Contact Information

Forescout Technologies, Inc.
190 West Tasman Drive
San Jose, CA 95134 USA
https://www.Forescout.com/support/
Toll-Free (US): 1.866.377.8771
Tel (Intl): 1.408.213.3191
Support: 1.708.237.6591

About the Documentation

- Refer to the Technical Documentation page on the Forescout website for additional documentation: https://www.Forescout.com/company/technical-documentation/
- Have feedback or questions? Write to us at documentation@forescout.com

Legal Notice

© 2020 Forescout Technologies, Inc. All rights reserved. Forescout Technologies, Inc. is a Delaware corporation. A list of our trademarks and patents can be found at https://www.Forescout.com/company/legal/intellectual-property-patents-trademarks. Other brands, products, or service names may be trademarks or service marks of their respective owners.
# Table of Contents

**About BigFix Integration** ................................................................. 5  
About Certification Compliance Mode ................................................. 5  
Use Cases ........................................................................................... 5  
Limitations ......................................................................................... 5  
Additional BigFix Documentation ....................................................... 6  

**About this Module** ........................................................................... 6  
About Support for Dual Stack Environments ........................................ 6  

**Concepts and Components** ............................................................... 6  
Concepts .............................................................................................. 7  
Deployment Options ........................................................................... 7  
Components .......................................................................................... 8  
What to Do ............................................................................................ 9  

**Requirements** .................................................................................. 9  
Forescout Requirements ....................................................................... 10  
IBM BigFix Requirements ..................................................................... 10  
Supported Systems .............................................................................. 10  
Supported Sites ................................................................................... 10  
Forescout eyeExtend (Extended Module) Licensing Requirements ........... 11  
Per-Appliance Licensing Mode ............................................................ 11  
Flexx Licensing Mode ......................................................................... 12  
More License Information .................................................................... 13  

**Install the Module** ........................................................................... 13  

**Configure the Module** ..................................................................... 14  
Create a BigFix Account ................................................................. 14  
Establish Connection to a BigFix Root Server ..................................... 14  
Add BigFix Connection ...................................................................... 14  
Add BigFix Properties ........................................................................ 18  
Add BigFix Fixlets ............................................................................. 21  
Edit BigFix Connection ....................................................................... 22  
Test Your Configuration ....................................................................... 22  
Delete BigFix Instance ......................................................................... 23  
Remove BigFix Fixlets ......................................................................... 23  
Remove BigFix Properties .................................................................... 23  
Remove the BigFix Root Server .......................................................... 24  
Manually Verify BigFix Agent is Running .......................................... 25  

**Create BigFix Policies Using Templates** ......................................... 25  
Create an IBM BigFix Active Directory Groups Policy .......................... 26  
How Devices Are Detected and Handled .......................................... 29  
Create an IBM BigFix Agent Compliance Policy ................................... 30
Create a BigFix Agent Compliance Policy ................................................... 30
How Devices Are Detected and Handled .................................................... 33
Create an IBM BigFix Patch Compliance Policy ........................................... 34
How Devices Are Detected and Handled .................................................... 37

Create Custom BigFix Policies ................................................................. 38
Policy Properties ....................................................................................... 38
Add BigFix MAC Address Custom Property .................................................. 40
Add Optional Host Properties ..................................................................... 41
Create a Custom Site ............................................................................... 41
Define Host Properties ........................................................................... 42
Policy Actions ........................................................................................... 45
BigFix Fixlet .......................................................................................... 45
BigFix Linux ......................................................................................... 46
BigFix Windows ....................................................................................... 48

Work with Forescout eyeExtend for IBM BigFix ........................................... 56
Access the Asset Inventory ..................................................................... 56
Access the Home Tab ............................................................................. 57

Appendix 1: Permissions for a Restricted User .......................................... 58

Additional Forescout Documentation .......................................................... 59
Documentation Downloads ..................................................................... 59
Documentation Portal ............................................................................. 60
Forescout Help Tools .............................................................................. 60
About BigFix Integration

The Forescout platform integrates with IBM® BigFix® Patch to provide 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, and servers, and then monitors and flags IT administrators when devices are not in compliance with corporate IT security standards. BigFix can make security fixes across 500,000 machines in a matter of minutes.

Forescout eyeExtend for IBM BigFix integrates BigFix patch management and endpoint security posture assessment into the Forescout platform.

About Certification Compliance Mode

Forescout eyeExtend for IBM BigFix supports Certification Compliance mode. For information about this mode, refer to the Forescout Installation Guide.

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 helps ensure full compliance on all supported endpoints within your network. See Create an IBM BigFix Agent Compliance Policy.

- **Forescout platform 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 the Forescout platform for non-compliant devices. See Create an IBM BigFix Agent Compliance Policy.

- **Collect and customize BigFix host properties:** This module continually assesses device hygiene and continuously monitors an endpoint's security posture. The Forescout platform can get a customizable number of additional host details from Unix/Win/Mac platforms, including chassis type, memory information, disk details, and more. See Add Optional Host Properties.

Limitations

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 TLS 1.2 communication among the BigFix components.
Additional BigFix Documentation

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


About this Module

Forescout eyeExtend for IBM BigFix integrates the Forescout platform and BigFix so that you can:

- Enforce BigFix Agent compliance
- Use BigFix Fixlets for patch compliance
- Obtain additional information on host properties, such as operating system and remediation items

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

About Support for Dual Stack Environments

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

Concepts and Components

This section provides a basic overview of the BigFix/Forescout platform architecture:

- Concepts – basic integration concepts and deployment options.
- Components – devices in your network that participate in the integration.
Concepts

This integration lets you connect one or more CounterACT® Appliances or Enterprise Managers to a unique BigFix deployment. When multiple CounterACT Appliances are mapped to a single BigFix deployment, they are grouped into a connecting CounterACT Appliance cluster. These Appliances handle communication between the BigFix deployment and the rest of the CounterACT Appliances in your environment. As part of the configuration, Forescout eyeExtend for IBM BigFix lets the operator control the rate of the Forescout platform’s directed actions to the BigFix deployment, thus avoiding the taking of 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 a logical URL and user credentials.

Deployment Options

There are two topologies that can be used to set up multiple CounterACT Appliances in 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 initiates queries whenever required. This is often the topology for remote sites.

A **CounterACT Connecting Appliance cluster** is a group of CounterACT Appliances connecting to the BigFix Enterprise Suite (BES™) through the logical URL associated with the BigFix server. There may be more than one connecting Appliance cluster in a company, typically set up by geographical region, business unit, or functional separation. These are the middlemen 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 Appliances that manage or monitor devices based on their assigned network segments. These Appliances reach out to BigFix through the CounterACT Connecting Appliance cluster(s).

• **Devices on the network** are the hardware assets whose information needs to be exchanged between the Forescout platform and BigFix. When these devices enter or leave the network, the Forescout platform monitors them and provides information.

In this context, when Forescout eyeExtend for IBM BigFix 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 a 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 advanced settings.

### What to Do

Perform the following steps to set up this integration:

1. Verify that requirements are met. See **Requirements** for details.
2. Download and install Forescout eyeExtend for IBM BigFix from the Forescout website: [www.forescout.com/support](http://www.forescout.com/support). See **Install the Module**.
3. Define a target BigFix instance and assign CounterACT Appliances to it. See **Establish Connection to a BigFix Root Server** for details.
4. Create policies for the Forescout platform to update BigFix assets. See **Create BigFix Policies Using Templates**.
5. When the configurations have been tested and the policies created, you are ready to **Work with Forescout eyeExtend for IBM BigFix**.

### Requirements

Verify that the following requirements are met:

• **Forescout Requirements**

• **IBM BigFix Requirements**

• **Supported Systems**

• **Forescout eyeExtend (Extended Module) Licensing Requirements**
Forescout Requirements

This module requires the following Forescout releases and other components:

- Forescout version 8.2.
- A module license for Forescout eyeExtend for IBM BigFix. See Forescout eyeExtend (Extended Module) Licensing Requirements.
- Microsoft Active Directory is recommended for the Create an IBM BigFix Active Directory Groups Policy.

IBM BigFix Requirements

The IBM BigFix requirements are as follows:

- IBM BigFix version 9.5.
- For information about the vendor models (hardware/software) and versions (product/OS) that are validated for integration with this Forescout component, refer to the Forescout Compatibility Matrix.
- Verify connectivity between the Forescout platform and targeted IBM BigFix servers to port 52311.
- Define a custom property on the BigFix server. See Add BigFix MAC Address Custom Property.

Supported Systems

Forescout eyeExtend for IBM BigFix works on the following platform:

- IBM BigFix Platform 9.5.0

Supported Sites

Forescout eyeExtend for IBM BigFix supports the following sites:

- Enterprise Security
- Patches* (anything that starts with Patches)
- Updates* (anything that starts with Updates)
- Client Manager for Anti-Virus

To enable BigFix sites, refer to the IBM documentation:

Forescout eyeExtend (Extended Module) Licensing Requirements

This Forescout eyeExtend product requires a valid license. Licensing requirements differ based on which licensing mode your deployment is operating in:

- Per-Appliance Licensing Mode
- Flexx Licensing Mode

To identify your licensing mode:
- From the Console, select Help > About Forescout.

Per-Appliance Licensing Mode

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

If you would like to continue exploring the module before purchasing a permanent license, you can request a demo license extension. Consult with your Forescout representative before requesting the extension. You will receive email notification and alerts at the Console before the demo period expires.

To continue working with the module after the demo period expires, you must purchase a permanent module license.

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

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

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

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

To view the number of currently detected devices:
1. Select the Home tab.
2. In the Views pane, select the All Hosts folder. The number in parentheses displayed next to the All Hosts folder is the number of devices currently detected.

Flexx Licensing Mode

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

*No demo license is automatically installed during system installation.*
License entitlements are managed in the Forescout Customer Portal. After an entitlement has been allocated to a deployment, you can activate or update the relevant licenses for the deployment in the Console.

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

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

More License Information

For more information on eyeExtend (Extended Module) licenses:

- **Per-Appliance Licensing.** Refer to the Forescout Administration Guide.
- **Flexx Licensing.** Refer to the Flexx Licensing How-to Guide.

You can also contact your Forescout sales representative for more information.

Install the Module

This section describes how to install the module. Before you install this module, verify that all of the Requirements are met.

**To install the module:**

1. Navigate to one of the following Forescout download portals, depending on the licensing mode your deployment is using:
   - **Product Updates Portal** - *Per-Appliance Licensing Mode*
   - **Customer Portal, Downloads Page** - *Flexx Licensing Mode*
   
   To identify your licensing mode, select Help > About ForeScout from the Console.

2. Download the module .fpi file.

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

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

5. Select Modules. The Modules pane opens.

6. Select Install. The Open dialog box opens.

7. Browse to and select the saved module .fpi file.

8. Select Install. The Installation screen opens.

9. Select I agree to the License Agreement to confirm that you have read and agree to the terms of the License Agreement and select Install. The installation cannot proceed unless you agree to the license agreement.
The installation begins immediately after selecting Install and cannot be interrupted or canceled.

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

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

Some components are not automatically started following installation.

Configure the Module

After Forescout eyeExtend for IBM BigFix is installed on your targeted CounterACT Appliance, configure the module to ensure that the Forescout platform can communicate with the BigFix deployment.

To complete the configuration of some of these connections, perform the following procedures:

1. (Optional) Create a BigFix Account
2. Establish Connection to a BigFix Root Server
3. Test Your Configuration

Create a BigFix Account

Forescout eyeExtend for IBM BigFix comes with a default administrator account, which you may use. Otherwise, you can create your own. For details, refer 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 need to map your CounterACT Appliance to a BigFix root server.

To add a BigFix connection:

1. In the Console toolbar, select Options from the Tools menu.
2. Select IBM BigFix from the Options pane.
3. In the BigFix Instance tab, select **Add**.

4. Configure the connection as follows:

<table>
<thead>
<tr>
<th><strong>BigFix Root Server (Host Name or IP)</strong></th>
<th>Enter the host name, a Fully Qualified Domain Name (FQDN) or the IPv4 address of the BigFix root server.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Username</strong></td>
<td>Enter the username used to access the BigFix root server.</td>
</tr>
<tr>
<td><strong>Password</strong></td>
<td>Enter the password used to access the BigFix root server. BigFix password restrictions apply.</td>
</tr>
<tr>
<td><strong>Verify Password</strong></td>
<td>Re-enter the password to verify it.</td>
</tr>
<tr>
<td>--------------------</td>
<td>------------------------------------</td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td>(Optional) Insert text, for example, a nickname of the BigFix connection. This is helpful if you have more than one BigFix connection.</td>
</tr>
<tr>
<td><strong>Validate Server Certificate</strong></td>
<td>Select this option to validate the identity of the third-party server before establishing a connection, when the eyeExtend product communicates as a client over SSL/TLS. To validate the server certificate, either of the following certificate(s) must be installed:</td>
</tr>
<tr>
<td></td>
<td>- Self-signed server certificate – the server certificate must be installed on the CounterACT Appliance</td>
</tr>
<tr>
<td></td>
<td>- Certificate Authority (CA) signed server certificate – the CA certificate chain (root and intermediate CA certificates) must be installed on the CounterACT Appliance</td>
</tr>
<tr>
<td></td>
<td>Use the Certificates &gt; Trusted Certificates pane to add the server certificate to the Trusted Certificate list. For more information about certificates, refer to the appendix, &quot;Configuring the Certificate Interface&quot; in the Forescout Administration Guide.</td>
</tr>
</tbody>
</table>

5. **Select Next.**
6. Configure the CounterACT device assignment as follows:

<table>
<thead>
<tr>
<th>Connecting CounterACT Device</th>
<th>Select the IP address of the 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 middleman between the BigFix instance and the CounterACT Appliance. The connecting CounterACT Appliance forwards all queries and requests to and from the BigFix instance.</th>
</tr>
</thead>
</table>
| 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 sends 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 if they are not explicitly assigned to another connecting Appliance. Select this option to make this connecting Appliance the middleman for all CounterACT Appliances not assigned to another connecting Appliance. |

For more information, see Deployment Options.

7. Select Next.

8. Configure the advanced settings as follows:

| Maximum number of actions allowed within a period of 1 minute | This setting limits the number of actions sent to this BigFix instance and prevents the BigFix instance from becoming inundated.  
- Select Use Default to use the default setting of one action per minute timeframe.  
- Select Specify and set the number of action items per minute timeframe. |

9. Select Finish. The server is listed in the BigFix Instance tab.
The best practice is to perform a **Test** after setting up a connection. See **Test Your Configuration**.

**Add BigFix Properties**

You can add custom BigFix properties in addition to the default Forescout 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 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.
6. Select **Add**.

7. Configure the following properties:

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Label</strong></td>
<td>Create a name or a label to associate to this new property. This label is displayed in the Asset Inventory view, Host tab in the Console.</td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td>(Optional) Insert text, for example, the nickname of this host property you are creating.</td>
</tr>
<tr>
<td><strong>Type</strong></td>
<td>From this drop-down menu, select the type of data the property contains. Single-value properties contain one value: string, Boolean, date, or integer.</td>
</tr>
</tbody>
</table>
8. Select **Next**.

9. Configure the following properties:

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display BigFix Property in Asset Inventory View</td>
<td>Select this option to display this property in the Asset Inventory tab.</td>
</tr>
<tr>
<td>Inventory Description</td>
<td>Enter a description of the property you want to display in the Asset Inventory. This description is displayed if <strong>Display BigFix Property in Inventory View</strong> is selected.</td>
</tr>
<tr>
<td>Display BigFix Property in Host Profiles Pane of Home View and Assets Portal</td>
<td>Selected by default, this option lists this property in the Profiles tab of the Home view and in the Assets portal.</td>
</tr>
<tr>
<td>Enable Track Changes</td>
<td>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. Select <strong>Enable Track Changes</strong> 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.</td>
</tr>
<tr>
<td>Track Name</td>
<td>The name of the property entered in the Label field in the General pane populates this field.</td>
</tr>
</tbody>
</table>
**Track Description**
The text from the Tag field in the General pane populates this field.

10. Select **Finish**. The property is added to the table in the BigFix Property tab.
11. Repeat the steps for every host property you want to create and use.
12. When finished, in the IBM BigFix pane, select **Apply**. The Forescout platform saves the configurations, updates the internal database, and restarts Forescout eyeExtend for IBM BigFix. It may take 1-2 minutes for the changes to take effect.
13. 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 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.
4. Select **Add**. The Add Fixlet dialog box opens.
   - *Custom Fixlets are not supported.*
5. Configure the following settings:

<table>
<thead>
<tr>
<th>Site</th>
<th>Select the site from the drop-down menu.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Selected the name you want to add. There may be multiple names to choose from.</td>
</tr>
<tr>
<td>Action</td>
<td>Select the appropriate action. A BigFix Fixlet may have multiple actions associated with the selected Name. If the Fixlet has no assigned actions, you cannot import that Fixlet into the Forescout platform.</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 is displayed in the IBM BigFix pane.
7. Select **Apply**. This Fixlet is now displayed in the **Policy Actions**.
**Edit BigFix Connection**

You can edit the BigFix connection, for example, if you need to change the connecting Appliance or assign a different CounterACT Appliance to the connecting Appliance.

**To edit a BigFix connection:**

1. In the Modules pane, select **IBM BigFix**. The BigFix pane opens.
2. Select the instance and then select **Edit**.
3. Edit the connection properties and select **OK**.

**Test Your Configuration**

After you configure a BigFix connection, it is recommended that you test the configuration.

**To test the configuration:**

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 fails. To correct this, add administrator rights to your BigFix account.

3. If the test fails, check your configuration and re-test.
4. If the test passes, repeat step 2 for any additional connections.

**Delete BigFix Instance**

The process for deleting a BigFix instance is as follows:
1. Remove BigFix Fixlets associated with the BigFix instance.
2. Remove BigFix Properties associated with the BigFix instance.
3. Remove the BigFix Root Server.

**Remove BigFix Fixlets**

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

To remove BigFix Fixlets:
1. In the 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. When prompted for confirmation, select OK.
6. Repeat the steps for other properties, as necessary.

Continue to the Remove BigFix Properties section.

**Remove BigFix Properties**

After you remove the BigFix properties, you can remove the BigFix root server.

To remove BigFix properties:
1. In the 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. When prompted for confirmation, select **OK**.
6. Repeat the steps for other properties, as necessary.
7. Continue to the **Remove the BigFix Root Server** section.

**Remove the BigFix Root Server**

After you delete the BigFix Fixlets and Properties, you can remove the BigFix instance from the Forescout platform.

**To remove a BigFix connection:**

1. In the 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. When prompted for confirmation, select **OK**.
5. In the IBM BigFix pane, select **Apply**.
Manually Verify BigFix Agent is Running

(Optional) You can verify the BigFix Agent is running on your endpoints.

To verify the BigFix Agent is running:

1. Go to Computer and then select Manage. The Computer Management dialog box opens.
2. Expand Services and Applications and then select Services.
   The path to the executable should be: \Program Files (x86)\BigFix Enterprise\BES Client\BESClient.exe.
4. Select OK.

Create BigFix Policies Using Templates

Forescout platform 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 Forescout eyeExtend for IBM BigFix, Forescout
platform policies can include collecting BigFix client, relay and server each host is using.

This section describes how to use BigFix templates to create policies to detect, manage, and remediate devices in a BigFix environment. Refer to the following sections:

- Create an IBM BigFix Active Directory Groups Policy
- Create an IBM BigFix Agent Compliance Policy
- Create an IBM BigFix Patch Compliance Policy

**Create an IBM BigFix Active Directory Groups Policy**

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 create a policy:**

1. Log in to the Console and select **Policy**.
2. Select **Add** from the Policy Manager. The Policy Wizard opens.
3. Expand **IBM BigFix** and select **IBM BigFix Active Directory Groups**.
4. Select **Next**.
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 are taken.
   - Ensure that the name indicates whether the policy criteria must be met or not met.
   - Avoid having another policy with a similar name.

   Policy names are displayed in the Policy Manager, the Views pane, NAC Reports and in other features. Precise names make working with policies and reports more efficient.

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

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

   The following options are available:
- **All IPs**: Include all IP addresses in the Internal Network.
- **Segment**: Select a previously defined segment of the network. To specify multiple segments, select **OK** or **Cancel** to close this dialog box, and select **Segments** from the Scope pane.
- **Unknown IP addresses**: Apply the policy to endpoints whose IP addresses are not known. Endpoint detection is based on the endpoint MAC address.

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

**9.** Select **Next**. The Main Rule pane opens.

**10.** The main rule detects if the endpoint is managed by Active Directory. For details, see [How Devices Are Detected and Handled](#).

**11.** Review/edit the main rule conditions and actions. For details, see [Policy Properties](#) and [Policy Actions](#).

**12.** Select **Next**. The Sub-Rule pane opens.
13. Review/edit the sub-rule conditions and actions as follows:
   a. In the Sub-Rules pane, double-click a sub-rule to open it. The Policy dialog box opens for the selected sub-rule.
   b. Add conditions and actions as required. For details, see Policy Properties and Policy Actions.
   c. Select OK.


15. In the Policy Manager, select Apply.

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 the Forescout platform how to detect and handle devices defined in the policy scope.

The main rule of this policy template detects if the endpoint is managed by Active Directory. The condition criteria for the main rule are populated by default. 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.

The sub-rules of the IBM BigFix Active Directory Groups policy list the items the Forescout platform is to check when applying the main rule. Sub-rules are checked 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.
Create an IBM BigFix Agent Compliance Policy

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.

Create a BigFix Agent Compliance Policy

Use the IBM BigFix Agent Compliance policy template to create a Forescout platform 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 create a policy:

1. Log in to the Console and select Policy.
2. Select Add from the Policy Manager. The Policy Wizard opens.
3. Expand IBM BigFix and select IBM BigFix Agent Compliance.
4. Select Next.
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 are taken.
   - Ensure that the name indicates whether the policy criteria must be met or not met.
   - Avoid having another policy with a similar name.

   *Policy names are displayed in the Policy Manager, the Views pane, NAC Reports and in other features. Precise names make working*

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

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

![IP Address Range](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 is displayed in the Scope pane.

9. Select **Next**. The Main Rule pane opens. The main rule detects if the endpoint is managed by BigFix by checking the last reported agent version. For details, see How Devices Are Detected and Handled.

10. Select **Next**. The Sub-Rule pane opens.
11. Review/edit the sub-rule conditions and actions as follows:
   a. In the Sub-Rules pane, double-click a sub-rule to open it. The Policy dialog box opens for the selected sub-rule.
   b. Add conditions and actions as required. For details, see Policy Properties and Policy Actions.
   c. Select OK.
12. In the Sub-Rules pane, select Finish.
13. In the Policy Manager, select Apply.

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 the Forescout platform 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 checked 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.
The sub-rules of the IBM BigFix Agent Compliance policy list the items the Forescout platform is to check when applying the main rule.

Create an IBM BigFix Patch Compliance Policy

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, Forescout eyeExtend for IBM BigFix flags that endpoint as non-compliant.

To use the IBM BigFix Patch Compliance policy template:

1. Log in to the Console and select Policy.
2. Select Add from the Policy Manager. The Policy Wizard opens.
3. Expand IBM BigFix and select IBM BigFix Patch Compliance.
4. Select Next.
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 are taken.
   - Ensure that the name indicates whether the policy criteria must be met or not met.
   - Avoid having another policy with a similar name.

   Policy names are displayed in the Policy Manager, the Views pane, NAC Reports and in other features. Precise names make working

6. Select Next. Both the Scope pane and the IP Address Range dialog box open.
7. Use the IP Address Range dialog box to define which endpoints are inspected.
- **All IPs**: Include all IP addresses in the Internal Network.
- **Segment**: Select a previously defined segment of the network. To specify multiple segments, select **OK** or **Cancel** to close this dialog box, and select **Segments** from the Scope pane.
- **Unknown IP addresses**: Apply the policy to endpoints whose IP addresses are not known. Endpoint detection is based on the endpoint MAC address.

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

9. Select **Next**. The Main Rule pane opens.

10. The main rule detects Windows devices identified by the Forescout platform as in scope for the IBM BigFix Patch Compliance policy. For details, see **How Devices Are Detected and Handled**.

11. Review/edit the main rule conditions and actions. For details, see **Policy Properties** and **Policy Actions**.

12. Select **Next**. The Sub-Rules pane opens.
13. Review/edit the sub-rule conditions and actions as follows:
   a. In the Sub-Rules pane, double-click a sub-rule to open it. The Policy dialog box opens for the selected sub-rule.
   b. Add conditions and actions as required. For details, see Policy Properties and Policy Actions.
   c. Select OK.


15. In the Policy Manager, select Apply.

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 the Forescout platform 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 checked 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 detects all Windows devices identified by the Forescout platform as in scope for the IBM BigFix Patch Compliance policy.
The sub-rules of the IBM BigFix Patch Compliance policy list the items the Forescout platform is to check when applying the main rule.

Create Custom BigFix Policies

You can 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 Forescout eyeExtend for IBM BigFix is installed.

Forescout platform policies contain a series of rules. Each rule includes:

- Conditions based on host property values. The Forescout platform 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 to be applied to hosts that match the conditions of the rule.

To create a custom policy:

1. In the Console, select **Policy**. The Policy Manager opens.
2. Select **Add** to create a policy. The Policy Type wizard opens.
3. Select **Custom** and configure the policy or select **Help** for more information about working with policies.

Policy Properties

In addition to the bundled Forescout 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 Forescout properties:

1. Go to the Properties tree from the Policy Conditions dialog box.
2. Expand **BigFix** in the Properties tree.
The following default properties are included with Forescout eyeExtend for IBM BigFix:

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>BigFix Active Directory Path</strong></td>
<td>Indicates the Active Directory service's distinguished name (DN).</td>
</tr>
<tr>
<td><strong>BigFix Agent Version</strong></td>
<td>Indicates the version of BigFix Agent on endpoint.</td>
</tr>
<tr>
<td><strong>BigFix BES Relay Selection Method</strong></td>
<td>Indicates the BigFix Agent Relay selection method.</td>
</tr>
<tr>
<td><strong>BigFix Computer Name</strong></td>
<td>Indicates the Computer Name of endpoint.</td>
</tr>
<tr>
<td><strong>BigFix CPU</strong></td>
<td>Indicates the CPU usage on endpoint.</td>
</tr>
<tr>
<td><strong>BigFix Device Type</strong></td>
<td>Indicates the endpoint device type.</td>
</tr>
<tr>
<td><strong>BigFix Free Disk Details</strong></td>
<td>Indicates the amount of free space on the endpoint.</td>
</tr>
<tr>
<td><strong>BigFix Total Disk Details</strong></td>
<td>Provides disk information.</td>
</tr>
<tr>
<td><strong>BigFix Distance to BES Relay</strong></td>
<td>Indicates the number of hops from the BES Relay.</td>
</tr>
<tr>
<td><strong>BigFix DNS Name</strong></td>
<td>Indicates the DNS Name associated with endpoint.</td>
</tr>
<tr>
<td><strong>BigFix Endpoint Locked</strong></td>
<td>Returns whether the endpoint is locked or not.</td>
</tr>
<tr>
<td><strong>BigFix Installed Apps</strong></td>
<td>Indicates installed Apps on the endpoint.</td>
</tr>
<tr>
<td>BigFix Property</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------------------</td>
<td>-------------------------------------------</td>
</tr>
<tr>
<td>BigFix Last Reported Time</td>
<td>Indicates 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>Indicates the relay the endpoint is connected to.</td>
</tr>
<tr>
<td>BigFix Relay Name of Client</td>
<td>Indicates the client relay name.</td>
</tr>
<tr>
<td>BigFix Remediation Items</td>
<td>Lists the missing patches on endpoint.</td>
</tr>
<tr>
<td>BigFix Running Process</td>
<td>Lists the running processes.</td>
</tr>
<tr>
<td>BigFix Running Services</td>
<td>Lists the running services.</td>
</tr>
<tr>
<td>BigFix Unix Installed Debian Packages and Repositories</td>
<td>Lists the Unix-installed Debian packages.</td>
</tr>
<tr>
<td>BigFix Unix Installed RPM Packages and Repositories</td>
<td>Lists the 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, refer to the IBM BigFix Platform documentation page.

3. When finished, select OK.

Add BigFix MAC Address Custom Property

The BigFix MAC address custom property is used by eyeExtend for IBM BigFix to query the endpoint ID, which is later used to query the detailed endpoint properties. The custom property collects all the MAC addresses on an endpoint.

If the BigFix MAC address custom property is not defined, the endpoint ID query will return an empty result and cause other BigFix properties to be irresolvable.

To add the BigFix MAC address custom property:

1. Log in to the IBM BigFix Console.
2. Select **Tools** and then select **Manage Properties**.
3. Configure the following settings:

<table>
<thead>
<tr>
<th>Name</th>
<th>Custom::BigFix MAC Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Relevance</td>
<td>mac addresses of adapters whose (not loopback of it) of network</td>
</tr>
<tr>
<td>Evaluate every</td>
<td>Every Report</td>
</tr>
</tbody>
</table>

4. Select OK.

**Add Optional Host Properties**

In addition to the default policy properties, you can add optional host properties. The Forescout platform can get a customizable number of additional host details from Unix/Win/Mac platforms, including chassis type, memory information, disk details, and more.

Host properties are information stored in the Forescout platform for each device discovered on the network. When you work with this module, you create new Forescout platform host properties to hold data extracted by querying the BigFix root server. This makes retrieved data available for use in Forescout platform policies.

You can create single-value properties that contain one value, for example, a string property that contains the GUID of the device. This version supports only string, integer, date, and Boolean property types.

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.

**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.

- Fixlets defined under custom sites are not supported.
To create a custom site:

Follow the instructions on the IBM BigFix Creating Custom Site page:

Your custom site must be named: Forescout Custom Site.

Define Host Properties

To define Forescout host properties:

1. In the 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.

4. Select Add.
5. Configure the following properties:

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Label</strong></td>
<td>Create a name or a label to associate to this new property. This label is displayed in the Asset Inventory view, Host tab in the Console.</td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td>(Optional) Insert text, for example, the nickname of this host property.</td>
</tr>
<tr>
<td><strong>Type</strong></td>
<td>From this drop-down menu, select the type of data the property contains. Single-value properties contain one value: string, Boolean, date, or integer.</td>
</tr>
</tbody>
</table>

6. Select **Next**.
7. Configure the following properties:

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display BigFix Property in Asset Inventory View</td>
<td>Select this option to display this property in the Asset Inventory tab.</td>
</tr>
<tr>
<td>Inventory Description</td>
<td>Enter a description of the property to display in the Asset Inventory. This description is only displayed if <strong>Display BigFix Property in Asset Inventory View</strong> is selected.</td>
</tr>
<tr>
<td>Display BigFix Property in Host Profiles Pane of Home View and Assets Portal</td>
<td>Selected by default, this option lists this property in the Profiles tab of the Home view and in the Assets portal.</td>
</tr>
<tr>
<td>Enable Track Changes</td>
<td>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. Use the change property in policies to identify changes in the property values retrieved from the BigFix instance.</td>
</tr>
<tr>
<td>Track Name</td>
<td>The text you entered in the Label field in the General pane populates this field. This field names the item you want to track.</td>
</tr>
<tr>
<td>Track Description</td>
<td>The text from the Tag field in the General pane populates this field and describes the Track Name.</td>
</tr>
</tbody>
</table>

8. Select **Finish**. The property is added to the table in the BigFix Property tab.
9. Repeat for every host property you want to create and use.
10. In the IBM BigFix pane, select **Apply**. The Forescout platform saves the configuration, updates the internal database, and restarts Forescout eyeExtend for IBM BigFix.

   *It may take 1-2 minutes for the changes to take effect.*

**Policy Actions**

In addition to the bundled Forescout 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.

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

**To access Forescout eyeExtend for IBM BigFix actions:**

1. In the Console, go to the Actions tree from the Policy Conditions dialog box.
2. Expand **BigFix** in the Actions tree. Select one of the following 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. In the Actions tree, expand **BigFix Fixlet**, and then select **Run Fixlet**.
2. Select **Custom Fixlet Name**.

3. Select the Schedule tab. You can use 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.

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

1. In the Actions tree, expand **BigFix Linux**, and then select **Run Script on Linux**.
2. In the Parameters tab, select the command or script you want to run from the **Command or Script** drop-down list, and continue to step 10.

3. If you need to import a script, select **Download**.

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

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

7. The File Editor is populated 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:

   ```bash
   Is al > abc.txt
   ```

   Select **Add Tags**.

10. Select the Schedule tab. You can use 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 let you 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.

**To configure the BigFix Execution Operations action:**

1. In the Actions tree, expand **BigFix Windows**, and then select **BigFix Execution Operations**.
2. From the **Command** drop-down menu, select an item (**dos**, **run**, **script**, or **wait**).

3. If you select **script**, enter the script or command parameters in 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 **Parameters** field and then select **Add Tags**.

5. Select the Schedule tab. You can use 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. In the Actions tree, expand **BigFix Windows**, select **BigFix File Operations - Copy**.
2. In the Parameters tab, enter the source filename in the **Source file** field 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. 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 into the Source File or Destination File fields. Click in the field and select **Add Tags**.

5. Select the Schedule tab. You can use 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. In the Actions tree, expand **BigFix Windows**, select **BigFix File Operations - Delete**.
2. In the Parameters tab, enter the filename in 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 in the field and then select Add Tags.

4. Select the Schedule tab. You can use 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. In the Actions tree, expand BigFix Windows, select BigFix File Operations - Download.
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 in the field and then select Add Tags.

4. Select the Schedule tab. You can use 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. In the Actions tree, expand BigFix Windows, select BigFix File Operations - Move.
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. 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 in the **Source File** or **Destination File** fields. Click in the field and select **Add Tags**.

5. Select the Schedule tab. You can use 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 deleting a registry key in Windows OS.

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

1. In the Actions tree, expand **BigFix Windows**, select **BigFix Registry - Delete**.
2. In the Parameters tab, enter the Registry Key in the required format. For example: [HKEY_LOCAL_MACHINE\Software\BigFix\TestKey].

3. Enter the value name in the Value Name field, for example, testValueName. The name cannot contain any spaces.

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 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. In the Actions tree, expand BigFix Windows, select BigFix Registry - Set.
2. In the Parameters tab, enter the **Registry Key** in the required format. For example: `HKEY_LOCAL_MACHINE\Software\BigFix\TestKey`

3. Enter the value name in the **Value Name** field, for example, `testValueName`. The name cannot contain any spaces.

4. Enter the value in the **Value** field, for example, `testValue`. The value cannot contain any spaces.

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 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.
Work with Forescout eyeExtend for IBM BigFix

Once Forescout eyeExtend for IBM BigFix has been configured, you can view and manage the devices from the Asset Inventory view in the Console. This provides activity information, accurate at the time of the poll, on endpoints based on specific instances’ properties. The Asset 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 asset inventory detections into policies

Access the Asset Inventory

To access the asset inventory:

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

If you did not configure the module to show the property in the Asset Inventory tab, your BigFix properties are not displayed in the Views pane of the Asset Inventory tab.

3. In the Views pane, expand **BigFix** and select any item 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 Console, select **Home**.
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 selected host.
Appendix 1: Permissions for a Restricted User

If your BigFix administrator requires more security in regard to user permissions, you need to set restricted access to the API user. You can restrict a user’s permissions in your BigFix BES Console account.

**To restrict user permissions:**

1. Log in to your BigFix BES Console.
2. In the left pane, select Operators. The Operators pane opens.
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>

| Post-Action Behavior               | None                 | None                 |
| Action Script Commands             | None                 | None                 |

**Interface Login Privileges**

| Can use Console                    | No                   | No                    |
| Can use WEBUI                       | No                   | No                    |
| Can use REST API                    | Yes                  | Yes                   |

5. Select **Save Changes**.

6. You can optionally test your changes by running a test (see [Test Your Configuration](#)).

When adding a new Operator, ensure that you have allocated patching sites, as well as assigned all computers to that operator that will be managed by the Forescout platform.
Additional Forescout Documentation

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

- Documentation Downloads
- Documentation Portal
- Forescout Help Tools

Documentation Downloads

Documentation downloads can be accessed from the Forescout Technical Documentation Page, and one of two Forescout portals, depending on which licensing mode your deployment is using.

- **Per-Appliance Licensing Mode** – Product Updates Portal
- **Flexx Licensing Mode** – Customer Support Portal

Software downloads are also available from these portals.

To identify your licensing mode:

- From the Console, select Help > About Forescout.

Forescout Technical Documentation Page

The Forescout Technical Documentation Page provides access to a searchable, web-based Documentation Portal as well as PDF links to the full range of technical documentation.

To access the Technical Documentation Page:

- Go to https://www.Forescout.com/company/technical-documentation/

Product Updates Portal

The Product Updates Portal provides links to Forescout version releases, Base and Content Modules, and eyeExtend products, as well as related documentation. The portal also provides a variety of additional documentation.

To access the Product Updates Portal:

- Go to https://updates.forescout.com/support/index.php?url=counteract and select the version you want to discover.

Customer Support Portal

The Downloads page on the Forescout Customer Support Portal provides links to purchased Forescout version releases, Base and Content Modules, and eyeExtend products, as well as related documentation. Software and related documentation will only appear on the Downloads page if you have a license entitlement for the software.
To access documentation on the Customer Support Portal:
  - Go to https://Forescout.force.com/support/ and select Downloads.

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

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

**Forescout Help Tools**
Access information directly from the Console.

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

**Forescout Administration Guide**
  - Select Administration Guide from the Help menu.

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

**Documentation Portal**
  - Select Documentation Portal from the Help menu to access the Documentation Portal.