method configured for IBM QRadar interaction. The default is an update every hour.

To use the IBM QRadar Send SIEM Updates 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 IBM QRadar folder and select IBM QRadar Send SIEM Updates. The IBM QRadar Send SIEM Updates pane opens.
4. Select Next. The Name pane opens.

Name the Policy

The Name pane lets you define a unique policy name and useful policy description. Policy names appear in the Policy Manager, the Views pane, NAC Reports and in other features. Precise names make working with policies and reports more efficient.

5. Define a unique name for the policy you are creating based on this template, and enter a description.
   - Make sure names are accurate and clearly reflect what the policy does. For example, do not use a generic name such as My_Compliance_Policy.
6. Select **Next**. The Scope pane and IP Address Range dialog box opens.

**Define Which Endpoints Will Be Inspected - Policy Scope**

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 Main Rule pane opens. See **How Endpoints Are Detected and Handled** for details of default policy logic.

**How Endpoints Are Detected and Handled**

This section describes the main rule and sub-rules of the policy created by this template. Policy rules instruct CounterACT how to detect and handle endpoints defined in the policy scope.

Endpoints that match the Main Rule are included in the policy inspection. *Endpoints that do not match this rule are not inspected for this policy*. Sub-rules automatically follow up with endpoints after initial detection and handling, streamlining separate detection and actions into one automated sequence.

Sub-rules are performed in order until a match is found. When a match is found, the corresponding action is applied to the endpoint. If the endpoint does not match the requirements of the sub-rule, it is inspected by the next rule.
Main Rule
For the main rule pane, only an Action item will be configured for the IBM QRadar Send SIEM Update policy.

10. Select Next. The Sub-Rules pane opens.

Sub-Rules
There are no default sub-rules.

11. Select Finish.
12. Select the Start button to execute the policy.
13. On the Policy Manager, select Apply to save the policy.

WinCollect Agent Compliance Policy Template

WinCollect is used to monitor Windows event logs (both local and remote) and transmits them to a remote console via syslog.

Before you create this policy you will need to install the WinCollect Agent on your server.

1. Go to Computer and then select Manage. The Computer Management dialog box displays.
2. Expand **Services and Applications** and then select **Services**.

3. Select **WinCollect** and the WinCollect Properties dialog box displays.

4. The path to executable should be \Program Files\IBM\WinCollect\bin\WinCollectSvc.exe.

Use the IBM QRadar WinCollect Agent Compliance template to create a CounterACT policy that:

- Detects endpoints on which the IBM QRadar WinCollect agent is installed and running.
- Detects endpoints on which that IBM QRadar WinCollect agent is not installed.
- Detects endpoints on which that IBM QRadar WinCollect agent is irresolvable.

In addition, optional actions can be used to:

- Direct users to a URL from which to install the agent if it is not installed. It is recommended that the URL be available from outside the network.
- Run a script to start the IBM QRadar WinCollect agent if it is installed but not running.

**To use the IBM QRadar WinCollect Agent Compliance 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 **IBM QRadar** folder and then select **IBM QRadar WinCollect Agent Compliance**. The IBM QRadar WinCollect Agent Compliance pane opens.

4. Select **Next**. The Name pane opens.

**Name the Policy**

The Name pane lets you define a unique policy name and useful policy description. Policy names appear in the Policy Manager, the Views pane, NAC Reports and in other features. Precise names make working with policies and reports more efficient.

5. Define a unique name for the policy you are creating based on this template, and enter a description.
   - Make sure names are accurate and clearly reflect what the policy does. For example, do not use a generic name such as My_Compliance_Policy.
   - Use a descriptive name that indicates what your policy is verifying and which actions will be taken.
   - Ensure that the name indicates whether the policy criteria needs to be met or not.
   - Avoid having another policy with a similar name.

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

**Define Which Endpoints Will Be Inspected - Policy Scope**

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 Main Rule pane opens.

**How Endpoints Are Detected and Handled**

This section describes the main rule and sub-rules of the policy created by this template. Policy rules instruct CounterACT how to detect and handle endpoints defined in the policy scope.

Endpoints that match the Main Rule are included in the policy inspection. *Endpoints that do not match this rule are not inspected for this policy*. Sub-rules automatically follow up with endpoints after initial detection and handling, streamlining separate detection and actions into one automated sequence.

Sub-rules are performed in order until a match is found. When a match is found, the corresponding action is applied to the endpoint. If the endpoint does not match the requirements of the sub-rule, it is inspected by the next rule.

**Main Rule**

The main rule of this policy detects all Windows devices detected by CounterACT to identify them as in scope for the IBM QRadar WinCollect Agent Compliance policy.
10. The Condition Criteria section is populated by default.

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

Sub-rules include default action to be taken on:

- IBM QRadar WinCollect Installed & Running
- IBM QRadar WinCollect Installed but NOT Running
- IBM QRadar WinCollect NOT Installed
- IBM QRadar WinCollect Irresolvable

See the CounterACT Administration Guide to understand the symbols listed in the Actions column.

12. Select Finish.
13. In the CounterACT Policy Manager, select Apply to save the policy. The Policy Manager refreshes with the IBM QRadar Action on Disposition rule and all the sub-rules.
14. Select the Start button to execute the policy.

Create Custom IBM QRadar Policies

CounterACT policies are powerful tools used for automated endpoint access control and management.

Policies and Rules, Conditions and Actions

CounterACT policies contain a series of rules. Each rule includes:
• Conditions based on host property values. CounterACT detects endpoints with property values that match the conditions of the rule. Several conditions based on different properties can be combined using Boolean logic.

• Actions can be applied to endpoints that match the conditions of the rule.

In addition to the bundled CounterACT properties and actions available for detecting and handling endpoints, you can use properties to create custom policies.

**To create a custom policy:**

1. In the CounterACT Console, select the **Policy** tab. The Policy Manager opens.
2. Select **Add** to create a policy, or select **Help** for more information about working with policies.

**Policy Properties**

This section describes the properties that are available when you install the ForeScout Extended Module for IBM QRadar.
To access QRadar properties:

1. In CounterACT, navigate to the Properties tree from the Policy Conditions dialog box.
2. Expand the IBM QRadar folder in the Properties tree.

The following properties are available.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>QRadar Last Offense</td>
<td>Information received from QRadar about an endpoint's most recent offense.</td>
</tr>
<tr>
<td>QRadar Last Policy Trigger</td>
<td>Information received from QRadar about an endpoint's most recent disposition.</td>
</tr>
<tr>
<td>QRadar Offenses</td>
<td>Lists the information about offenses received by QRadar.</td>
</tr>
<tr>
<td>QRadar Policy Triggers</td>
<td>Lists the information about dispositions received by QRadar.</td>
</tr>
</tbody>
</table>

Policy Actions

CounterACT policy actions let you instruct CounterACT how to control detected endpoints. For example, assign an endpoint infected with a virus to an isolated VLAN or send the device user or IT team an email.

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

To access the ForeScout Extended Module for IBM QRadar actions:

1. In the CounterACT Console, navigate to the Action tree from the Policy Conditions dialog box.
2. Expand the Audit folder in the Actions tree.
The following actions are available.

| Send Updates to QRadar SIEM Server | Sends the policy status and host information from CounterACT to the QRadar SIEM Server. See the next section for more information. |

**Send Data from CounterACT to IBM QRadar**

To implement IBM QRadar reporting, define a CounterACT policy that includes the IBM QRadar update action. When the conditions of this policy are met, IBM QRadar notification is implemented in one of several modes:

- **One-time report**: current policy/host information is sent once when the conditions of the policy are met.
- **Update reporting**: a message is sent whenever the host information or policy status changes.
- **Periodic reporting**: a message is sent at regularly defined intervals.

The policy conditions need to be met at least once to initiate update reporting or periodic reporting. Similarly, CounterACT stops change reporting and periodic reporting when the conditions of the policy are no longer met.

You can further modify notification behavior using standard action scheduling options.
To create an IBM QRadar reporting action in a CounterACT policy:

1. Create or edit a policy, and edit policy actions.
2. In the Actions tree, select Audit and then select Send Updates to QRadar SIEM Server. The Contents tab opens. Use this tab to determine the information that is reported to IBM QRadar for hosts in the scope of the policy.
3. Select the Send host property results check box to send host property values to the IBM QRadar server.
   - Select Send all to include all properties discovered.
   - Select Send specific to send the values of specific properties. Choose the properties to report from the list.
4. Select Send policy status to send the CounterACT policy status (Match/Unmatch/Pending/Irresolvable).
5. Select the Trigger tab. Use this tab to determine reporting behavior.

6. Select the following options:
   - Select Send when the action starts to send information once when the conditions of the policy are met.
   - Select Send when information is updated to send information when there is a change in the host properties you specified in the Content tab.
   - Select Send periodically every to send information at fixed intervals.
7. Select the Schedule tab. You can use these standard action scheduling options to further customize message delivery. For example, you can choose the Customize action start time option to delay message delivery, or to limit the duration of repeated or regularly scheduled messages.
Using the ForeScout Extended Module for QRadar

See also Send Data from CounterACT to IBM QRadar.

For more information on how to use this module, refer to the ForeScout App for IBM QRadar How-To-Guide.

Integrate the ForeScout Functionalities into IBM QRadar

Now that you have established communication between the ForeScout Extended Module for IBM QRadar and the IBM QRadar SIEM server, you can work with ForeScout functionalities in the IBM QRadar Dashboard.

There are five dashboard widgets that can be imported.

1. In the Dashboard tab, make sure the Show Dashboard field displays System Monitoring.
2. Select the Add Item drop-down, select ForeScout and then select the widget.

<table>
<thead>
<tr>
<th>Compliance Status Summary</th>
<th>The number of endpoints that have or have not fulfilled organizational requirements for compliance policies. For example, the number of endpoints that have or have not installed prohibited applications such as instant messaging or peer-to-peer applications.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Classification</td>
<td>Indicates the percentage of all the different types of devices that are connected to the network. Example: Windows, Mac, Android, Unknown.</td>
</tr>
<tr>
<td>Host Connection Status</td>
<td>The number of endpoints that are currently connected to your network.</td>
</tr>
<tr>
<td>Corporate/Guest Status</td>
<td>The number of endpoints in your organization not considered part of the corporate network, for example, personal laptops used by outside contractors. CounterACT may have detected these endpoints when they did not properly authenticate with the network.</td>
</tr>
</tbody>
</table>
You can have multiple CounterACT Dashboards.

1. Select the IP address in the ForeScout CounterACT field and then select **Open**. The CounterACT login opens.
2. **Log in**. The CounterACT Dashboard opens. The widget displays on the Dashboard as a pie chart.

### View Widget Details

Each widget watches IP addresses related to their subject matter. You can drill-down into each widget to get detailed information:

1. Within a widget, select the **View Detail** link. The **Details** page opens.
2. In the **Time Range** field, select the time slot for which you want to view more details then select **Update**. The information displays as a pie chart.
Customize the Display of the Dashboard

You can re-order the widgets on the Dashboard using the drag-and-drop method. Simply drag the grey bar of the widget frame to the desired location.

Display Inventory Data

Use the CounterACT Asset Inventory to view a real-time display of threats detected by IBM QRadar. The Asset Inventory lets you:

- Broaden your view of the organizational network from device-specific to activity-specific.
- View endpoint information reported by the IBM QRadar Offences and Disposition Triggers.
- View endpoints that have been detected with specific Offences.
- Easily track IBM QRadar Offence detection activity.
- Incorporate inventory detections into policies.

To access the Access Inventory:

1. In the CounterACT Console, select the Asset Inventory icon from the Console toolbar.
2. Navigate to the IBM QRadar folder. The list of QRadar offenses display.
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](https://updates.forescout.com/support/index.php?url=counteract)
- **Centralized Licensing Mode** - [Customer Portal](https://forescout.force.com/support/)

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 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.
Legal Notice

Copyright © ForeScout Technologies, Inc. 2000-2018. All rights reserved. ForeScout, the ForeScout logo, ActiveResponse, ControlFabric, CounterACT, CounterACT Edge and SecureConnector are trademarks or registered trademarks of ForeScout. It is strictly forbidden to copy, duplicate, sell, lend or otherwise use this document in any way, shape or form without the prior written consent of ForeScout. All other trademarks used in this document are the property of their respective owners.

These products are based on software developed by ForeScout. The products described in this document may be protected by one or more of the following U.S. patents: #6,363,489, #8,254,286, #8,590,004, #8,639,800 and #9,027,079 and may be protected by other U.S. patents and foreign patents.

Send comments and questions about this document to: support@forescout.com

2018-03-09 14:33