ForeScout Extended Module for IBM® BigFix®
Configuration Guide

Version 1.0.0
Table of Contents

About this Integration .................................................................................. 4
Use Cases .................................................................................................. 4
Additional BigFix Documentation ................................................................. 4

About this Module ........................................................................................ 4

Concepts, Components, Considerations .................................................... 5
Concepts ..................................................................................................... 5
  Deployment Options .................................................................................. 5
Components ................................................................................................ 6
Considerations ............................................................................................. 7
What to Do .................................................................................................. 7

Requirements ............................................................................................... 8
  CounterACT Software Requirements ....................................................... 8
  ForeScout Module License Requirements ............................................... 8
    Requesting a License .............................................................................. 9
    More License Information ..................................................................... 9
  BigFix Requirements .............................................................................. 10
  Supported Systems .................................................................................. 10

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

Configure the Module .................................................................................. 11
  Create an optional BigFix Account .......................................................... 11
  Establish Connection to a BigFix Root Server ........................................ 11
    Add BigFix Connection ......................................................................... 11
    Add BigFix Properties .......................................................................... 15
    Add BigFix Fixlets ............................................................................... 18
    Edit BigFix Connection ....................................................................... 19
  Test Your Configurations ......................................................................... 19
  Delete BigFix Instance ........................................................................... 20
    Remove BigFix Fixlets .......................................................................... 20
    Remove BigFix Properties .................................................................... 20
    Remove BigFix Root Server .................................................................. 21

Run BigFix Policy Templates ....................................................................... 22
  IBM BigFix Active Directory Groups Policy Template ............................ 22
  IBM BigFix Agent Compliance Policy Template ..................................... 27
    Manually Verify BigFix Agent is Running (Optional) ......................... 27
    BigFix Agent Compliance Template ..................................................... 28
  IBM BigFix Patch Compliance Policy Template ..................................... 33
Create Custom BigFix Policies ............................................................... 37
  Policy Properties .................................................................................. 38
  Add Optional Host Properties ............................................................... 39
  Create a Custom Site ........................................................................... 40
  Define Host Properties .......................................................................... 40
  Policy Actions ....................................................................................... 43
  BigFix Fixlet ......................................................................................... 43
  BigFix Linux ........................................................................................ 45
  BigFix Windows .................................................................................... 47

Using the BigFix Extended Module ....................................................... 54
  Access the Inventory ............................................................................ 54
  Access the Home Tab ........................................................................... 55

Appendix 1: Permissions for a Restricted User .................................... 55

Additional CounterACT Documentation ............................................. 56
  Documentation Portal ........................................................................... 56
  Customer Support Portal ....................................................................... 57
  CounterACT Console Online Help Tools ............................................. 57
About this Integration

IBM® BigFix® Patch provides an automated, simplified patching process that is administered from a single console. It provides real-time visibility and enforcement to deploy and manage patches to all endpoints – on and off the corporate network. BigFix security software identifies all of a company’s PCs, laptops, server and then monitors and flags IT administrators when devices are not in compliance with corporate IT security standards. BigFix can make security fixes across at least 500,000 machines in a matter of minutes.

The Extended Module for IBM BigFix integrates BigFix patch management and endpoint security posture assessment into CounterACT®.

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.

**BigFix Agent compliance** - Installation and configuration of the BigFix Agent allows full compliance on all supported endpoints within your network. See IBM BigFix Agent Compliance Policy Template.

**CounterACT policies designed for BigFix enforcements** - You can manage and automate your BigFix solution using policies to identify whether or not an endpoint is patched with all security updates. See Add BigFix Fixlets. This includes a variety of commercial compliance standards and prevents network access via CounterACT for non-compliant devices. See IBM BigFix Patch Compliance Policy Template.

**Collect and customize BigFix host properties:** Continually assesses device hygiene and continuously monitors an endpoint's security posture. CounterACT can get a customizable number of additional host details from Unix/Win/Mac platforms including chassis type, memory info, disk detail and more. See Add Optional Host Properties.

Additional BigFix Documentation

Refer to the IBM BigFix Knowledge Center online documentation for more information about the BigFix solution:


About this Module

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

- Enforce BigFix Agent compliance.
- BigFix Fixlets are used to orchestrate patch compliance.
- Gain additional information on host properties such as operating system, remediation items, etc.

You must install and configure both CounterACT and IBM BigFix to work with the features described in this document.

**Concepts, Components, Considerations**

This section provides a basic overview of BigFix/CounterACT architecture:

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

**Concepts**

This integration lets you connect one or more CounterACT Appliance(s) or Enterprise Managers to a unique BigFix deployment. When multiple CounterACT Appliances are mapped to a single BigFix deployment, they are grouped into *connecting CounterACT Appliance cluster*. These appliances handle communication between the BigFix deployment and the rest of CounterACT Appliances in your environment. As part of the configuration, the BigFix Module allows the operator to control the rate of CounterACT directed actions to the BigFix deployment, thus avoiding the taking too many actions on a single network at one time.

Typically, there is only one BigFix production deployment per customer. CounterACT Appliances are connected to this BigFix deployment using logical URL and user credentials.

**Deployment Options**

There are two topologies that can be used to set up multiple CounterACT Appliances to a BigFix deployment. For both topologies, a single CounterACT Appliance can be assigned to only one BigFix deployment.

- The actual deployments can be designed to combine both topologies to meet particular network requirements.

**Peer-to-Peer:** Each CounterACT Appliance communicates directly with a BigFix instance. This is a one-to-one relationship, where each CounterACT Appliance or Enterprise Manager prompts initiates queries whenever required. This is often the topology for remote sites.
A **CounterACT Connecting Appliance cluster** is a group of one or more CounterACT Appliances connecting to the BigFix® Enterprise Suite (BES™) through that logical URL associated with the BigFix server. There may be more than one connecting appliance clusters in a company, typically set up by geographical region, business unit or functional separation. These are the middle men for other CounterACT Appliances reaching out to the BigFix instance.

**Components**

- Key components of the BigFix service delivery platform include the BigFix Agent, BigFix Server and Console, BigFix Fixlet messages and BigFix Relays.

- The **BigFix Agent** resides on BigFix managed devices and acts as a universal policy engine capable of delivering multiple management services. A single BigFix Agent can execute a diverse and extensible array of management services that range from real-time client status reporting, to patch and software distribution, to security policy enforcement. The BigFix Agent also automatically notifies the BigFix Server and Console of changes in managed device configuration, providing a real-time view of device status.

- The **BigFix [Root] Server** is a control center and repository for managed system configuration data, software updates and patches, and other management information.
The **BigFix Console**, which runs from the BigFix Server, provides an operations control center for BigFix administrators and includes graphical displays of device, group, and enterprise-wide device status and dashboards for executing management actions through the BigFix infrastructure. The console also includes reporting functions and templates that enable graphical and tabular views on infrastructure status.

**BigFix Fixlet** messages are instructions to the BigFix Agent to perform a management or reporting action. Fixlet messages can be programmed to target specific groups of devices to perform management actions.

**BigFix Relays** act as concentration points for Fixlet messages on network infrastructures. Relays are a software module that execute as a shared service on non-dedicated hardware.

**CounterACT Appliances** are the ones that are managing or monitoring devices based on the network segments assigned to a particular CounterACT Appliance. When these appliances have to reach out to BigFix, they go through the CounterACT Connecting Appliance cluster(s).

**Devices on the network** these are considered the hardware assets whose information has to be exchanged between CounterACT and BigFix. When these devices enter or leave the network, CounterACT monitors them and provides information.

With this as the context, when the BigFix Module is installed on CounterACT connecting appliance clusters (each CounterACT Appliance individually), the operator can configure connection parameters to the BigFix instance. These connection parameters include logical URL (for example, mycompany.bigfix-instance.bigfix.com), user credentials (this user would have the right privileges / permissions to perform the necessary operations), proxy settings and advance settings.

### Considerations

This section addresses any additional ForeScout Extended Module for IBM BigFix considerations. See IBM BigFix 9.5 - System Requirements.

### What to Do

Perform the following to carry out the integration:

1. Verify that requirements are met. See Requirements for details.
2. Download and install the ForeScout Extended Module for IBM BigFix Module from the ForeScout website: www.forescout.com/support. See Install the Module.
3. Define target BigFix instance. Assign CounterACT Appliances to it. See Establish Connection to a BigFix Root Server for details.
4. Create policies for CounterACT to update BigFix assets. See Run BigFix Policy Templates.
5. When the configurations have been tested and the policies created, you are ready to start Using the BigFix Extended Module.

Requirements

This section describes:

- CounterACT Software Requirements
- ForeScout Module License Requirements
- BigFix Requirements

CounterACT Software Requirements

The BigFix Module requires the following CounterACT releases and other CounterACT components:

- CounterACT version 7.0.0.
- Service Pack 2.3.4 or above (SP 3.0 recommended). It is recommended to install the latest service pack to take advantage of the most current CounterACT updates.
- A module license for IBM BigFix Module.
- An active Maintenance Contract for the licensed IBM BigFix module is required.
- Microsoft Active Directory recommended for the IBM BigFix Active Directory Groups Policy Template.

ForeScout Module License Requirements

This ForeScout Module requires a module license. The installation package for the module is in the form of a CounterACT plugin. When installing the plugin 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.
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.

More License Information

See the CounterACT Console User Manual for information on requesting a permanent license or a demo license extension. You can also contact your ForeScout representative or license@forescout.com for more information.
**BigFix Requirements**

- IBM BigFix version 9.5
- Verify connectivity between CounterACT and targeted IBM BigFix servers to port 52311.

**Supported Systems**

The BigFix Extended Module works on the following platform:

*IBM BigFix Platform 9.5.0*

**Install the Module**

The installation package for the module is in the form of a CounterACT plugin.

**To install the plugin:**

1. Navigate to the [Customer Support, ForeScout Modules](#) page and download the plugin `.fpi` file.
2. Save the file to the machine where the CounterACT Console is installed.
3. Log into the CounterACT Console and select **Options** from the **Tools** menu.
4. Select **Plugins**. The Plugins pane opens.
5. Select **Install**. The Open dialog box opens.
6. Browse to and select the saved plugin `.fpi` file.
7. Select **Install**.
8. If you have not yet purchased a permanent module license, a message appears indicating that the plugin will be installed with a demo module license. Select **Yes** and then select **Install**.
9. An installation or upgrade information dialog box and an End User License Agreement will open. Accept the agreement to proceed with the installation.
10. When the installation completes, select **Close**. The plugin is displayed in the Plugins pane. The **Module Status** column indicates the status of your license. See ForeScout Module License Requirements or the CounterACT Console User Manual for details on requesting a permanent license or a demo license extension.
11. Select the plugin and select **Start**. The Select Appliances dialog box opens.
12. Select the CounterACT devices on which to start the plugin.
13. Select **OK**. The plugin runs on the selected devices.
Configure the Module

Configure the module to ensure that CounterACT can communicate with BigFix deployment.

Perform this procedure after the ForeScout Extended Module for BigFix is installed on your targeted CounterACT Appliance.

To complete configuration of some of these connections, you must perform the following configuration steps on the BigFix instance:

1. Establish Connection to a BigFix Root Server
2. Test Your Configurations

In BigFix module release 1.0.0, the following BigFix security configuration scenarios are not supported:

- Capability to follow the NIST security standards by configuring an enhanced security option. This setting enables SHA-256 as the hashing algorithm for digital signatures as well as content verification.
- Enabling the TLS 1.2 communication among the BigFix components.

Create an optional BigFix Account

The BigFix Module comes with a default administrator account and you can optionally use this. Otherwise, create your own by going to Setting up users.

Establish Connection to a BigFix Root Server

This section addresses the configuration of your BigFix root server.

Add BigFix Connection

You will need to map your CounterACT Appliance to a BigFix root server.

To add BigFix targets for CounterACT:

1. In the CounterACT Console toolbar, select Options from the Tools menu.
2. Select IBM BigFix from the Options pane. The right pane opens to display three tabs: BigFix Instance, BigFix Properties, and BigFix Fixlet.
3. In the BigFix Instance tab, select **Add**. The Add BigFix Connection wizard opens.
4. Enter your configurations.

<table>
<thead>
<tr>
<th>BigFix Root Server (Host Name or IP)</th>
<th>Enter the host name or IP address for your BigFix root server followed by the port number. The port number is optional, but if no port number is provided, CounterACT will use port 52311. For example: bigfix.com:52311.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>Enter the username used to access the BigFix root server.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter the password used to access BigFix root server. BigFix password restrictions will apply.</td>
</tr>
<tr>
<td>Verify Password</td>
<td>Re-enter the password.</td>
</tr>
<tr>
<td>Description (Optional)</td>
<td>Insert text, for example, a nick name of the BigFix connection. This is helpful if you have more than one BigFix connection.</td>
</tr>
</tbody>
</table>

5. Select Next. The Assign CounterACT Devices pane displays.

Connecting CounterACT Device
In an environment where more than one CounterACT device is assigned to a single BigFix instance, the connecting CounterACT Appliance functions as a middle man between the BigFix instance and the CounterACT Appliance. The connecting CounterACT Appliance forwards all queries and requests to and from the BigFix instance. Select the IP address of the connecting CounterACT Device.
Assign specific devices
This CounterACT Appliance is assigned to a BigFix instance, but it does not communicate with it directly. All communication between the BigFix instance and its assigned CounterACT Appliance is handled by the connecting CounterACT Appliance defined for the BigFix instance.

1. Select Available Devices and then select an item in the Available Devices list.
2. Select Add. The selected device will send its requests to the BigFix server through the connecting appliance.

Assign all devices by default
This is the connecting appliance that CounterACT Appliances are assigned to by default - if they are not explicitly assigned to another connection appliance.
Select Assign all devices by default to make this connecting appliance the middle man for all CounterACT Appliances not assigned to another connecting appliance.

For more information, see Deployment Options.


Maximum number of actions allowed within a period of 1 minute
Addresses the rate limiting. This means CounterACT has to limit the number of actions sent to this BigFix instance. This prevents the BigFix instance from becoming inundated, and therefore, causes problems.

- **Use Default** - select if you want to use the default setting of one action per minute timeframe.
- **Specify** - select a number from the list to specify the number of action items per minute timeframe.

7. Select Finish. The server appears in the BigFix Instance tab.
Add BigFix Properties

You can add custom BigFix properties in addition to the default CounterACT properties.

To add BigFix properties:

1. In the BigFix Patch Console, create a new Retrieved Property and a Relevance Expression using the instructions located here: Creating Retrieved Properties

2. Add the Retrieved Property and the Relevance Expression to the Master Actions Site. For example:

3. In the CounterACT Console, select Options from the Tools menu.

4. Select IBM BigFix. The IBM BigFix pane opens to the BigFix Connections tab.

5. Select the BigFix Properties tab.

<table>
<thead>
<tr>
<th>Label</th>
<th>Create a name or a label to associate to this new property. This label will display in the Inventory view, Host tab on the CounterACT Console.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>(Optional) Insert text, for example, the nickname of this host property you are creating.</td>
</tr>
</tbody>
</table>
7. Select **Next**. The Display/Track pane displays.

| Type | In the Type drop-down list, select the type of data the property contains. Single-value properties contain one value: string, Boolean, date, or integer. |

**Select Next.** The Display/Track pane displays.

| Display BigFix Property in Inventory View | Display Property in Inventory View shows this property in the CounterACT Console Inventory tab. De-select if you do not want it displayed there. |
| Inventory Description | Enter a description of the property you want to display in the CounterACT Console Inventory. This description will only display if you have the Display Property in Inventory View box checked. |
| Display BigFix Property in Host Profiles Pane of Home View and Assets Portal | Checked by default, **Display Property in Host Profiles Pane of Home View** lists this property in the Profiles tab of the Home view and in the Assets portal. De-select if you do not want it displayed there. |
| Enable Track Changes | The Track Changes properties let you define policy conditions that identify changes in the value of custom properties you define. You can define track changes properties for single-value properties that you create. Select **Enable Track Changes** to create a second, parallel change property under the Track Changes folder of the Properties tree. Use the change property in policies to identify changes in the property values retrieved from the BigFix instance. |
8. Select Finish. The property is added to the table in the BigFix Property tab.
9. Repeat steps 2-4 for every host property you want to create and use.
10. When finished, in the IBM BigFix pane, select Apply. The CounterACT infrastructure will save the configurations, update the internal database, and restart the BigFix Module. This may take 1-2 minutes for the changes to take effect.
11. Continue to the Add BigFix Fixlets section.

For information about adding host properties, see Policy Properties.

**Add BigFix Fixlets**

BigFix Fixlet messages are instructions to the BigFix Agent to perform a management or reporting action. You can program Fixlet messages to target specific devices (or groups of devices) to perform management actions. This is done in the BigFix Fixlet tab.

**To add BigFix Fixlets:**
1. In the CounterACT Console, select Options from the Tools menu.
2. Select IBM BigFix. The IBM BigFix pane opens to the BigFix Connections tab.
3. Select the BigFix Fixlets tab.
5. Enter appropriate settings:

<table>
<thead>
<tr>
<th>Site</th>
<th>Use the drop-down to select the Site.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Selected the name you want to add to CounterACT. There may be multiple names to choose from.</td>
</tr>
<tr>
<td>Action</td>
<td>Select the appropriate action. Every BigFix Fixlet may have multiple actions associated to the selected Name.</td>
</tr>
<tr>
<td>Custom Name</td>
<td>Assign a short, usable and descriptive name to this Fixlet.</td>
</tr>
</tbody>
</table>

6. Select OK. The new Fixlet information displays in the IBM BigFix pane.
7. Select Apply. This Fixlet will now display in the Policy Actions.
Edit BigFix Connection

If you need to change the connecting appliance or assign a different CounterACT Appliance to the connecting appliance, use the Edit option:

To edit a BigFix connection:
1. In the Plugins pane, select IBM BigFix. The BigFix pane opens.
2. Select the instance then select Edit. The Edit BigFix Connection dialog box opens.
3. Make your edits and select OK.

Test Your Configurations

1. Select Options and then select IBM BigFix. The IBM BigFix pane opens to the BigFix Instance tab.
2. Select a connection and then select Test.
   - If you configured the BigFix root server without the correct administrator permissions the Test will fail. To correct this, add administrator rights to your BigFix account.
3. Check your configurations and re-test. If the test passed, repeat step 2 for any additional connections.

The configuration of the IBM BigFix Module is now complete.
Delete BigFix Instance

The process for deleting a BigFix Instance is the reverse path of creating it:

1. Remove BigFix Fixlets associated with the BigFix instance.
2. Remove BigFix Properties associated with the BigFix instance.
3. Remove BigFix Root Server

Remove BigFix Fixlets

You need to first remove the BigFix Fixlets before you can remove the BigFix properties.

To remove BigFix Fixlets:

1. In the CounterACT Console, select Options from the Tools menu.
2. Select IBM BigFix. The IBM BigFix pane opens to the BigFix Instances tab.
3. Select the BigFix Fixlets tab.
4. Select a Fixlet and then select Remove.
5. Confirm removal.
6. Repeat the steps for other properties, as necessary.

Continue to the Remove BigFix Properties section.

Remove BigFix Properties

You need to first remove the BigFix properties before you can remove the BigFix root server.

To remove BigFix properties:

1. In the CounterACT Console, select Options from the Tools menu.
2. Select IBM BigFix. The IBM BigFix pane opens to the BigFix Instances tab.
3. Select the BigFix Properties tab.
4. Select a property and then select Remove.
5. **Confirm** removal.
6. Repeat the steps for other properties, as necessary.
7. Continue to the [Remove BigFix Root Server](#) section.

### Remove BigFix Root Server

Once the BigFix Fixlets and Properties have been deleted, you can now remove the BigFix instance from CounterACT.

**To remove a BigFix connection:**

1. In the CounterACT Console, select **Options** from the **Tools** menu.
2. Select **BigFix**. The BigFix pane opens to the BigFix Instance tab.
3. Select the server name and then select **Remove**.

4. **Confirm** removal.
5. In the IBM BigFix pane, select **Apply**.
Run BigFix Policy Templates

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 BigFix, CounterACT policies can include collecting BigFix client, relay and server each host is using.

IBM BigFix Active Directory Groups Policy Template

Use the IBM BigFix Active Directory Groups policy template to create policies to classify and manage all Windows computers seen by BigFix. In order to utilize this policy, Microsoft Active Directory is required.

To use the IBM BigFix Active Directory Groups 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 IBM BigFix and select IBM BigFix Active Directory Groups. The IBM BigFix Active Directory Groups 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 must be met or not met.
   - Avoid having another policy with a similar name.


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

The Scope pane and IP Address Range dialog box lets you define a range of hosts to be inspected for this policy.
7. Use the IP Address Range dialog box to define which hosts are inspected. The following options are available for defining a scope:
   - **All IPs**: Include all addresses in the Internal Network. The Internal Network was defined when CounterACT was set up.
   - **Segment**: Select a previously defined segment of the network. To specify multiple segments, select OK to close the IP Address Range dialog box, and select **Segments** from the Scope pane.
   - **IP Range**: Define a range of IP addresses. These addresses must be within the Internal Network.
   - **Unknown IP addresses**: Apply the policy to devices whose IP addresses are not known. Device detection is based on the MAC address of the device. Not applicable for this policy template.

8. Select **OK**. The added range appears in the Scope pane.

9. Select **Next**. The Main Rule pane opens. Continue to the next section.

**How Devices 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 devices defined in the policy scope.

Hosts that match the Main Rule are included in the policy inspection. **Hosts that do not match this rule are not inspected for this policy.** Sub-rules automatically follow up with hosts 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 host. If the host does not match the requirements of the sub-rule, it is inspected by the next rule.

**Main Rule**

The main rule of this policy template detects if the endpoint is managed by Active Directory.
10. The Condition Criteria section is populated by default.

11. You can **Add** conditions and actions. A list of these items can be found in the **Policy Properties** and **Policy Actions** sections.

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

**Sub-Rules**

The sub-rules of the IBM BigFix Active Directory Groups policy list the items CounterACT is to check when applying the Main Rule.
13. Double-click the DCs (datacenters) sub-rule to open it. The Policy: [Name of IBM BigFix Active Directory Groups policy] Sub-Rule: DCs dialog box opens.

14. You can Add conditions and actions. A list of these items can be found in the Policy Properties and Policy Actions sections.

15. Select OK. In the Policy: [Name of IBM BigFix Active Directory Groups policy] Sub-Rule: DCs dialog box, select OK.

16. Repeat steps 13 - 15 to make changes in other sub-rules.

17. In the Sub-Rules pane of the Policy Wizard, select Finish.

18. On the CounterACT Console, select Apply to save the policy.

IBM BigFix Agent Compliance Policy Template

An IBM BigFix administrator can ensure that the IBM BigFix agent is installed and functioning properly on endpoints within the network. An IBM BigFix agent is a stand-alone Windows, Linux, Mac or other application that is installed on both the IBM BigFix Server and network hosts to allow IBM BigFix to manage devices-based BigFix Policy.

Manually Verify BigFix Agent is Running (Optional)

You can optionally verify the BigFix Agent onto your endpoints.

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 BES Client Properties and the BES Client Properties dialog box displays.

4. The path to executable should be \Program Files (x86)\BigFix Enterprise\BES Client\BESClient.exe.
5. Select **OK**.

**BigFix Agent Compliance Template**

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

- Detects endpoints on which the BigFix Agent is installed and running.
- Detects endpoints on which that BigFix Agent is not installed.
- Detects endpoints on which that BigFix 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.

**To use the IBM BigFix 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 **IBM BigFix** and select **IBM BigFix Agent Compliance**. The IBM BigFix 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 must be met or not met.
   - Avoid having another policy with a similar name.

Define which Devices will be Inspected - Policy Scope

The Scope pane and IP Address Range dialog box lets you define a range of hosts to be inspected for this policy.

7. Use the IP Address Range dialog box to define which hosts are inspected. The following options are available for defining a scope:

   - **All IPs**: Include all addresses in the Internal Network. The Internal Network was defined when CounterACT was set up.
   - **Segment**: Select a previously defined segment of the network. To specify multiple segments, select OK to close the IP Address Range dialog box, and select **Segments** from the Scope pane.
   - **IP Range**: Define a range of IP addresses. These addresses must be within the Internal Network.
   - **Unknown IP addresses**: Apply the policy to devices whose IP addresses are not known. Device detection is based on the MAC address of the device. Not applicable for this policy template.

   Filter the range by including only certain CounterACT groups and/or by excluding certain devices or users or groups when using this policy.

8. Select OK. The added range appears in the Scope pane.

9. Select **Next**. The Main Rule pane opens. Continue to the next section.

How Devices 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 devices defined in the policy scope.
Hosts that match the Main Rule are included in the policy inspection. *Hosts that do not match this rule are not inspected for this policy.* Sub-rules automatically follow up with hosts 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 host. If the host does not match the requirements of the sub-rule, it is inspected by the next rule.

The main rule of this policy template detects if the endpoint is managed by BigFix by checking the last reported agent version.

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

### Sub-Rules

The sub-rules of the IBM BigFix Agent Compliance policy list the items CounterACT is to check when applying the Main Rule.

![Policy Wizard - Step 4 of 4](image)

11. Double-click the IBM BigFix Client Running and checked in within the last 30 minutes sub-rule to open it. The Policy: [Name of IBM BigFix Agent Compliance policy] Sub-Rule: IBM BigFix Client Running and checked in within the last 30 minutes dialog box opens.

12. You can **Add** conditions and actions. A list of these items can be found in the [Policy Properties](#) and [Policy Actions](#) sections.

13. Select **OK**. In the Policy: [Name of IBM BigFix Agent Compliance policy] Sub-Rule: IBM BigFix Client Running and checked in within the last 30 minutes dialog box, select **OK**.

14. Repeat steps 13 - 15 to make changes in other sub-rules.

15. In the Sub-Rules pane of the Policy Wizard, select **Finish**.

16. On the CounterACT Console, select **Apply** to save the policy.
IBM BigFix Patch Compliance Policy Template

Use this template to create policies that checks whether the endpoint is meeting specific security compliance, PCI-DSS compliance, and more. If the endpoint is not in compliance, then the BigFix Module flags that endpoint as non-compliant.

**To use the IBM BigFix Patch 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 **IBM BigFix** and select **IBM BigFix Patch Compliance**. The IBM BigFix Patch 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 must be met or not met.
   - Avoid having another policy with a similar name.

6. Select **Next**. The Scope pane and IP Address Range dialog box opens.
Define which Devices will be Inspected - Policy Scope

The Scope pane and IP Address Range dialog box lets you define a range of hosts to be inspected for this policy.

7. Use the IP Address Range dialog box to define which hosts are inspected. The following options are available for defining a scope:
   - **All IPs**: Include all addresses in the Internal Network. The Internal Network was defined when CounterACT was set up.
   - **Segment**: Select a previously defined segment of the network. To specify multiple segments, select OK to close the IP Address Range dialog box, and select Segments from the Scope pane.
   - **IP Range**: Define a range of IP addresses. These addresses must be within the Internal Network.
   - **Unknown IP addresses**: Apply the policy to devices whose IP addresses are not known. Device detection is based on the MAC address of the device. Not applicable for this policy template.

   *Filter the range by including only certain CounterACT groups and/or by excluding certain devices or users or groups when using this policy.*

8. Select OK. The added range appears in the Scope pane.


How Devices 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 devices defined in the policy scope.
Hosts that match the Main Rule are included in the policy inspection. *Hosts that do not match this rule are not inspected for this policy.* Sub-rules automatically follow up with hosts 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 host. If the host 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 BigFix Patch Compliance policy.

10. The Condition Criteria section is populated by default.

11. You can **Add** conditions and actions. A list of these items can be found in the **Policy Properties** and **Policy Actions** sections.

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

**Sub-Rules**

The sub-rules of the IBM BigFix Patch Compliance policy list the items CounterACT is to check when applying the Main Rule.

14. You can **Add** conditions and actions. A list of these items can be found in the Policy Properties and Policy Actions sections.

15. Select **OK**. In the Policy: [Name of IBM BigFix Patch Compliance policy] Sub-Rule: Critical dialog box, select **OK**.

16. Repeat steps 13 - 15 to make changes in other sub-rules.

17. In the Sub-Rules pane of the Policy Wizard, select **Finish**.

18. On the CounterACT Console, select **Apply** to save the policy.

---

**Create Custom BigFix Policies**

You may choose to create custom policies to deal with issues not covered in the IBM BigFix policy templates. Custom policy tools provide you with an extensive range of options for detecting and handling endpoints. This section describes the policy properties and actions available when the BigFix Module is installed.

CounterACT policies contain a series of rules. Each rule includes:

- Conditions based on host property values. CounterACT detects hosts 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 hosts that match the conditions of the rule.
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. The Policy Type wizard opens.
3. Select Custom and configure it, or select Help for more information about working with policies.

Policy Properties
In addition to the bundled CounterACT properties and actions available for adding and updating the BigFix root server, you can work with policy properties to create custom policies. These items are available when you install the module.

To access CounterACT properties:
1. In CounterACT, navigate to the Properties tree from the Policy Conditions dialog box.
2. Expand BigFix in the Properties tree.

The following default property comes with the BigFix Module:
<table>
<thead>
<tr>
<th>BigFix Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BigFix Active Directory Path</td>
<td>The Active Directory service's distinguished name (DN).</td>
</tr>
<tr>
<td>BigFix Agent Version</td>
<td>Version of BigFix Agent on endpoint.</td>
</tr>
<tr>
<td>BigFix BES Relay Selection Method</td>
<td>BigFix Agent Relay Selection Method.</td>
</tr>
<tr>
<td>BigFix Computer Name</td>
<td>Computer Name of endpoint.</td>
</tr>
<tr>
<td>BigFix CPU</td>
<td>CPU usage on endpoint.</td>
</tr>
<tr>
<td>BigFix Device Type</td>
<td>Device Type of the endpoint.</td>
</tr>
<tr>
<td>BigFix Free Disk Details</td>
<td>The amount of free space on the endpoint.</td>
</tr>
<tr>
<td>BigFix Total Disk Details</td>
<td>Lists disk information.</td>
</tr>
<tr>
<td>BigFix Distance to BES Relay</td>
<td>Number of hops from the BES Relay.</td>
</tr>
<tr>
<td>BigFix DNS Name</td>
<td>DNS Name associated with endpoint.</td>
</tr>
<tr>
<td>BigFix Endpoint Locked</td>
<td>Returns whether the endpoint is locked or not.</td>
</tr>
<tr>
<td>BigFix Installed Apps</td>
<td>Installed Apps on the endpoint.</td>
</tr>
<tr>
<td>BigFix Last Reported Time</td>
<td>The last time the BigFix Agent checked in.</td>
</tr>
<tr>
<td>BigFix Memory Info</td>
<td>Lists memory information.</td>
</tr>
<tr>
<td>BigFix OS</td>
<td>Lists information about the OS.</td>
</tr>
<tr>
<td>BigFix Relay</td>
<td>Relay the endpoint is connected to.</td>
</tr>
<tr>
<td>BigFix Relay Name of Client</td>
<td>Relay Name of Client.</td>
</tr>
<tr>
<td>BigFix Remediation Items</td>
<td>Lists the missing patches on endpoint.</td>
</tr>
<tr>
<td>BigFix Running Process</td>
<td>Provides a list of running processes.</td>
</tr>
<tr>
<td>BigFix Running Services</td>
<td>Provides a list of running services.</td>
</tr>
<tr>
<td>BigFix Unix Installed Debian Packages and Repositories</td>
<td>Provides a list of Unix-installed Debian packages.</td>
</tr>
<tr>
<td>BigFix Unix Installed RPM Packages and Repositories</td>
<td>Provides a list of Unix-installed RPM packages.</td>
</tr>
<tr>
<td>BigFix User Name</td>
<td>Lists information on the logged-on user.</td>
</tr>
</tbody>
</table>

- To learn more about the BigFix properties, see the IBM BigFix Platform documentation page.

3. When finished, select OK.

### Add Optional Host Properties

In addition to the default policy properties, you can add additional host properties. Host properties are information stored in CounterACT for each device discovered on the network. When you work with this module, you create new CounterACT host properties to hold data extracted by querying the BigFix root server. This makes retrieved data available for use in CounterACT policies.
You can create single-value properties that contain one value, for example, a string property that contains the GUID of the device. In this version we only support String, Integer, Date and Boolean.

Track Changes properties let you define policy conditions that identify changes in the value of custom properties you define. You can define track changes properties for single-value, list, or Record Exists properties that you create.

Create a Custom Site

Before you can use these new properties, you must create a custom site on the IBM BigFix site and import your customized properties.

To create a custom site:


   > Your custom site must be named: ForeScout Custom Site.

Define Host Properties

To define CounterACT host properties:

1. In the CounterACT Console, select Options from the Tools menu.
2. Select IBM BigFix. The IBM BigFix pane opens to the BigFix Connections tab.
3. Select the BigFix Properties tab.

Label
Create a name or a label to associate to this new property. This label will display in the Inventory view, Host tab on the CounterACT Console.

Description
(Optional) Insert text, for example, the nick name of this host property you are creating.

Type
In the Type drop-down list, select the type of data the property contains. Single-value properties contain one value: string, Boolean, date, or integer.

5. Select Next. The Display/Track pane displays.
Display BigFix Property in Inventory View shows this property in the CounterACT Console Inventory tab. De-select if you do not want it displayed there.

Inventory Description
Enter a description of the property you want to display in the CounterACT Console Inventory. This description will only display if you have the Display Property in Inventory View box checked.

Checked by default, Display BigFix property in Host Profiles Pane of Home View and Assets Portal lists this property in the Profiles tab of the Home view and in the Assets portal. De-select if you do not want it displayed there.

Enable Track Changes
The Track Changes properties let you define policy conditions that identify changes in the value of custom properties you define. You can define track changes properties for single-value properties that you create.

Select Enable Track Changes to create a second, parallel change property under the Track Changes folder of the Properties tree. Use the change property in policies to identify changes in the property values retrieved from the BigFix instance.

Track Name
The text you entered in the Label field in the previous screen populates this field. This field names the item you want to track.

Track Description
The text from the Tag field in the previous screen populates the Track Description field. This field provides a description to the Track Name.

6. Select Finish. The property is added to the table in the BigFix Property tab.
7. Repeat steps 2-4 for every host property you want to create and use.
8. When finished, in the IBM BigFix pane, select **Apply**. The CounterACT infrastructure will save the configurations, update the internal database, and restart the BigFix Module.

⚠️ This may take 1-2 minutes for the changes to take effect.

## Policy Actions

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

⚠️ **CounterACT will re-check to see if the action completed successfully for the first 10 minutes; after that, CounterACT checks periodically for the next 48 hours until it times out.**

**To access the ForeScout Extended Module for BigFix actions:**

1. In the CounterACT Console, navigate to the Actions tree from the Policy Conditions dialog box.
2. Expand **BigFix** in the Actions tree. Select one of the three options:
   - **BigFix Fixlet**
   - **BigFix Linux**
   - **BigFix Windows**

## BigFix Fixlet

Fixlets are used for fixing lack of compliance to enforced rules. It takes a known, non-compliant condition and fixes it.
To configure the Run Fixlet action:

1. Select **BigFix Fixlet**, select **Run Fixlet** and the Parameters pane displays.
2. Select **Custom Fixlet Name** from the check box.
3. 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.
4. Select **OK** to save the changes.
**BigFix Linux**

The functionality of this action is similar to the *Run Script on Linux* action that comes with CounterACT.

**To configure the Run Script on Linux action:**

1. Select **BigFix Linux**, select **Run Script on Linux** and the Parameters pane displays.

2. In the Parameters tab, select the **Command or Script** from the drop-down list. Continue to step 10.

3. If you need to import a script, select the blue **Browse** button. The Scripts Repository dialog box opens.
4. Select **Add**. The File Editor dialog box opens.

5. Select **Add**. The Upload File dialog box opens.

6. Browse and select all the files you want to use and then select **Open**.

7. The File Editor populates with the information. Make any changes in the Title and Description fields and then select **OK**.

8. In the Scripts Repository dialog box, select the script you just imported and then select **OK**.

9. (Optional) If you need to send a host property as a part of the script use a tag to insert the appropriate host property. For example, `ls al > abc.txt` in bash script. Select **Add Tags**.

10. 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.

11. Select **OK** to save the changes.
BigFix Windows

BigFix Windows actions are designed to run specific tasks on Windows devices. Many of the fields used in the BigFix Actions allow you to run a script. To have an optional host property as part of the script, click inside the desired field and then select Add Tags.

BigFix Execution Operations

The functionality of this action is similar to the Run Script on Windows action that comes with CounterACT.

To configure the BigFix Execution Operations action:

1. Select BigFix Windows, select BigFix Execution Operations and the Parameters pane displays.
2. Select an item from the Command drop-down. Options are dos, run, script, and wait.
3. If you select script, enter the script or command parameters into the Parameters field.
4. (Optional) If you need to send a host property as a part of the script, for example, `dir > print.txt`, use a tag to insert the appropriate host property. Click in the Param field and then select Add Tags.
5. 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.
6. Select OK to save the changes.
BigFix File Operations - Copy

This action is similar to the Copy functionality in Windows OS.

To configure the BigFix File Operations - Copy action:

1. Select BigFix Windows, select BigFix File Operations - Copy and the Parameters pane displays.

2. In the Parameters tab, enter the name of the Source file in standard format, for example: C:\Windows\old_filename.

3. Enter the Destination File field, in standard format, for example: C:\Windows\new_filename.

4. For either the Source File or Destination File fields, if you need to send an optional host property as a part of the file name, use a tag to insert the appropriate host property. Click inside the field and then select Add Tags.

5. 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.

6. Select OK to save the changes.
**BigFix File Operations - Delete**

This action is similar to the Delete functionality in Windows OS.

**To configure the BigFix File Operations - Delete action:**

1. Select **BigFix Windows**, select **BigFix File Operations - Delete** and the Parameters pane displays.

2. In the Parameters tab, enter the **File** field, in standard format, for example: `C:\Windows\filename`.

3. Optionally, if you need to send a host property as a part of the file name use a tag to insert the appropriate host property. Click inside the field and then select **Add Tags**.

4. 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.

5. Select **OK** to save the changes.
**BigFix File Operations - Download**
This action is similar to the download functionality in Windows OS.

**To configure the BigFix File Operations - Download action:**

1. Select **BigFix Windows**, select **BigFix File Operations - Download** and the Parameters pane displays.

2. In the Parameters tab, enter the name of the **URL** that is to be downloaded.

3. Optionally, if you need to send a host property as a part of the file name use a tag to insert the appropriate host property. Click inside the field and then select **Add Tags**.

4. 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.

5. Select **OK** to save the changes.
**BigFix File Operations - Move**

This action is similar to the cut and paste functionality in Windows OS.

**To configure the BigFix File Operations - Move action:**

1. Select **BigFix Windows**, select **BigFix File Operations - Move** and the Parameters pane displays.

2. In the Parameters tab, enter the name of the **Source file** in standard format, for example: `C:\Windows\old_filename`.

3. Enter the **Destination File** field, in standard format, for example: `C:\Windows\new_filename`.

4. For either the Source File or Destination File fields, if you need to send an optional host property as a part of the file name, use a tag to insert the appropriate host property. Click inside the field and then select **Add Tags**.

5. 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.

6. Select **OK** to save the changes.
**BigFix Registry - Delete**

This action is similar to the deleting a registry key in Windows OS.

**To configure the BigFix File Registry - Delete action:**

1. Select **BigFix Windows**, select **BigFix Registry - Delete** and the Parameters pane displays.

2. In the Parameters tab, enter the **Registry Key**. An example of formatting the Registry Key is: [HKEY_LOCAL_MACHINE\Software\BigFix\TestKey]

3. Enter the **Value Name**. There cannot be any spaces, for example, testValueName.

4. Select **Add Tags** if you need to send an optional host property as part of deleting the registry name from the endpoint.

5. 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.

6. Select **OK** to save the changes.
BigFix Registry - Set
This action is similar to the setting the value of a registry key in Windows OS.

To configure the BigFix File Registry - Set action:

1. Select **BigFix Windows**, select **BigFix Registry - Delete** and the Parameters pane displays.

2. In the Parameters tab, enter the **Registry Key**. An example of formatting the Registry Key is: `[HKEY_LOCAL_MACHINE\Software\BigFix\TestKey]`

3. Enter the **Value Name**. There cannot be any spaces, for example, `testValueName`.

4. Enter the **Value**. There cannot be any spaces, for example, `testValue`.

5. Select **Add Tags** if you need to send an optional host property as part of setting the key/value name/value of the registry key.

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** to save the changes.
Using the BigFix Extended Module

Once the IBM BigFix Module has been configured, you can view and manage the devices from Inventory view in the CounterACT Console. This provides activity information, accurate at the time of the poll, on endpoints based on certain instances’ properties. The Inventory lets you:

- Complement a device-specific view of the organizational network with an activity-specific view
- View endpoints that were detected with specific attributes
- Incorporate inventory detections into policies

Access the Inventory

To access the inventory:

1. Log in to the CounterACT Console and select the **Inventory** tab.
2. In the Views pane, expand the **BigFix** folder.

If you did not configure to show the property in the Inventory tab, your BigFix properties will not display in the Views pane of the Inventory tab.

3. In the left pane, select the **BigFix** icon to expand it and then select any of the items in the list to view its properties.
4. Check that the properties match the configuration requirements.
Access the Home Tab

To access the Home tab:
1. In the CounterACT Console, select the Home tab.
2. In the Views tree, expand BigFix.
3. Select an item in the Detections pane. The Profile, Compliance and All policies tabs display the information related to the host selected.

Appendix 1: Permissions for a Restricted User

If your BigFix administrator requires more security in regards to users' permissions, then you need to set restricted access to the API user. You can restrict a user's permissions by going to IBM BigFix and logging into your BigFix BES Console account.

1. Login to your BigFix BES Console.
2. In the left pane, select Operators. The Operators pane displays.
3. Select a user and then in the bottom half of the screen, select the Details tab.
4. Enter the following permission settings.

<table>
<thead>
<tr>
<th>Permissions</th>
<th>Explicit Permissions</th>
<th>Effective Permissions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Master Operator</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Show Other Operators' Actions</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Stop Other Operators' Actions</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Can Create Actions</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Can Lock</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Can Send Refresh to Multiple Computers</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Can Submit Queries</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Unmanaged Assets</td>
<td>Show None</td>
<td>Show None</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Restart and Shutdown</th>
<th>Explicit Permissions</th>
<th>Effective Permissions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Post-Action Behavior</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>Action Script Commands</td>
<td>None</td>
<td>None</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Interface Login Privileges</th>
<th>Explicit Permissions</th>
<th>Effective Permissions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Can use Console</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Can use WEBUI</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Can use REST API</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

5. When finished, select **Save Changes**.

6. You can optionally test your changes by running a test (see **Test Your Configurations**).

### Additional CounterACT Documentation

For more detailed information about the CounterACT features described here or additional CounterACT features and modules, refer to the following resources:

- Documentation Portal
- Customer Support Portal
- CounterACT Console Online Help Tools

### Documentation Portal

The ForeScout Documentation Portal is a Web-based library containing information about CounterACT tools, features, functionality and integrations.
To access the Documentation Portal:
2. Use your customer support credentials to log in.
3. Select the CounterACT version you want to discover.

Customer Support Portal
The Customer Support Portal provides links to CounterACT version releases, service packs, plugins and modules as well as related documentation. The portal also provides a variety of How-to Guides, Installation Guides and more. To access the Customer Support Portal, go to:

To access the Customer Support Portal:
2. Select the CounterACT version you want to discover.

CounterACT Console Online 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.

Console User Manual
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 Plugins.
2. Select the plugin and then select Help.

Documentation Portal
Select Documentation Portal from the Help menu.
Legal Notice

Copyright © ForeScout Technologies, Inc. 2000-2017. All rights reserved. The copyright and proprietary rights in this document belong to ForeScout Technologies, Inc. ("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.

Redistribution and use in source and binary forms are permitted, provided that the above copyright notice and this paragraph are duplicated in all such forms and that any documentation, advertising materials and other materials related to such distribution and use acknowledge that the software was developed by ForeScout.

Unless there is another valid written agreement executed by you and ForeScout that governs the ForeScout products and services:

- If you have purchased any ForeScout products or services, your use of such products or services is subject to your acceptance of the terms set forth at http://www.forescout.com/eula/;
- If you have purchased any ForeScout support service ("ActiveCare"), your use of ActiveCare is subject to your acceptance of the terms set forth at http://www.forescout.com/activecare-maintenance-and-support-policy/;
- If you are evaluating ForeScout’s products, your evaluation is subject to your acceptance of the applicable terms set forth below:
  - If you have requested a General Availability Product, the terms applicable to your use of such product are set forth at: http://www.forescout.com/evaluation-license/.
  - If you have requested a Beta Product, the terms applicable to your use of such product are set forth at: http://www.forescout.com/beta-test-agreement/.
  - If you have purchased any ForeScout Not For Resale licenses, such license is subject to your acceptance of the terms set forth at http://www.forescout.com/nfr-license/.

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

2017-09-22 12:50