Application Control Administrator Guide

Special notice

Before using this information and the product it supports, read the information in Notices.

Edition notice

This edition applies to version 10.0 of BigFix and to all subsequent releases and modifications until otherwise indicated in new editions.

Contents

Chapter 1. Overview

Set a secure environment by using Application Control.

BigFix® Application Control is a lightweight, native enforcement system designed for comprehensive management of application execution across enterprise endpoints. The solution addresses the critical need for native, policy-driven application control within BigFix environments.

Note:

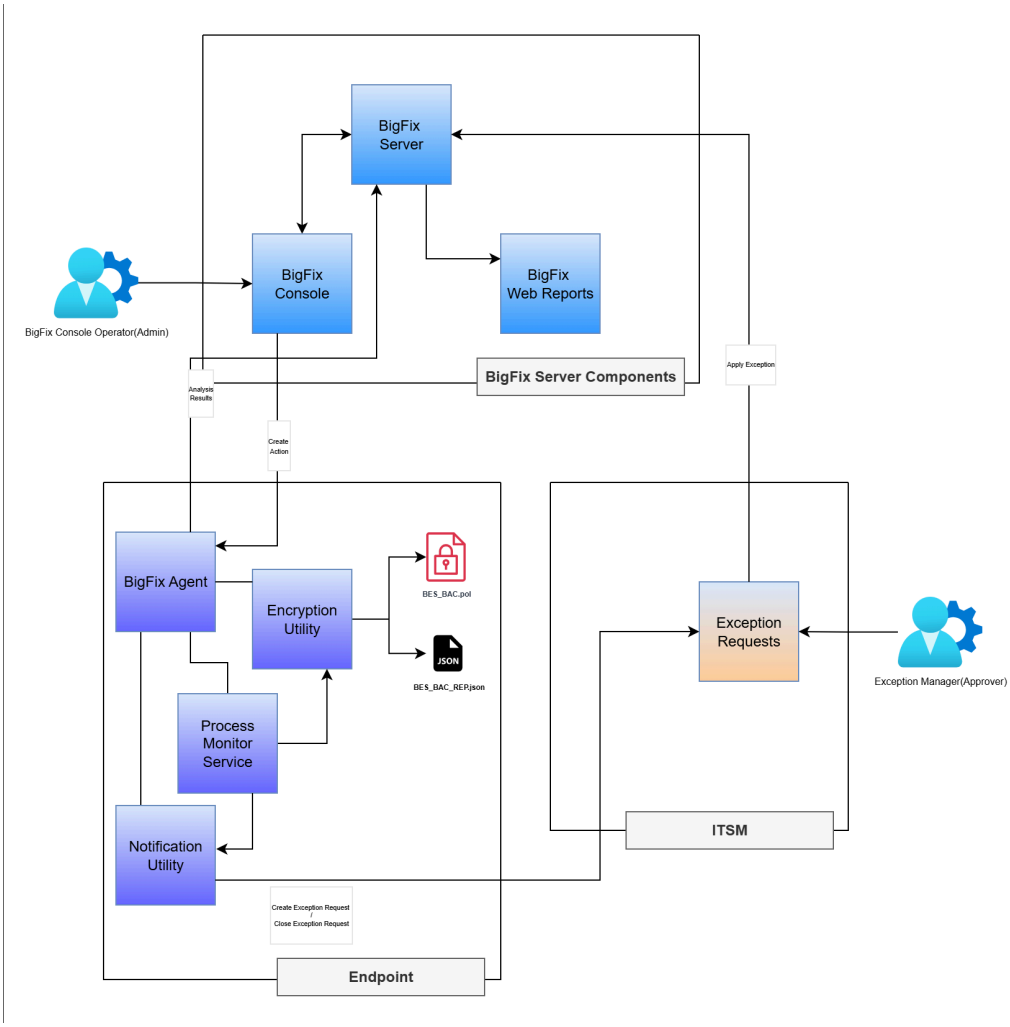
- BigFix Application Control currently supports application enforcement for both physical and virtual Windows™ (environment) devices only.
- Non-windows environment (macOS™ & UNIX™/Linux™) support is planned in the future.

System Architecture Diagram

The system architecture diagram of Application Control.

For a better understanding of BigFix Application Control refer to its system architecture diagram below:

Figure 1. BigFix® Application Control Architecture



The above diagram shows how the BigFix Server components interact with BigFix endpoints and third-party ITSM applications (like ServiceNow™ for raising exception approval tickets).

The system architecture diagram illustrates the interaction between BigFix Server components, BigFix endpoints, and third-party ITSM applications/solutions, such as ServiceNow™ for exception approval tickets. This visual representation aids in understanding the structure and functionality of the BigFix Application Control system.

For Application Control to work properly, we need the following three components:

- **BigFix Server Components**

  Application Control mainly utilizes the following three BigFix® Server Components:

  - **BigFix® Core Server**

    This is the central processing component for this solution. It manages all communications with the BigFix clients (agents), distributes content (like Fixlets, tasks, and analysis), and enforces policies. It is accepts REST

API calls from ITSM applications/solutions (like ServiceNow™) to execute action to allow the blocked app.

- **BigFix® Console**

  The console is the primary administrative interface for BigFix Application Control. It is a key part of the server-side infrastructure used to manage all aspects of the environment, including creating content and deploying actions. All BigFix Console integrations will be in the External Site.

- **BigFix® Web Reports**

  It provides a web-based interface for reporting and data visualization. The BigFix Agent on the endpoint runs an analysis and sends the result to the BigFix server. Below are the administrative reports that are shown for Application Control:
  - Effective Policy on Endpoint
  - Approved Exceptions
  - Endpoints With BAC Service

- **Endpoints**

  There are three services running along with BigFix® Agent in the endpoint machines. The BigFix agent receives instructions from BigFix® console to install following services:

  - **Process Monitor Service**

    This component is deployed as a Windows® service, and will receive notifications of process executions using the `ManagementEventWatcher` class, and the service will compare the process meta data generated by the process execution events against the Effective Policy (`bes_bac.pol`) on the endpoint. If a process is to be blocked, the service will kill the process and initiate the Notification Utility to notify the logged in user of a blocked process. Default location for this service is `C:\Program Files (x86)\BigFix Enterprise\BES Client\BAC\`.

  - **Notification Utility**

    Since the Process Monitor Service will be running in a non-interactive session, a notification utility is there to enable notification of the logged in users for a blocked process event. Upon invocation, this utility presents the logged in user with an alert indicating that a process has been blocked. Default location for this service is `C:\Program Files (x86)\BigFix Enterprise\BES Client\BAC\`

  - **Encryption Utility**

    Encryption Utility is used to encrypt and decrypt the data into files. Latest payload data is encrypted through this utility and updated into the `bes_bac.pol` file and the latest payload data (in decrypted form) is

updated to the `bes_bac.rep` file for reporting on BigFix® Web Reports. Default location for this service is `C:\Program Files (x86)\BigFix Enterprise\BES Client\BAC\`

- **ITSM Applications (like ServiceNow™)**

  ServiceNow™ is an ITSM application/tool where each exception raised from the endpoint through Notification Utility is created as a ticket. This ticket needs to be approved by the exception manager. Once the ticket is approved, BigFix Action API is called to send the approved exception to the respective endpoint and allow the blocked application on that endpoint machine. When an endpoint receives the approval for an exception, an action is executed to update the ServiceNow™ ticket with the status: fulfilled/completed. From the endpoint machine, an unauthenticated ServiceNow™ API is called to raise an exception on the blocked application.

User Roles

This document outlines the various user roles associated with the BigFix Console, including the Policy Manager/Administrator, Desktop User, and Exception Manager. Each role is defined with its responsibilities and interactions within the system, providing clarity on user responsibilities in managing and utilizing the solution.

The following user roles are present in BigFix® Application Control:

- **Policy Manager/Administrator**

  This role is the BigFix Console User/Operator, who deploys and configures the Application Control policies, creates and manages the control rules, and reviews the effective configuration of the endpoints.

- **Desktop User**

  A user of an endpoint that is managed/restricted by BigFix Application Control. Such users can also be called the end users. They receive notifications when applications are blocked and can raise exceptions through the Notification Utility.

- **Exception Manager**

  A user of an ITSM application/solution who is authorized to approve or reject the exception requests raised by the desktop or end users. They review the exception requests in the ITSM application, approve or deny temporary access requests, set time limitations on exceptions, and ensure compliance with their organization's security policies.

Key concepts and terminology

Application Control enables policy-driven management of application usage on Windows devices within BigFix. This document outlines key terms such as Application Control Policy, Application Control Rule, CSV Ruleset File, and Effective Control Policy, which are essential for understanding the functionality and configuration of Application Control.

Application Control provides the functionality of a policy-driven way to control and enforce application usage across managed Windows physical devices only in BigFix.

Some important Application Control terms are described below:

- **Application Control Policy:**

  A collection of rules that is applied to an endpoint to restrict or allow the execution of an application or process.

- **Application Control Rule:**

  A configuration that instructs the monitoring service on the endpoint to allow or block the execution of an application or process.

- **CSV Ruleset File:**

  A CSV file with Application Control Rules to be enforced on the endpoints that are subscribed to the content site it has been uploaded to.

- **Effective Control Policy:**

  A collective ruleset consisting of CSV Ruleset Files and Individual Control Rules applied to an endpoint.

Audience

This guide is intended for administrators overseeing Application Control, detailing the features available in the BigFix® interface. It covers tasks such as installation, configuration, rule management, and monitoring, providing essential information for effective administration.

This guide is for administrators who want to supervise and manage Application Control.

It provides details of the features that are available to an admin user when using the Application Control interface in BigFix®. For example: installing and configuring Application Control on endpoints, creating and managing the control rules (by allowing or blocking processes), monitoring the watcher service (BigFix® Application Control service), viewing the effective configuration of an endpoint from the BigFix® Console, viewing the approved exceptions on an endpoint from the BigFix console or Web Reports, uploading control rules to a Content Site from where subscribed computers will add the rulesets to their effective policy.

Let us explore the above points in detail in the following topics:

- Installing BigFix Application Control *(on page 10)*
- Managing BigFix Application Control *(on page 17)*

Chapter 2. Installing BigFix® Application Control

Install BigFix Application Control in two steps: first, identify the endpoints lacking the application, and second, execute the installer task on those endpoints. This process ensures that the application is properly deployed across your desired systems.

You can perform the installation of BigFix Application Control in two steps by executing the specific Fixlet and tasks on the desired endpoints. First identify the endpoints that do not yet have Application Control on them. Second, run the installer task for BigFix Application Control on the desired endpoints to install Application Control on them.

Identifying Endpoints Not Configured for Application Control

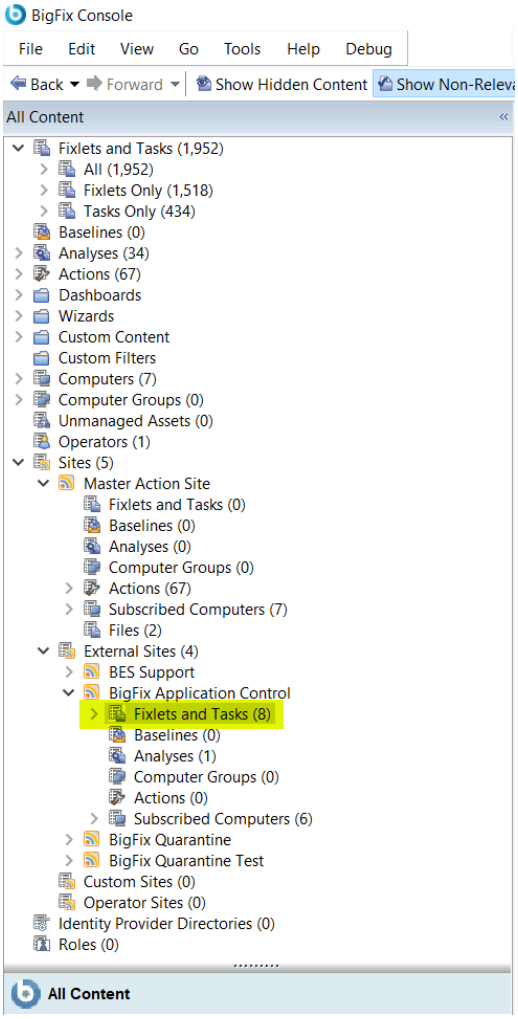
Use this Fixlet to identify endpoints that are not configured for Application Control, serving as a prerequisite for installation. This Fixlet lists devices that are not protected by the application but are subscribed to the external site, allowing administrators to assess endpoint readiness.

Use this Fixlet to identify endpoints that are not yet configured for BigFix Application Control.

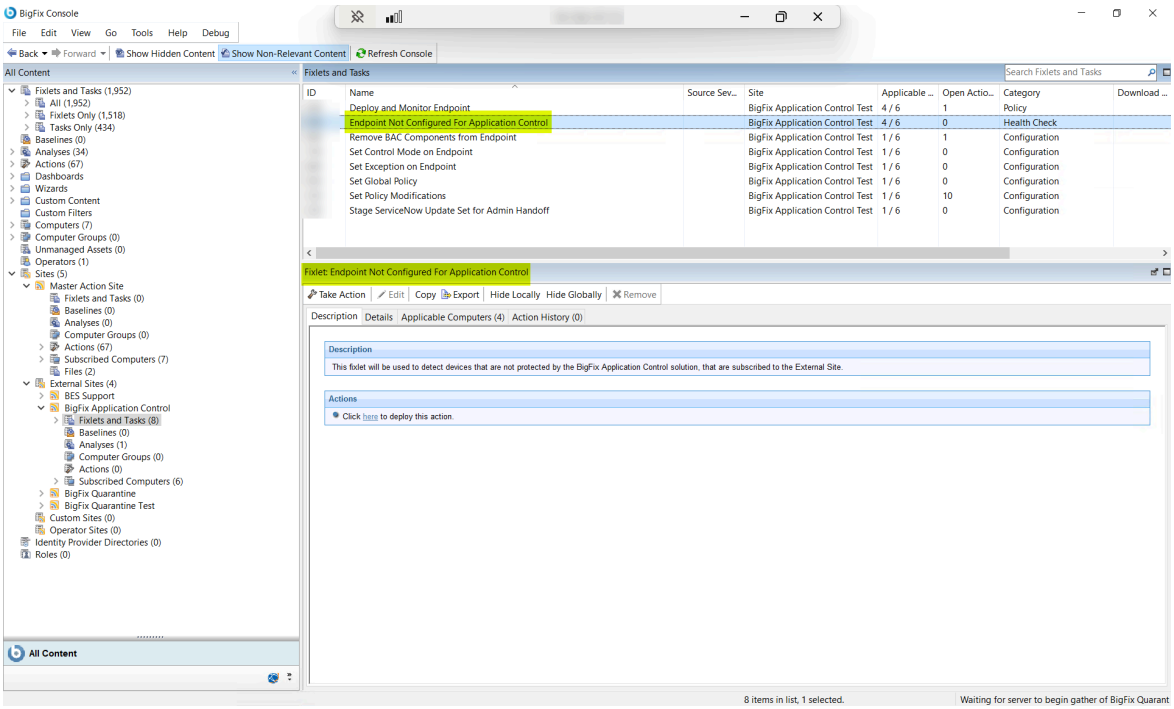
This identification step *can be* considered as a prerequisite for installing Application Control on an endpoint. You need to use **Fixlet: Endpoint Not Configured For Application Control** to identify the endpoints or devices that are not protected by BigFix Application Control but are subscribed to the external site. This Fixlet will list the devices on which you can configure Application Control.

1. In the BigFix Console, navigate to **All Content > BigFix Application Control > Fixlets and Tasks**.

Figure 2. Navigate to Fixlets & Tasks

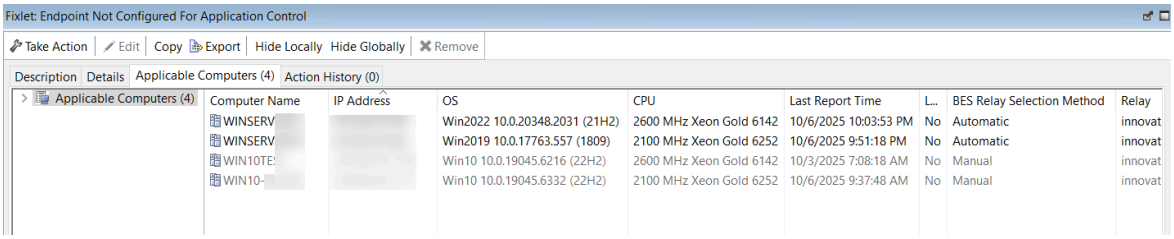


2. From the **Fixlets and Tasks** pane, select **Fixlet: Endpoint Not Configured For Application Control**.



This Fixlet does not contain any action script and the result set is based on client relevance's to get the details of devices not managed by Application Control.

3. Select the **Applicable Computers** tab and view the list of devices not managed by Application Control.



This Fixlet is more of a health-check Fixlet that can be used by administrators before installing the solution on any BigFix® managed endpoint.

Deploying & Monitoring Endpoints Using Application Control

This topic outlines the process for deploying and monitoring endpoints using Application Control through a specific installer task. It details the steps for installation, service configuration, and policy enforcement to ensure application allowlisting and unauthorized process blocking on managed endpoints.

It is recommended to first run the **Fixlet: Endpoint Not Configured For Application Control** to identify non-managed endpoints before running the installer task.

Use this task to deploy and monitor Application Control to endpoints that are not yet managed by the solution.

You can install BigFix Application Control using **Task: Deploy And Monitor Endpoint**. By running this task on an endpoint, you will deploy and activate a custom BigFix® Application Control (BAC) service on a Windows™ endpoint and a user pop-up service. This service enforces an application allowlisting policy and blocks unauthorized processes from running on the endpoint.

This task performs a multi-step process to install, configure, and enable the BAC service to monitor and control application software. The steps are as follows:

1. **Installation & setup**

   In this step, the task first downloads the three pre-requisite files - `.NET 8 SDK`, `ProcessMonitorService.zip`, and `NotificationUtility.zip`. Post downloading, the task installs the .NET 8 SDK, creates a dedicated folder at `\Program Files (x86)\ BigFix Enterprise\ BES Client\BAC`, and unzips the `ProcessMonitorService.zip` and `NotificationUtility.zip` files in the folder.

2. **Service & policy configuration**

   In this step, the task creates a Windows™ service called `BESBAC`. This service is configured to:
   - run the ProcessMonitorService.exe,
   - start automatically with the system, and
   - automatically attempt to restart if it fails.

   Next, the task deploys a security policy by generating a JSON policy file `effective_policy.json`. This policy works in a default-deny mode, which means that all applications are blocked for running except those explicitly allowed. The initial policy is a allowlist for:
   - essential Windows™ system processes
   - BigFix agent processes
   - any other processes running from `C:\Windows directory`

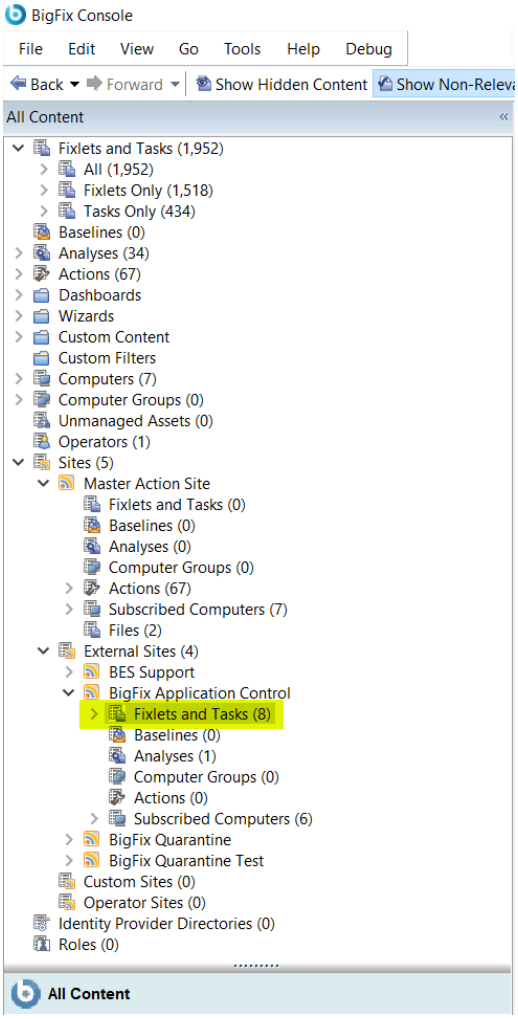
3. **Activation & Monitoring**

   In this step, the task starts the `BESBAC` service and immediately begins enforcing the security policy. Next, it creates a monitoring task named `BAC Monitoring Service` that runs every 5 minutes to check if the `BESClient` and `BESBAC` are running. If either of the services are stopped, the monitoring service restarts it ensuring that the solution is always active.

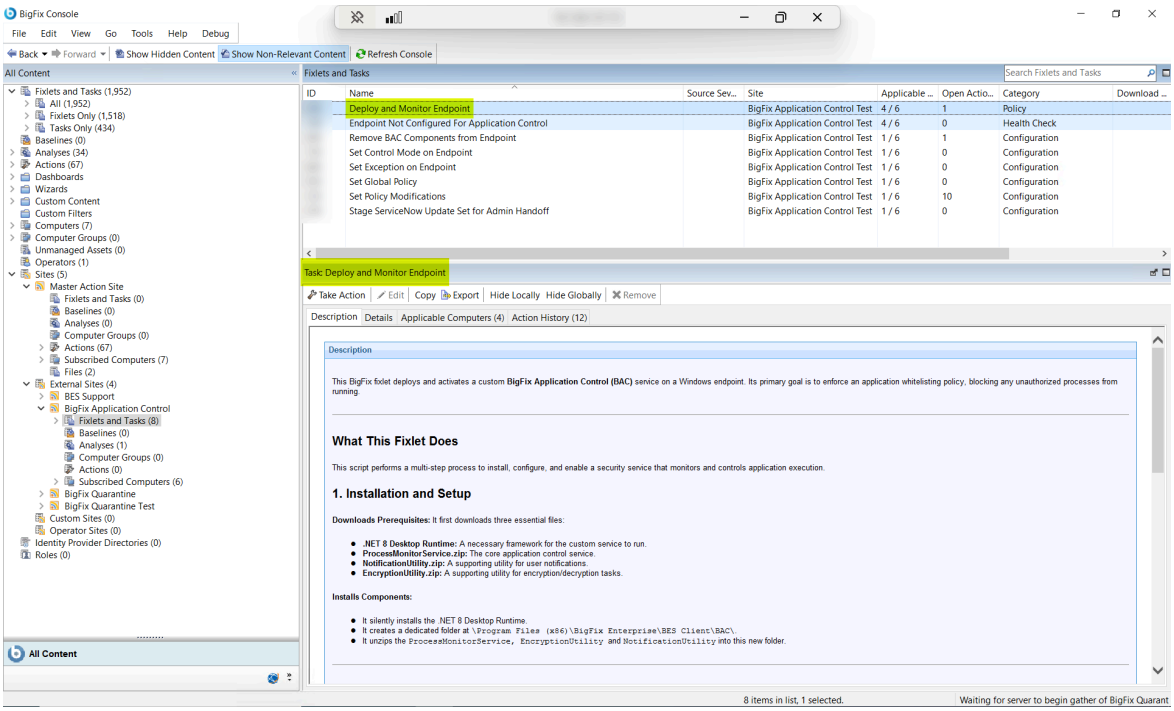
Follow the steps below to deploy the Application Control on the endpoints:

1. In the BigFix Console, navigate to **All Content > BigFix Application Control > Fixlets and Tasks**.

Figure 3. Navigate to Fixlets & Tasks



2. From the **Fixlets and Tasks** pane, select **Task: Deploy And Monitor Endpoint**.



This task does not contain any action script and the result set is based on client relevance to get the details of devices not managed by Application Control.

3. From the **Task: Deploy And Monitor Endpoint** pane, under **Configuration Options** enter the following information:

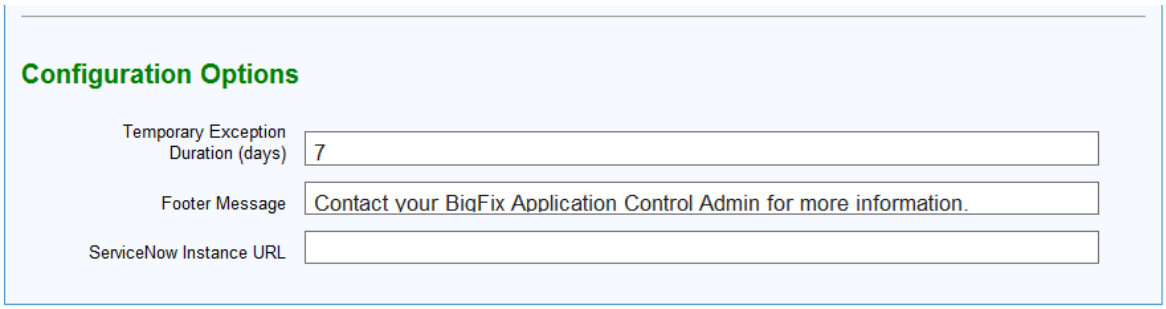


Table 1. Task: Deploy And Monitor Endpoint Configuration Options

Field Name	Description
Temporary Exception Duration (days)	Number of days for which the block listed applications are to be allowed for usage as per your organization's policies.
Footer Message	Message to be displayed to the endpoint users when they are raising exception requests.
ServiceNow Instance URL	Your organization's ServiceNow™ instance URL where the tickets are created for the exceptions raised by Application Control end-users.

4. From the **Task: Deploy And Monitor Endpoint** pane, click the **Applicable Computers(n)** tab and view the endpoints on which you want to run the task.
5. Select the **Take Actions** tab and select the endpoints on which you want to apply this installer task.
6. Click **OK**.

Chapter 3. Managing BigFix® Application Control

This section covers post-installation activities such as configuring and overseeing application settings to ensure optimal performance and security. This process is essential for maintaining system integrity and user access control.

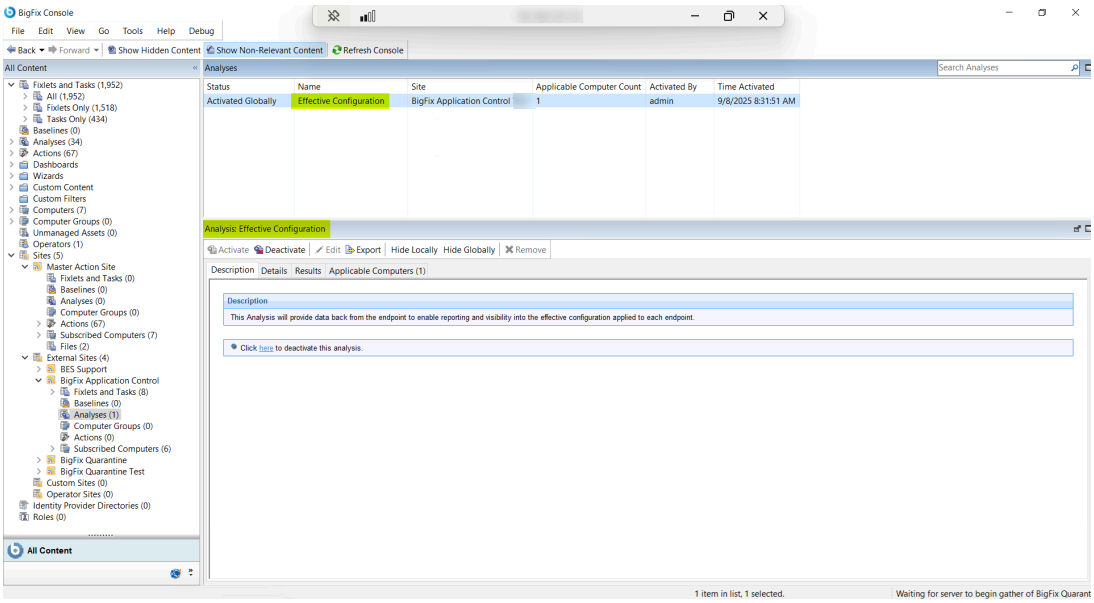
Analyses: Effective Configuration

This task describes how administrators can view the effective configuration applied to each endpoint from the BigFix console. It includes details on various data points available for all endpoints, such as Control Mode, Blocked Path Patterns Rules, and Exceptions.

Use **Analyses: Effective Configuration** to identify the configuration of the endpoints that are managed by the solution.

As an administrator, you can view the effective configuration applied to each endpoint from the BigFix console.

Figure 4. Analyses: View Effective Configuration



From the **Details** tab under **Analysis: Effective Configuration** pane, you can view the following data of all the managed endpoints:

- Control Mode
- Blocked Path Patterns Rules
- Blocked Hashes Rules
- Allowed Path Pattern Rules
- Allowed Hash Rules
- Exceptions
- BESBAC Service Status

View Endpoint Details using BigFix® Web Reports

As an administrator, you can utilize BigFix Web Reports to view a comprehensive, read-only overview of all enterprise endpoints with the application installed. This topic outlines the steps to access and navigate the various tabs that display managed devices, blocklisted applications, allowlisted applications, and exception access logs.

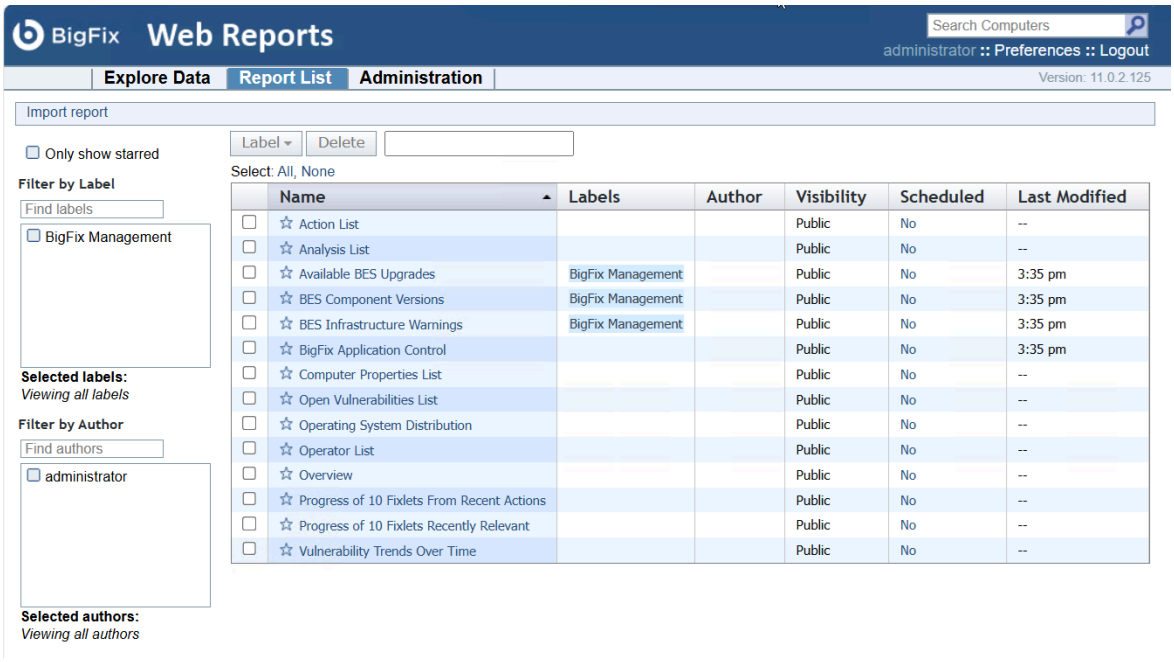
Learn how to use BigFix Web Reports to view a read-only overview of all the Application Control managed endpoints.

As an administrator, you can use the BigFix Web Reports to see a holistic, read-only view of all the endpoints of your enterprise which have BigFix Application Control installed on them.

Follow the steps below to view details from BigFix Web Reports:

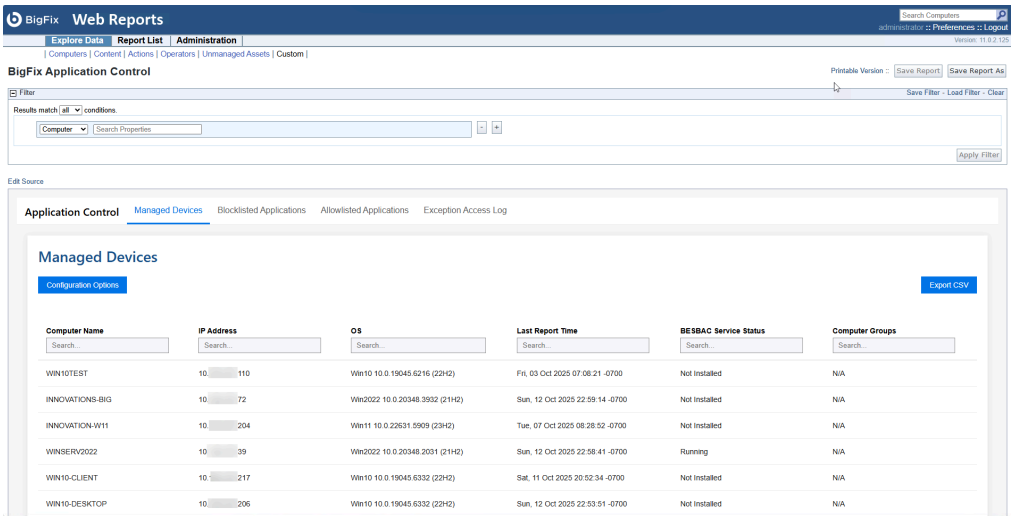
1. Login to **BigFix Web Reports**.

2. On the **Web Reports** home page, select the **Report List** tab and click **BigFix Application Control**.



3. On the BigFix Application Control pane, you will see the following 4 tabs:

Figure 5. Managed Devices screen



a. **Managed Devices**

All the managed endpoints will be listed in this tab in a tabular format. You can filter the managed devices lists using endpoint/BigFix properties. There are two features on this tab: **Configuration Options** & **Export CSV**.

- **Configuration Options**

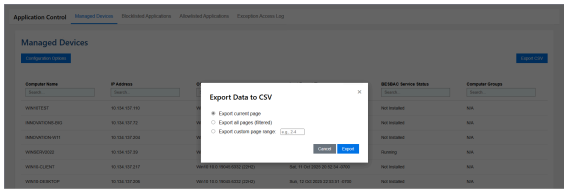
This feature lets you add properties or settings that you can use to filter the list of managed devices. We can broadly divide this feature into 3 parts:

- The first row has a Search field, an OS Filter & Group Filter to filter the list of managed devices.
- Next rows have the **Add Property** and the **Add Setting** fields. Start typing in the fields to get a list of properties or settings and click **Add Property** or **Add Setting** button as applicable.
- The last row has the **Rows per page** drop-down where you can set the number of managed devices that are displayed on a page.

- **Export CSV**

  This feature will export the list of managed devices in CSV format to your machine.

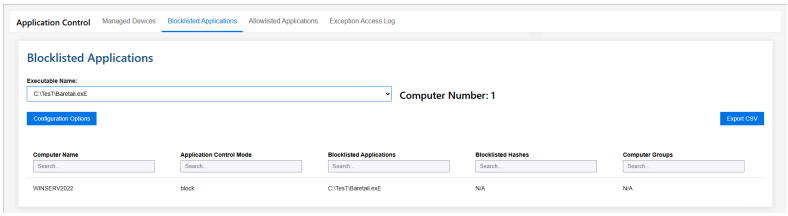
  Figure 6. Export CSV screen

b. **Blocklisted Applications**

This tab will display the list managed devices for a specific blocklisted application. Select an application name from the **Executable Name** field and it will display a count of endpoints on which it is blocklisted. It will also list those endpoints below in a tabular format.

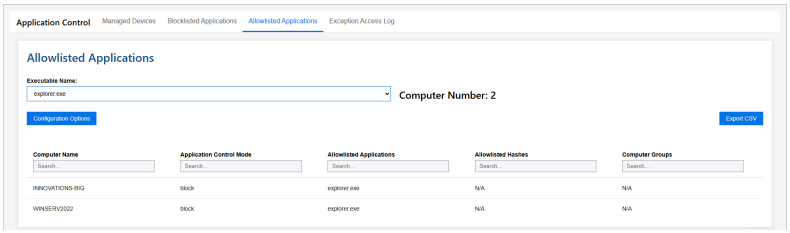
Figure 7. Blocklisted Applications screen



c. **Allowlisted Applications**

This tab will display the list managed devices for a specific allowlisted application. Select an application name from the **Executable Name** field and it will display a count of endpoints on which it is allowed. It will also list those endpoints below in a tabular format.

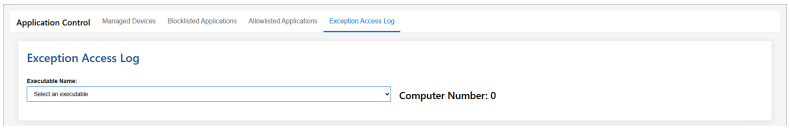
Figure 8. Allowlisted Applications screen



d. **Exception Access Log**

This tab will display the list of managed devices for a specific blocklisted application for which an exception was raised. When a desktop user raises an access request for a blocked application on his endpoint, an admin can see the details on this tab. For more details refer to Raising Request Access from *BigFix Application Control User's Guide*.

Figure 9. Exception Access Log screen



Set Control Mode on an Endpoint

This topic outlines the process for setting the operational mode on an endpoint in BigFix Application Control, allowing administrators to choose between Allow Mode and Block Mode. Each mode enforces different rules for application execution, enhancing security or flexibility based on the environment's needs.

Learn how to set the control mode on Application Control managed endpoints.

As an Administrator, you can set the operational mode for the Application Control policy on the endpoints. This setting determines the default execution and which set of rules (Allow or Block) are enforced on the endpoint.

There are two modes in BigFix Application Control:

- **Allow Mode**

  This mode has a default-deny policy. This means that all applications are blocked from running by default. Only applications and processes that match a specific "Allow Rule" are permitted to run. This is the most secure mode and is intended for highly controlled environments.

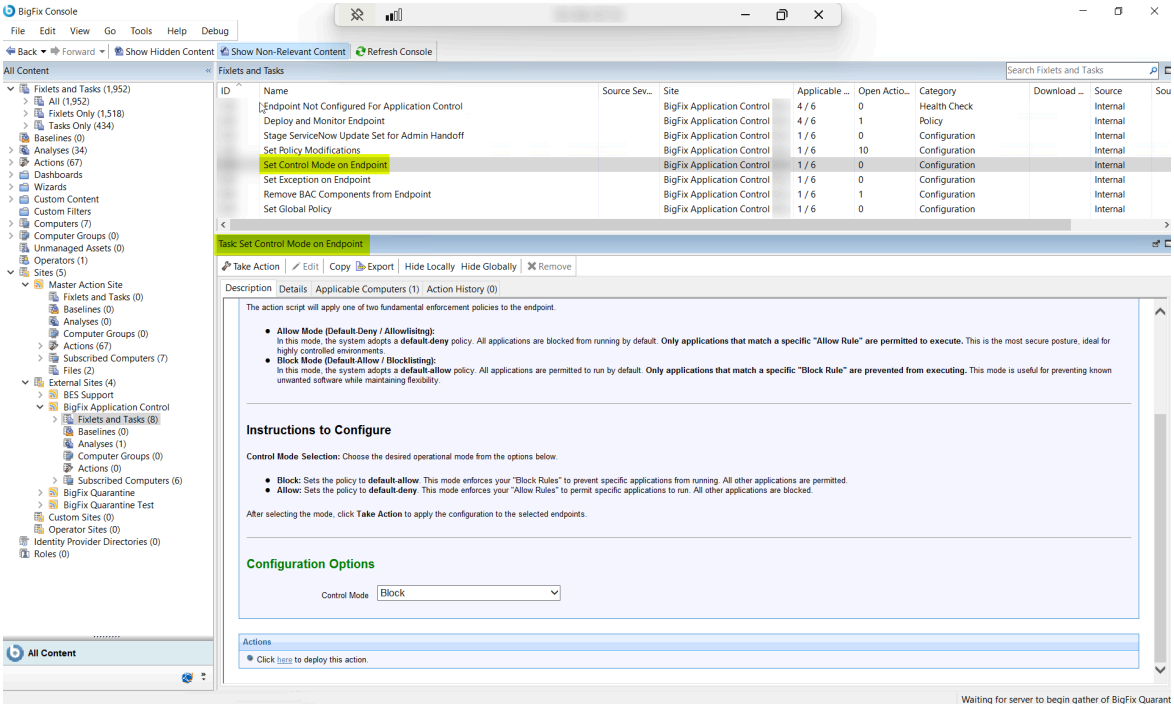
- **Block Mode**

  This mode has a default-allow policy. This means that all applications are permitted to run by default. Only applications and processes that match a specific “Block Rule” are prevented from running. This mode is intended for flexible environments.

You need to use **Task: Set Control Mode on Endpoint** for setting the desired control mode on an endpoint.

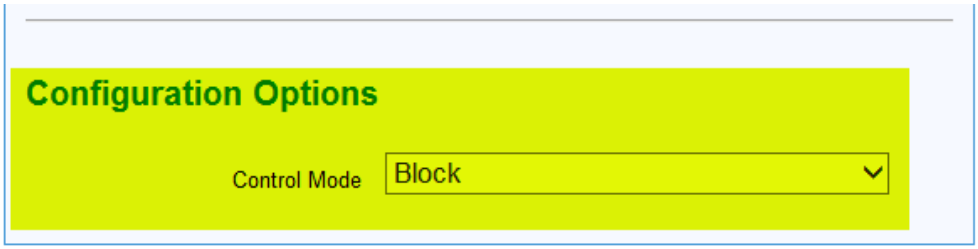
Follow the steps below to configure the mode on the endpoints:

1. From the **Fixlets and Tasks** pane, select **Task: Set Control Mode on Endpoint**.



2. From the **Task: Set Control Mode On Endpoint** pane, select the relevant Mode from the drop-down, either **Allow** or **Block**.

Figure 10. Task: Set Control Mode on Endpoint



3. Select the **Take Actions** tab and select the endpoints on which you want to apply the selected mode.
4. Click **OK**.

Set Policy Modifications

This topic provides instructions for setting policy modifications on endpoints, including creating new rules, removing existing ones, and applying rules from a CSV file. It is essential for managing application control rules to enforce security policies and prevent unauthorized software execution.

Learn how to set new rules, remove existing rules, and apply CSV ruleset using this task.

This task provides a comprehensive solution for managing application control rules on target endpoints. It is essential for enforcing security policies, preventing the execution of unauthorized software, and hardening endpoints against malwares. By modifying the local policy file (`...\BES Client\BAC\bes_bac.pol`), this task allows an administrator to create, update, or remove rules based on file patterns, file hashes, or a centrally managed CSV file. The action this task performs is determined by the **Select Mode** parameter chosen by the administrator.

This task has three **Select Mode** options available to an admin. They are as follows:

- **Mode 1: Set New Rule**

  This mode allows you to create and deploy a new, custom application control rule. The policy operates in a default block mode, meaning any new rule is added to a central configuration that determines which applications are permitted or denied. The configuration supports:
  - Allow Rules: Explicitly permit necessary applications to run.
  - Block Rules: Explicitly deny unauthorized or risky applications.

Table 2. Task: Set Policy Modifications Configuration Options

Field Name	Description
Rule Name	Name of the rule. Provide a clear, unique name for the policy (for example, "Block unauthorized torrent applications"). If a rule with the same name already exists, the task will fail.
Rule Type	Type of rule. Can be either Block or Allow.
Path Pattern	Path of the application or process to be allowed or blocked. Enter an executable name (for example, `msedge.exe`) or a full file path. Wildcards (*) are supported. For multiple entries, use a comma-separated list (for example, `C:\Temp*.exe,C:\Users*\downloads*.exe`).
File Hash	Hash value of the application file. For a more specific rule, provide the SHA-256 or SHA-384 hash of the file. For multiple hashes, use a comma-separated list.
Rationale	Description or reasoning of the rule.

Note: Provide a value for either Path Pattern or File Hash for the rule to be valid. For more effective control, it is recommended to use a combination of both wherever feasible.

- **Mode 2: Remove Existing Rule**

  This mode is used to modify or completely remove an existing application control rule. It offers granular control, allowing you to either delete an entire rule or selectively remove specific criteria (like file paths or hashes) from within a rule. When executed, the task performs one of the following operations:

- **Full Rule Deletion**: To delete an entire rule, provide the Rule Name and Rule Type, but leave both the Path Pattern and File Hash fields empty. The task will find the matching rule and remove it completely.
- **Partial Rule Modification**: To remove specific criteria from an existing rule, provide the Rule Name, Rule Type, and the Path Pattern or File Hash you wish to remove. The task will find the matching rule and remove only the specified path(s) or hash(es), leaving the rest of the rule intact.

After modifying the policy file, the task restarts the BES Application Control service ("BESBAC") to ensure the changes are applied immediately. If no rule matching the specified criteria is found, no changes will be made.

- **Mode 3: Apply CSV Ruleset**

  This mode creates or updates application control rules by dynamically reading from centrally managed CSV files. This allows for bulk management of application block/allow lists without altering the task action script itself. When executed, the task performs one the following actions:

  - Based on the Rule Type you select (Block or Allow), it reads from a corresponding source file: `allowlisted_applications.csv` or `blocklisted_applications.csv`.

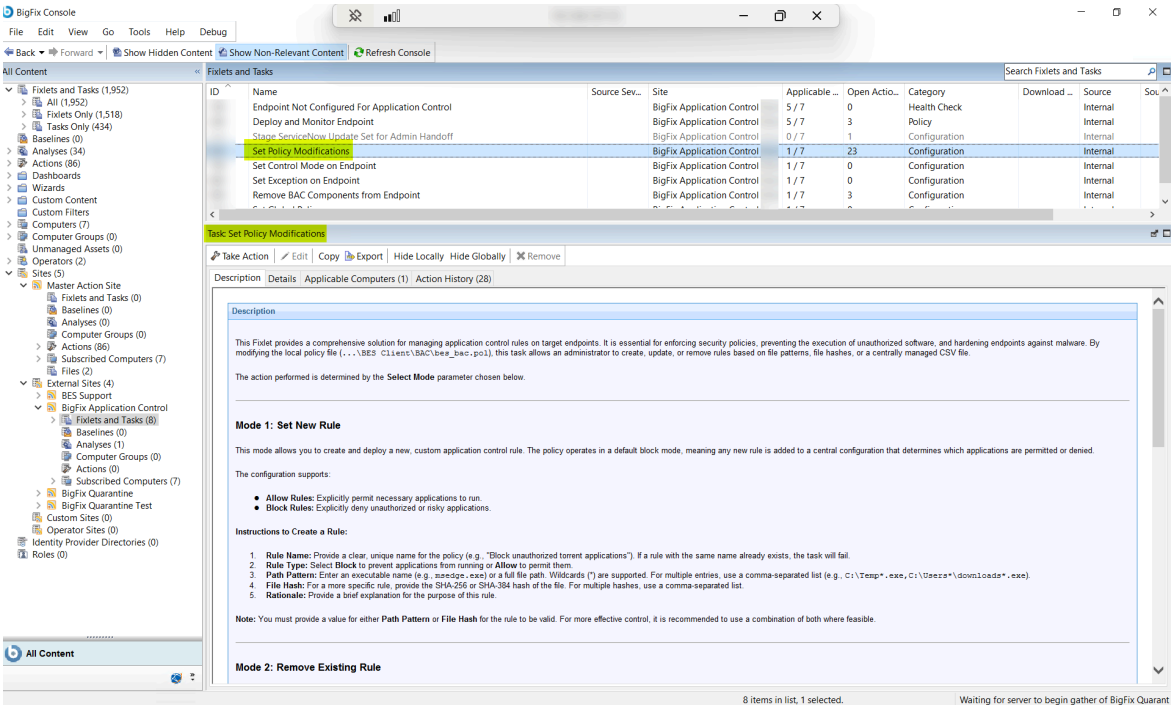
    Note: For reference, you can download the sample allowlisted and blocklisted CSV format files from the links below:
    - allowlisted_applications.csv
    - blocklisted_applications.csv

  - It parses the source file to extract a list of application file paths and/or file hashes.
  - It then finds the rule specified by the Rule Name in the local policy file. If the rule exists, it is updated with the information from the CSV; if it does not exist, it is added as a new entry.

  Remember: For this mode to function correctly, perform the following steps:
  1. First, create and upload the source CSV file(s) to the BigFix server.
  2. Next, create the CSV File(s). Create a file named blocklisted_applications.csv (for blocking) or allowlisted_applications.csv (for allowing). The files must contain the headers Path Patterns and Hashes.
  3. Finally, upload the file(s) to the Master Action Site. In BigFix Console, navigate to **Master Action Site > Files** tab. Right-click and select **Add Files**. Choose your CSV file and, most crucial, select the check-box labeled **Send to clients** before adding.

Perform the following steps to set policy modifications as needed:

1. From the **Fixlets and Tasks** pane, select **Task: Set Rule on Endpoint**.



2. From the **Task: Set Policy Modifications** pane, enter the following information on the **Description** tab:

Table 3. Task: Set Rule on Endpoint Configuration Options

Field Name	Description
Select Mode	Select the mode: Set New Rule, Remove Existing Rule, Apply CSV Ruleset as needed.

Based on the mode selected, you will get different configuration options.

Based on the mode selection, refer to the appropriate topic to complete this task.

- For setting a new rule, refer to Set New Rule on Endpoints *(on page 25)*.
- For removing an existing rule, refer to Remove Existing Rule from Endpoints *(on page 27)*.
- For applying a CSV ruleset, refer to Apply CSV Ruleset to an Endpoint *(on page 28)*.

Set New Rule on Endpoints

This topic describes the mode which enables administrators to create and deploy new rules on target endpoints. It allows for the definition of new application rules based on file patterns or specific file hashes, thereby enforcing security policies and preventing unauthorized process execution.

Learn how to set new rules on Application Control managed endpoints.

This mode in the **Set Policy Modifications** task allows an administrator to create and deploy Application Control rules on target endpoints. One can define allow or block application rules based on file patterns or specific file hash. This mode helps in enforcing security policies, prevents execution of unauthorized processes, and hardens endpoints against malware.

Note: All rule or policy related data is encrypted in BigFix Application Control. Application Control uses JSON files to communicating between BigFix® console and its endpoints. All data in the JSON files are encrypted and cannot be circumvented.

You need to use the mode **Set New Rule** for setting new rules on endpoints.

Perform the following steps to set new rules on endpoints as needed:

1. From the **Task: Set Policy Modifications** pane, enter the following information on the **Description** tab:

Figure 11. Set New Rules

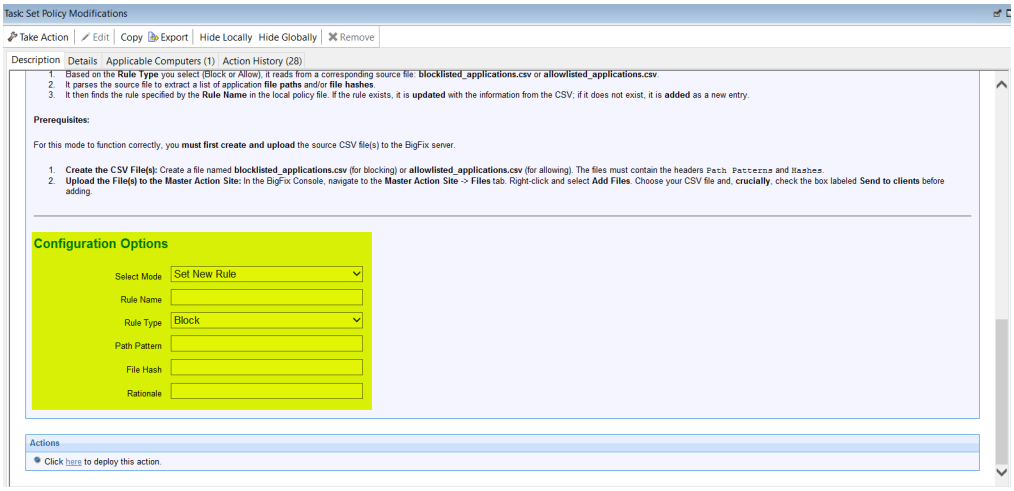


Table 4. Task: Set Policy Modifications: Set New Rules Mode Configuration Options

Field Name	Description
Select Mode	Select the mode: Set New Rule.
Rule Name	Name of the rule.
Rule Type	Type of the rule. Can be either Block or Allow.
Path Pattern	Path of the application or process to be allowed or blocked.
File Hash	Hash value of the application file.
Rationale	Description or reasoning of the rule.

2. Select the **Take Actions** tab and select the endpoints on which you want to apply the new rules.
3. Click **OK**.

Remove Existing Rule from Endpoints

This topic describes the mode which allows administrators to remove or modify Application Control rules from an endpoint's policy file using the Task: Set Policy Modifications. Users can either delete a rule entirely or adjust specific file paths or hashes, ensuring immediate application of changes by restarting the BESBAC service.

Learn how to remove existing rules on Application Control managed endpoints.

As an administrator, you can use this mode to modify or delete an existing application control rule from an endpoint's policy file. You can either completely delete a rule or remove specific file paths or hashes from a rule.

For a full rule deletion, update only the **Rule Name** and **Rule Type** fields but leave the other fields empty. For a partial rule modification, update all the fields. After the JSON policy file is modified, BESBAC service restarts to ensure that the changes are applied immediately.

You need to use the mode **Remove Existing Rule** for deleting or modifying rules on endpoints.

Perform the following steps to remove and/or modify the existing rules from endpoints as needed:

1. From the **Task: Set Policy Modifications** pane, enter the following information on the **Description** tab:

Figure 12. Remove Existing Rule

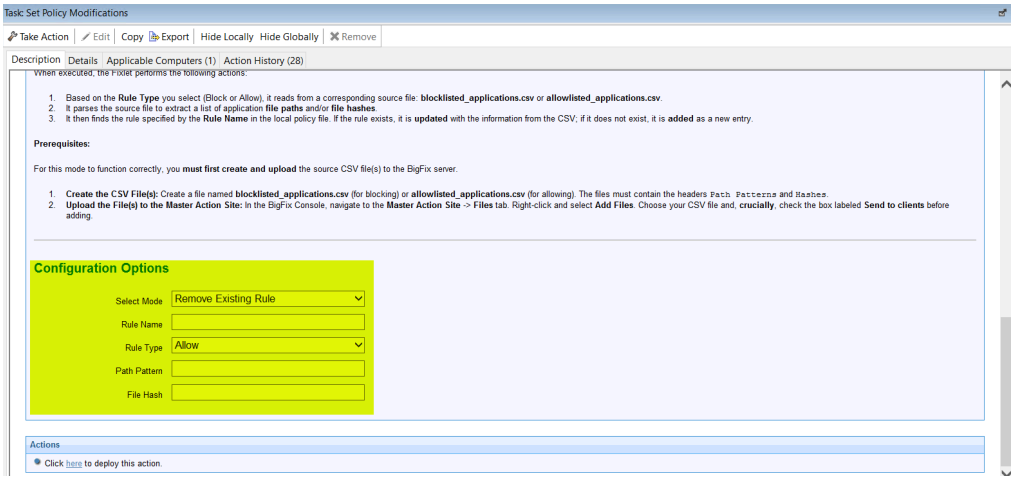


Table 5. Task: Set Policy Modifications Remove Existing Rule Mode Configuration Options

Field Name	Description
Select Mode	Select the mode: Remove Existing Rule.
Rule Name	Name of the rule.
Rule Type	Type of rule. Can be either Block or Allow.
Path Pattern	Path of the application or process to be allowed or blocked.
File Hash	Hash value of the application file.

Note: For full rule deletion, update only the **Rule Name** and **Rule Type** fields. But for a partial rule modification, you will need to update all the fields.

2. Select the **Take Actions** tab and select the endpoints from which you want to remove the rules.
3. Click **OK**.

Apply CSV Ruleset to an Endpoint

This topic describes the mode which outlines how to apply a CSV ruleset to an endpoint using the BigFix console. It enables administrators to dynamically manage application block and allow lists by reading from centrally managed CSV files, ensuring that the local JSON policy file on the endpoint is updated accordingly.

For the mode: Apply CSV Ruleset to Endpoint to work correctly:

1. **Create CSV files**

   First, create the `blocklisted_applications.csv` and `allowlisted_applications.csv` files. Both files must contain **Path Patterns** and **Hashes** column headers.

2. **Upload CSV files to Master Action Site**

   a. In BigFix console, navigate to **Master Action Site**.
   b. Browse to the **Files** tab.
   c. Right-click and select **Add Files**.
   d. Choose the CSV files you created.
   e. Select the **Send to Clients** check-box.
   f. Click **Add Files**.

This task performs the following actions:

- Based on the selected rule type (**Block** or **Allow**), it reads the corresponding source file: `blocklisted_applications.csv` or `allowlisted_applications.csv`.
- From the source file the list of application file paths and/or file hashes are extracted.
- The task then searches for the rule specified by the **Rule Name** in the `effective_policy.json` file.
  - If the rule exists, the JSON file is updated with the latest information.
  - If the rule does not exist, it's added as a new entry.

This way bulk dynamic management of application block/allow list is achieved without altering the task action script.

Learn how to apply CSV rulesets on Application Control managed endpoints.

As an administrator, you can create or update Application Control rules on endpoints by dynamically reading from centrally managed CSV files. BigFix Application Control updates the local JSON policy file on the endpoint with application paths and hashes, allowing administrators to either allow or block specific applications as needed.

You need to use the mode **Apply CSV Ruleset** for dynamically creating or modifying rules on endpoints.

Perform the following steps to apply CSV rulesets to an endpoint:

1. From the **Task: Set Policy Modifications** pane, enter the following information on the **Description** tab:

Figure 13. Apply CSV Ruleset

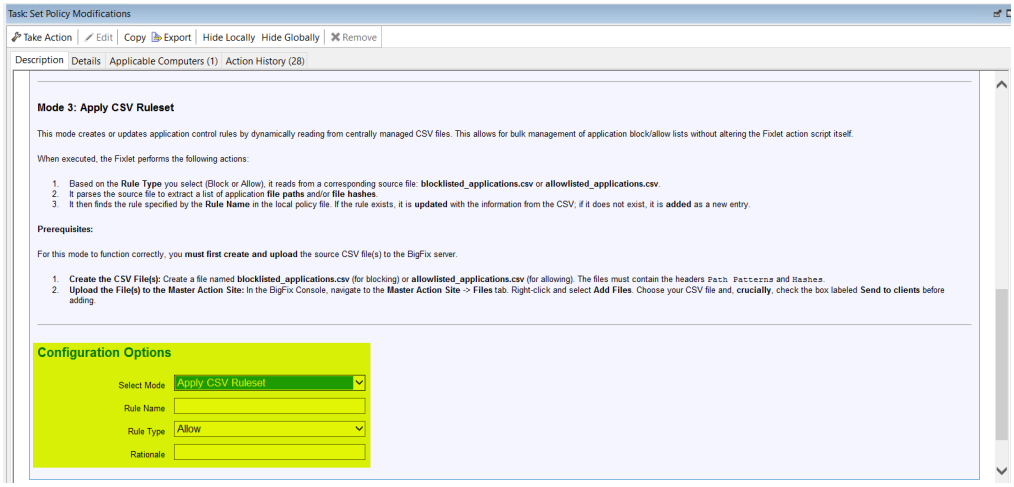


Table 6. Task: Set Policy Modifications Apply CSV Ruleset Mode Configuration Options

Field Name	Description
Select Mode	Select the mode: Apply CSV Ruleset.
Rule Name	Name of the rule.
Rule Type	Type of the rule. Can be either Block or Allow.
Rationale	Description or reasoning of the rule.

2. From the **Take Actions** tab and select the endpoints on which you want to apply the CSV rulesets.
3. Click **OK**.

Set Exception on an Endpoint

This topic outlines what all administrators can view the exceptions on an endpoint using the Task: Set Exception on Endpoint. It details the additional parameters required, including File_Name, Approved_By, Expiration_Date, and Reason, and explains the task's role in facilitating ServiceNow™ work flow for exception approval tickets.

Learn how to view all the exceptions applied on Application Control managed endpoints.

Note: This task cannot be triggered from BigFix® console. This task is intended to be triggered by ITSM applications (like ServiceNow™) for leveraging application exceptions on an endpoint.

As an administrator, you can view the **Task: Set Exception on Endpoint** to know about the exceptions set on managed endpoints. Exceptions are allow-rules with some additional data parameters. These additional parameters are **File_Name**, **Approved_By**, **Expiration_Date**, and **Reason**. This is a placeholder task to allow the execution of ServiceNow™ work flow for tickets (raised by desktop users for exception approval).

Stage ServiceNow™ Update Set for Admin Handoff

This topic outlines the process for staging a ServiceNow Update Set file on the BigFix® Root Server, facilitating the handoff between BigFix® and ServiceNow™ administration teams. It includes steps for notifying the ServiceNow™ administrator and importing the file to the ServiceNow™ instance after staging.

This task prepares a ServiceNow™ Update Set file for deployment by placing it at a designated location on the BigFix Root Server. Its purpose is to facilitate the work flow between BigFix® and ServiceNow™ administration teams.

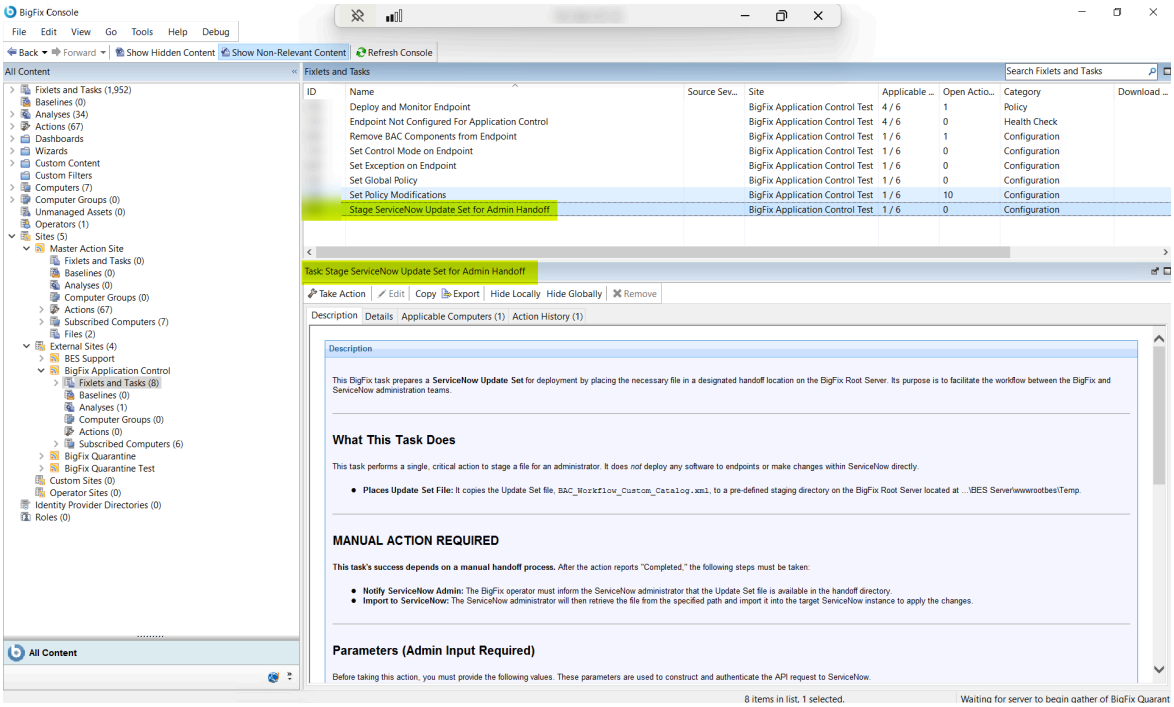
Note: This task performs a single, critical action to stage a file for BigFix® and ServiceNow™ administrator. It does not deploy any software to endpoints or make changes within ServiceNow™ directly.

The Update Set file, **ServiceNowUpdateSet.xml**, is copied to a predefined directory on the BigFix™ Root Server located at `...\BES Server\wwwrootbes\Temp`. This task depends on a manual handoff process. After the task action is complete, following steps are needed:

1. Notify ServiceNow™ Admin: The BigFix® operator must inform the ServiceNow™ administrator that the Update Set file is now available in the staging directory.
2. Import to ServiceNow™: The ServiceNow™ administrator needs to then retrieve the file from the specified path and import it to the target ServiceNow™ instance to apply the changes.

Perform the following steps to stage the Update Set files at the handoff directory in BigFix™ Root Server:

1. From the **Fixlets and Tasks** pane, select **Task: Stage ServiceNow Update Set for Admin Handoff**.

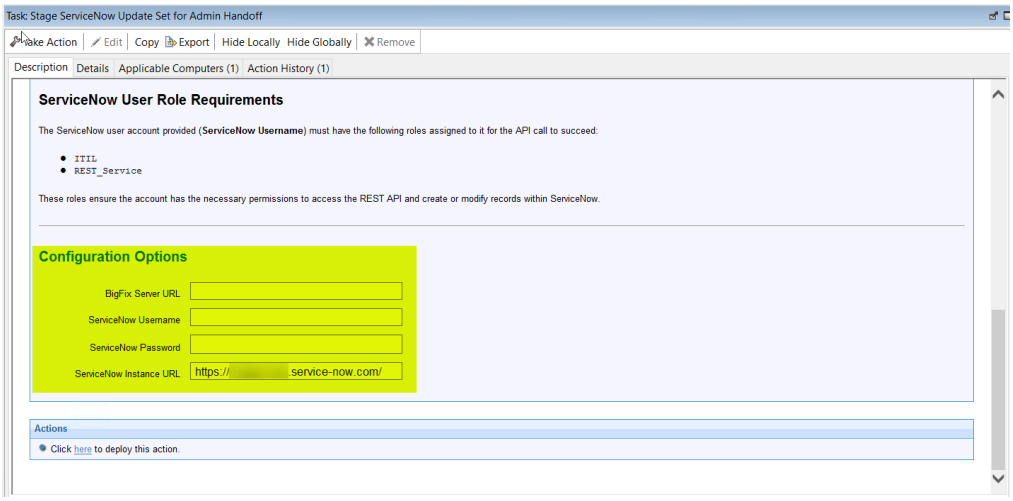


2. From the **Task: Stage ServiceNow Update Set for Admin Handoff** pane, enter the following information on the **Description** tab:

Table 7. Task: Stage ServiceNow Update Set for Admin Handoff Configuration Options

Field Name	Description
BigFix Server URL	The base URL for your organization's ServiceNow™ instance. For example, `https://your-instance.service-now.com`.
ServiceNow Username	The ServiceNow™ user name for the ServiceNow™ account that will be used for integration.
ServiceNow Password	The password for the ServiceNow™ user. This is a secure parameter and will not be displayed in plain text.
ServiceNow Instance URL	The BigFix Root Server instance URL which can be passed to the ServiceNow™ for reference.

Figure 14. Task: Stage ServiceNow Update Set for Admin Handoff



Note: The ServiceNow™ user account provided above must have the **ITIL** and **REST_Service** roles assigned to it for API calls to succeed. These roles ensure that the account has necessary permissions to access the REST API and create or modify records within ServiceNow™.

3. From the **Take Actions** tab, select the endpoints on which you want to apply the CSV rulesets.
4. Click **OK**.

By performing the step above, BigFix Application Control stage the Update Set file at the appropriate location in the BigFix Root Server.

Configuring Update Sets, Catalog Files, & System Properties in ServiceNow™

This task provides step-by-step instructions for configuring update sets, catalog files, and system properties in ServiceNow™. Administrators will learn how to set up the Update Sets property, import update sets from XML, and configure REST message properties to ensure effective communication with managed endpoints.

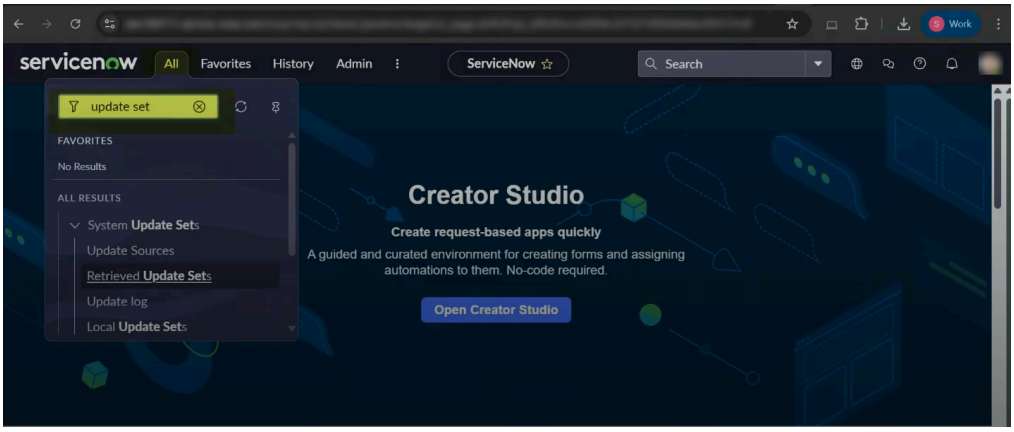
Perform the steps mentioned in the Stage ServiceNow Update Set for Admin Handoff *(on page 30)* task before attempting this task.

Learn how to configure update sets, catalog files, and system properties in ServiceNow™.

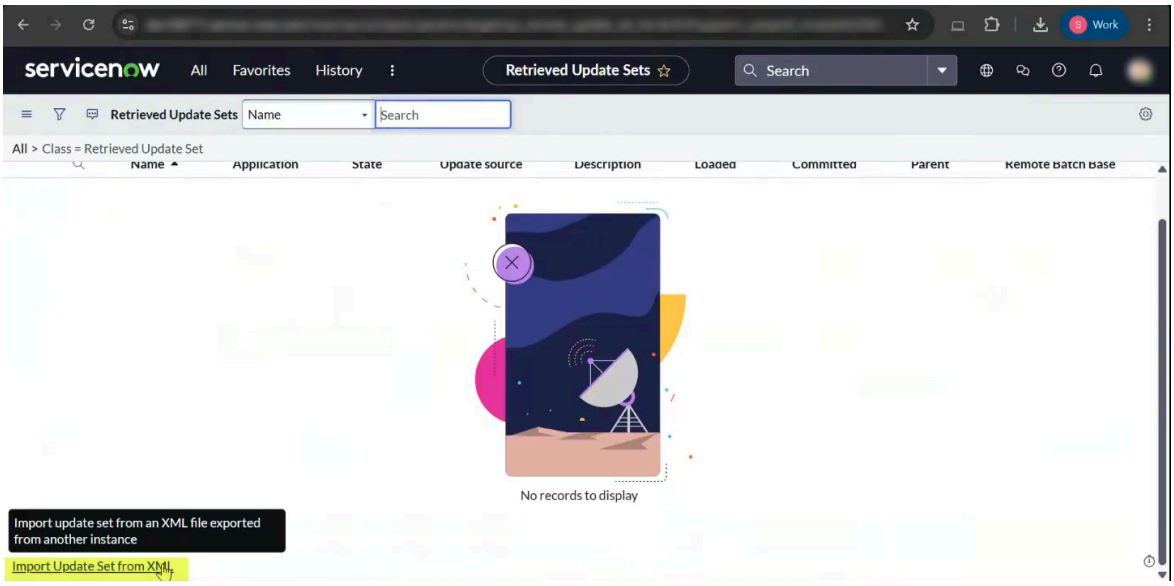
As an administrator, you will need to configure the **Update Sets**, catalog files, and system properties on the customer's instance of ServiceNow™ portal. This configuration is necessary so that the exceptions raised on Application Control managed endpoints are created in customer's instance of ServiceNow™.

1. Browse to the customer's ServiceNow™ instance portal where the exception requests raised by the end-users will reflect.
2. From **All** tab, search for `Update Sets` properties.

Figure 15. Search Update Set Properties in ServiceNow



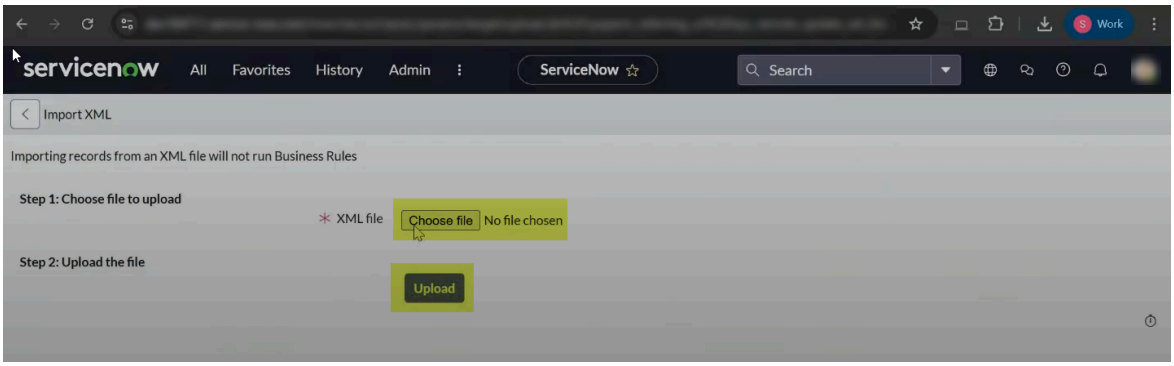
3. Click **Retrieved Update Sets**. This property updates the **Update Sets** property that are pulled form another ServiceNow™ instance.
4. From **Retrieved Update Sets** screen, click the **Import Update Set from XML** link at the bottom-left of the screen.



The link **Import Update Set from XML** imports an update set from an XML file exported from another ServiceNow™ instance, in this case it will be the customers instance.

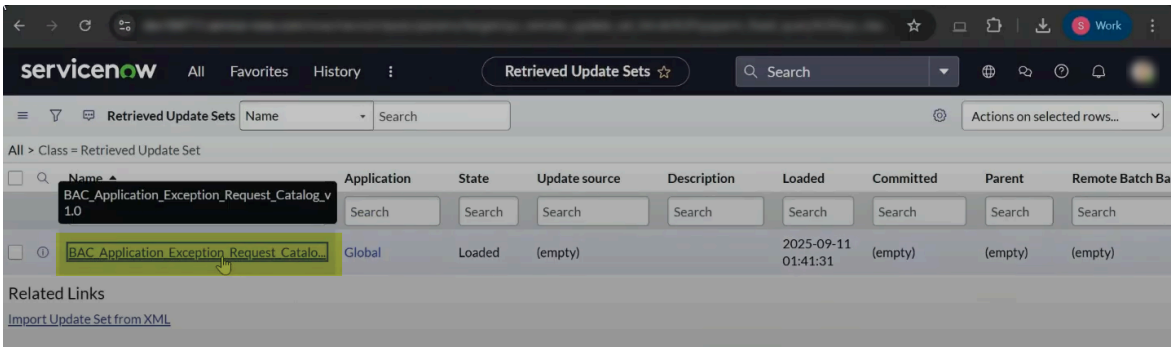
Note: Perform the steps mentioned in the Stage ServiceNow Update Set for Admin Handoff *(on page 30)* task to get the Update Set file that you need to import.

5. From the **Import XML** screen, click **Choose file** to select the XML file from the customer's instance that you need to import. After the file is selected, click **Upload**.

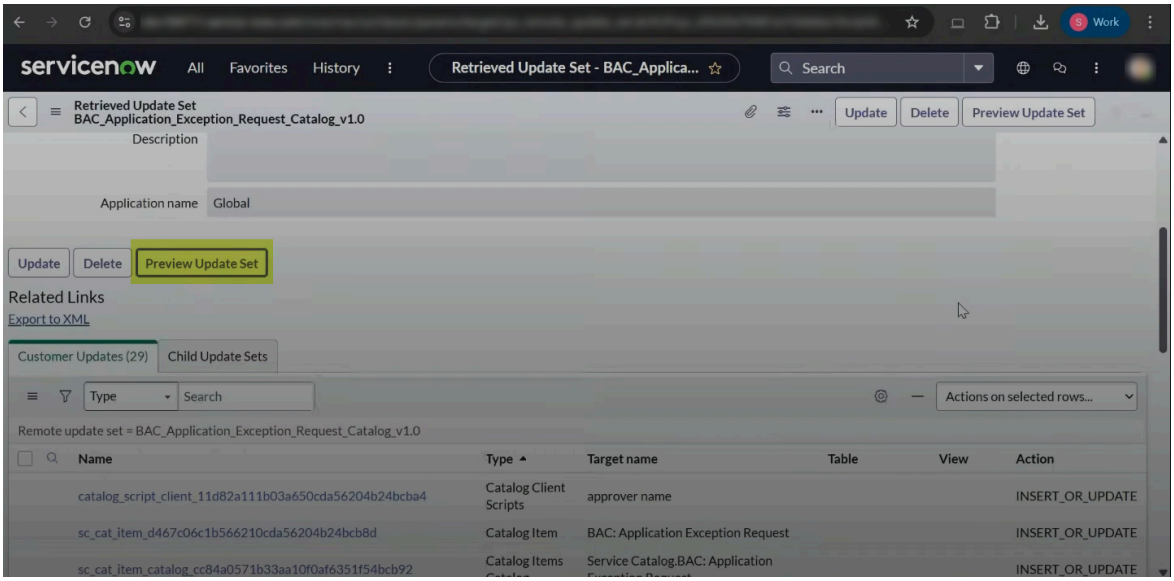


Once successfully uploaded, you will see the uploaded file on the **Retrieved Update Set** screen.

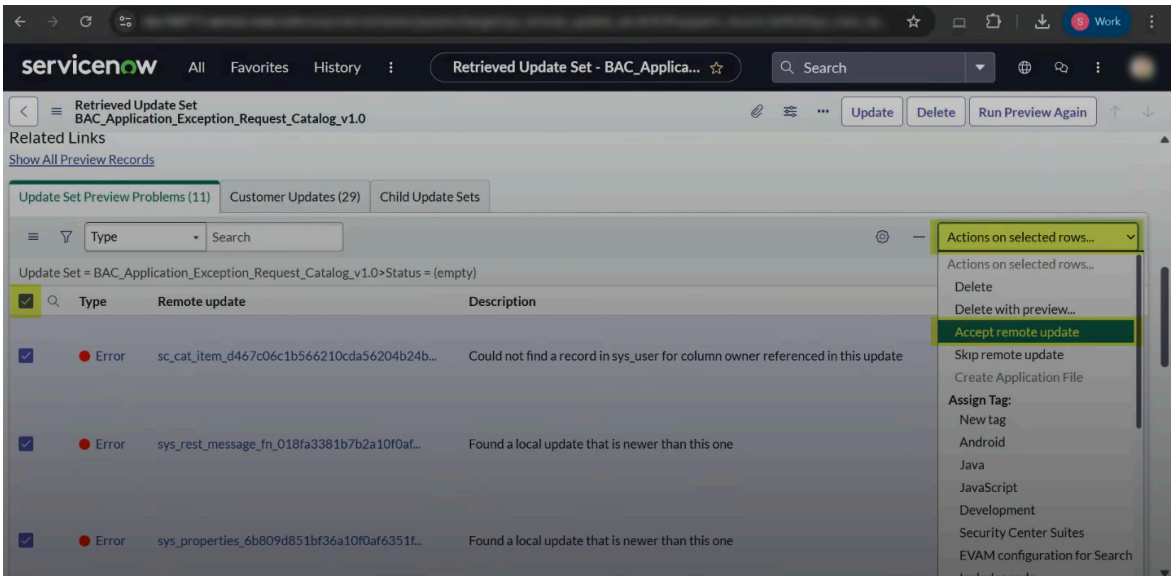
6. On the **Retrieved Update Set** screen, click to open the newly uploaded update set.



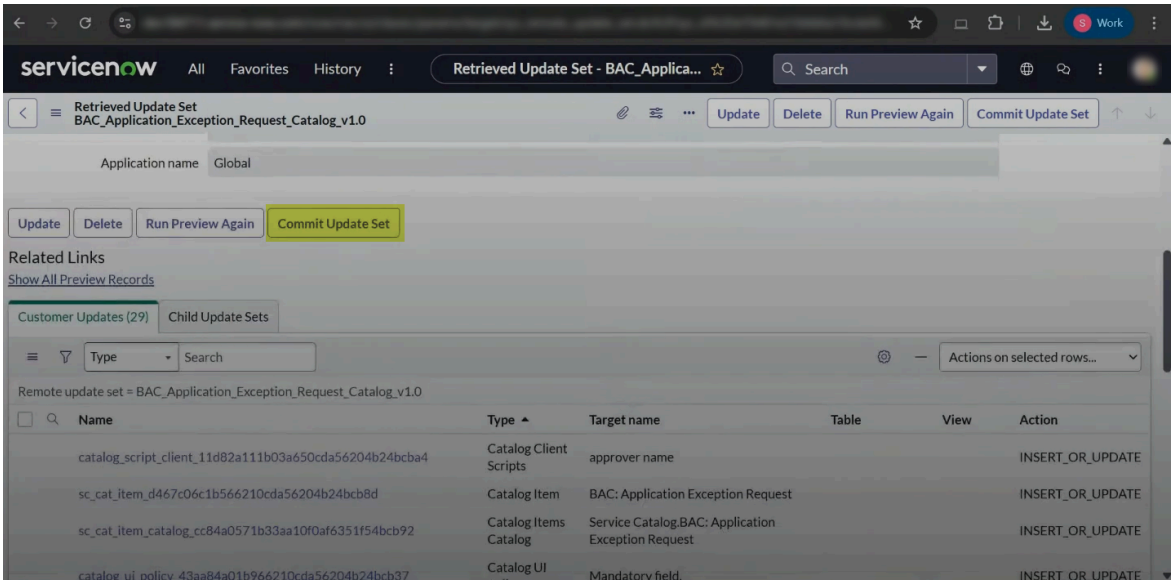
7. On the **Retrieved Update Set <file-name>** screen, click the **Preview Update Set** button. Click **Close** once the preview processing is complete.



8. Browse to **Select All > Actions on selected rows... > Accept remote update**.

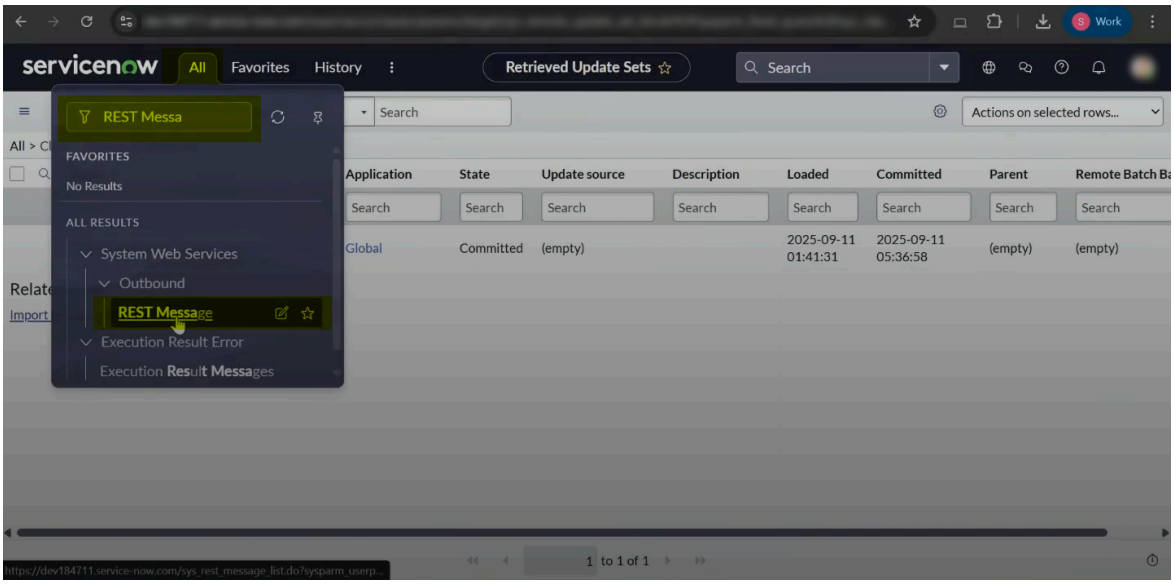


9. Once the **Accept remote update** action is complete, click the **Commit Update Set** button.

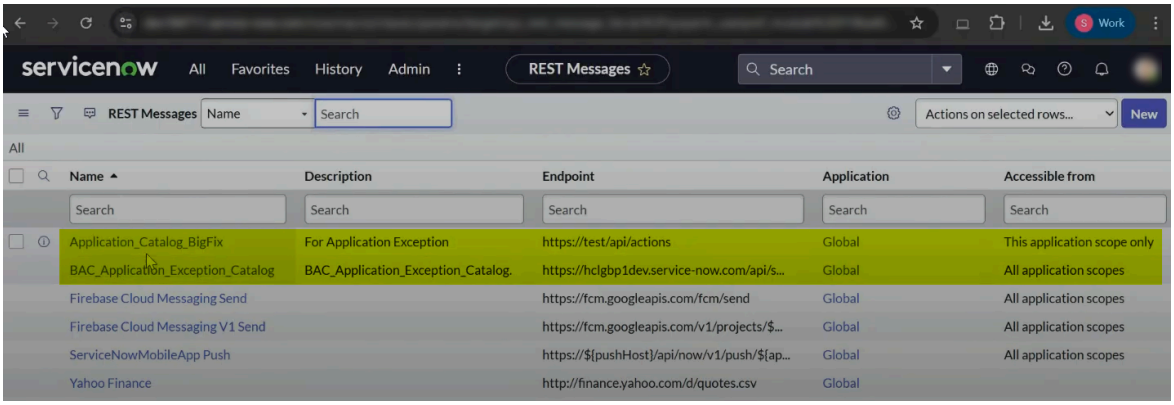


Click **Close** once the **Commit Update Set** action is complete.

10. Next, configure the **REST Message** property. To do so, browse back to the **All** tab and search for **REST Message** property.



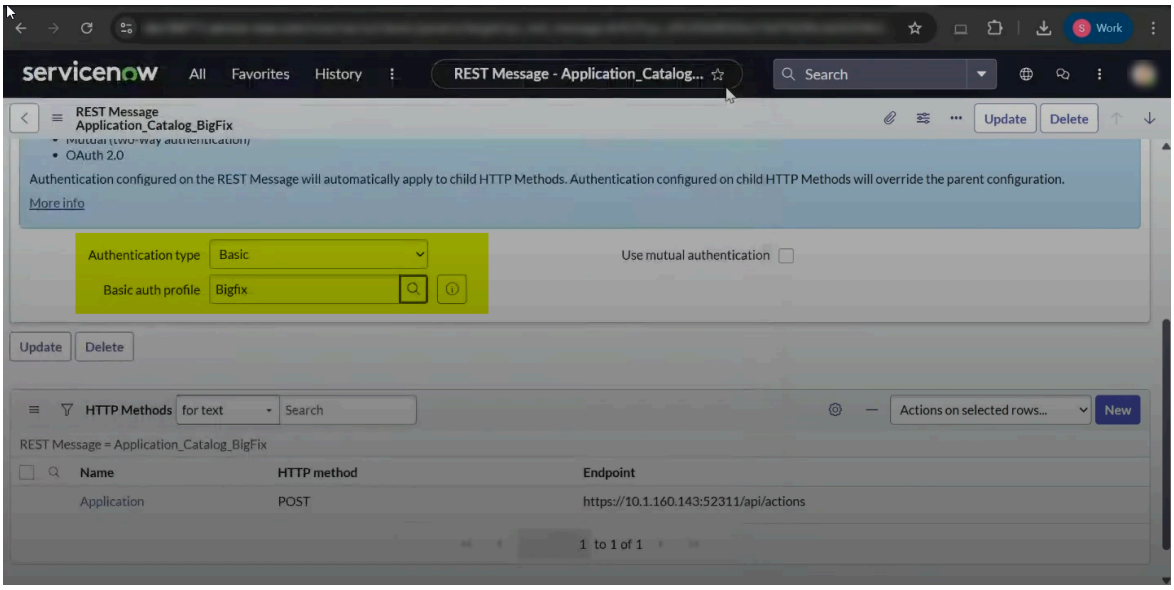
11. On the **REST Message** screen, there will be two Application Control catalog files.



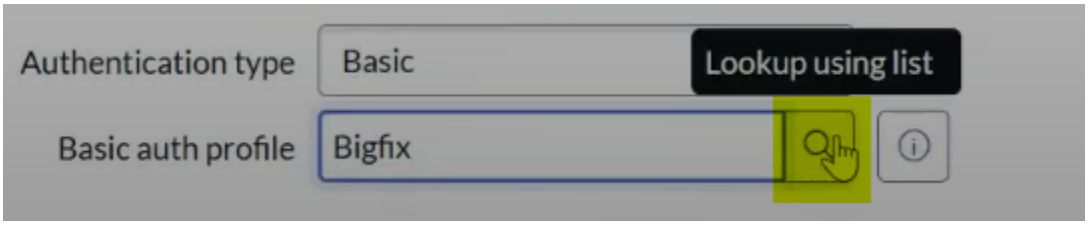
These files will be used for communicating with BigFix Application Control REST APIs by ServiceNow™.

12. **Note:** Before executing this step, ensure that you have BigFix REST API credentials available with you.

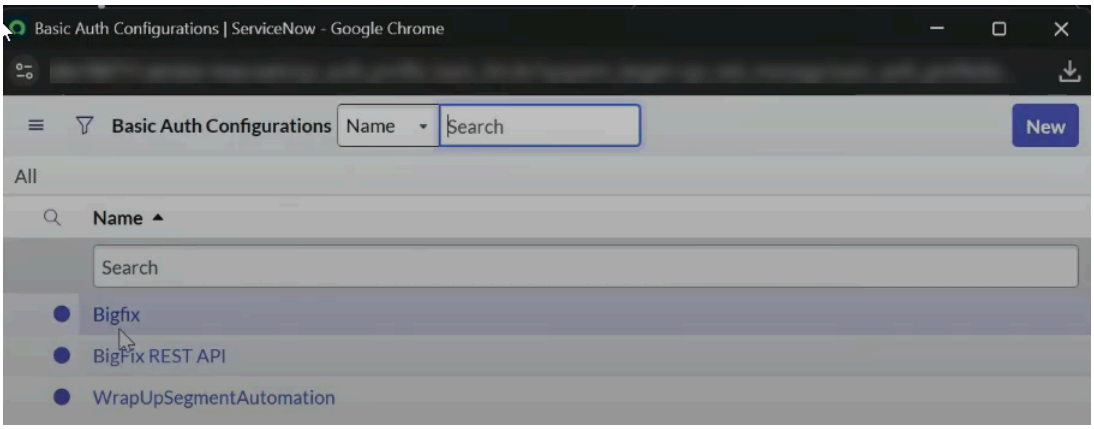
Click the **Application_Catalog_BigFix** file, and select the **Authentication type** as **Basic**. In the **Basic auth profile** field, enter BigFix REST API credentials. These fields set the authentication type for communicating with BigFix REST APIs.



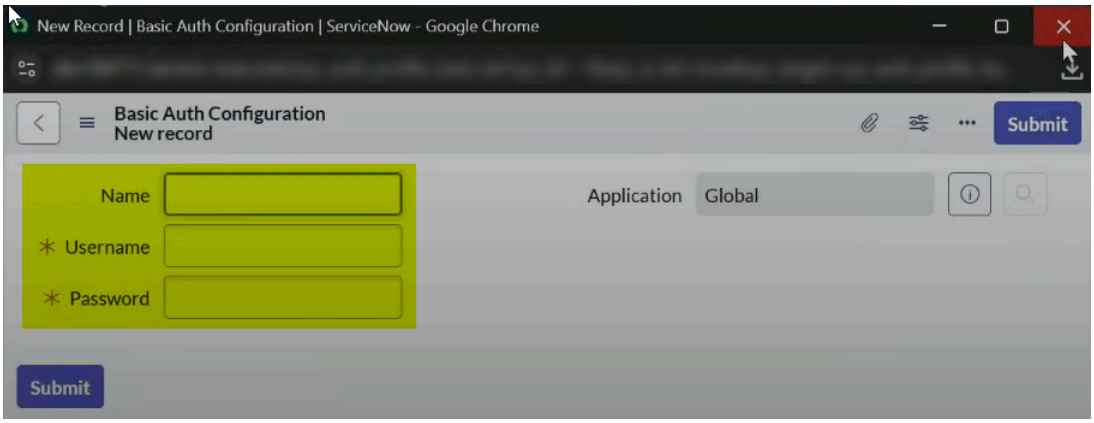
a. You can search for the BigFix REST API credentials by clicking the **Lookup using list** option.



b. On the **Basic Auth Configuration | ServiceNow** screen, either search and select the credentials from the list or click **New** to create new record in ServiceNow™.

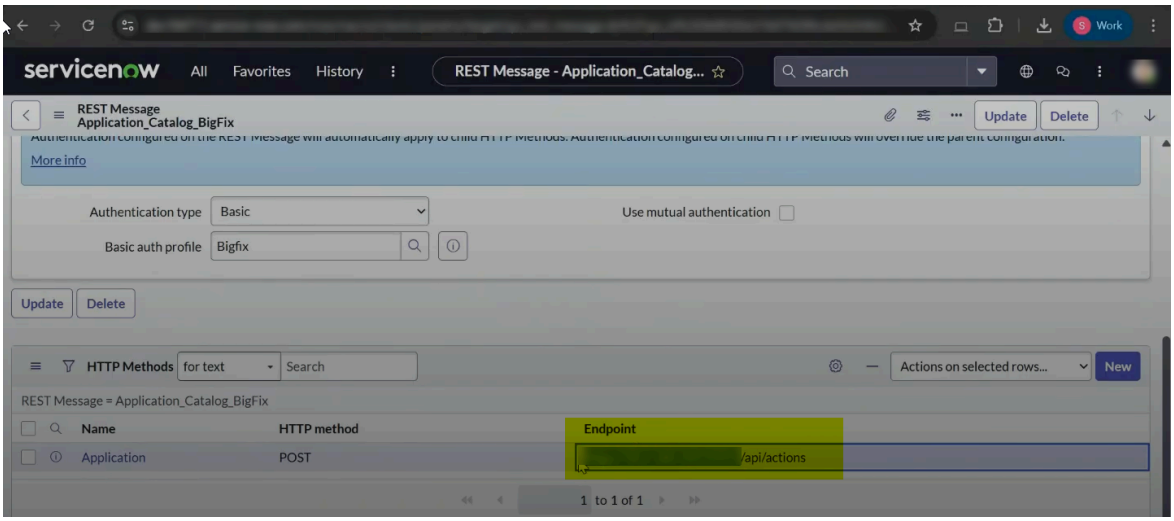


c. On the **New Record | Basic Auth Configuration | ServiceNow** screen, enter the **Name**, **Username**, and **Password** of the record.



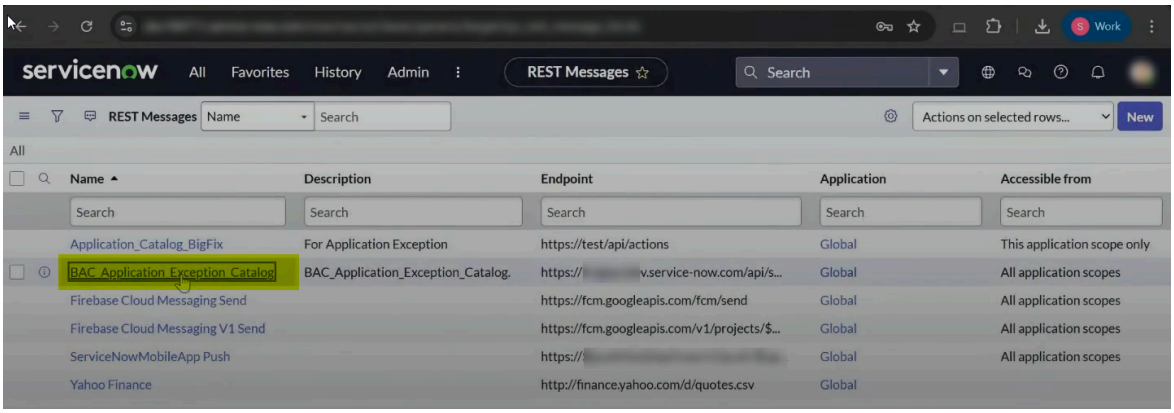
Click **Submit**.

13. Now, update the endpoints for the REST POST and PUT methods.

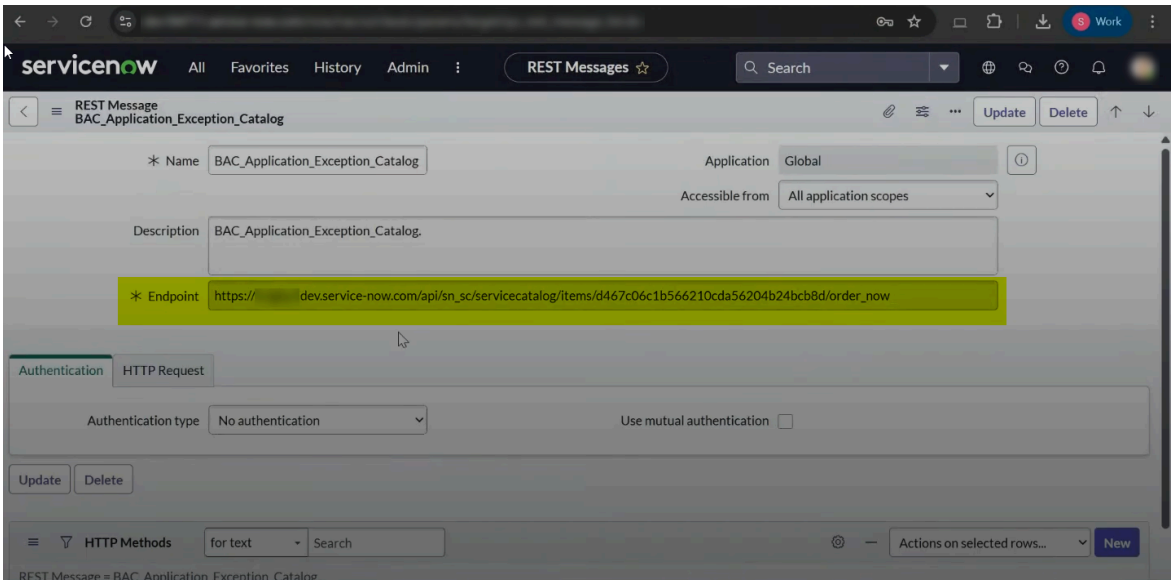


This endpoint is the BigFix REST API server with which ServiceNow™ will communicate.

14. Next, browse to the **REST Message** screen and select the **BAC_Application_Exception_Catalog file** file.

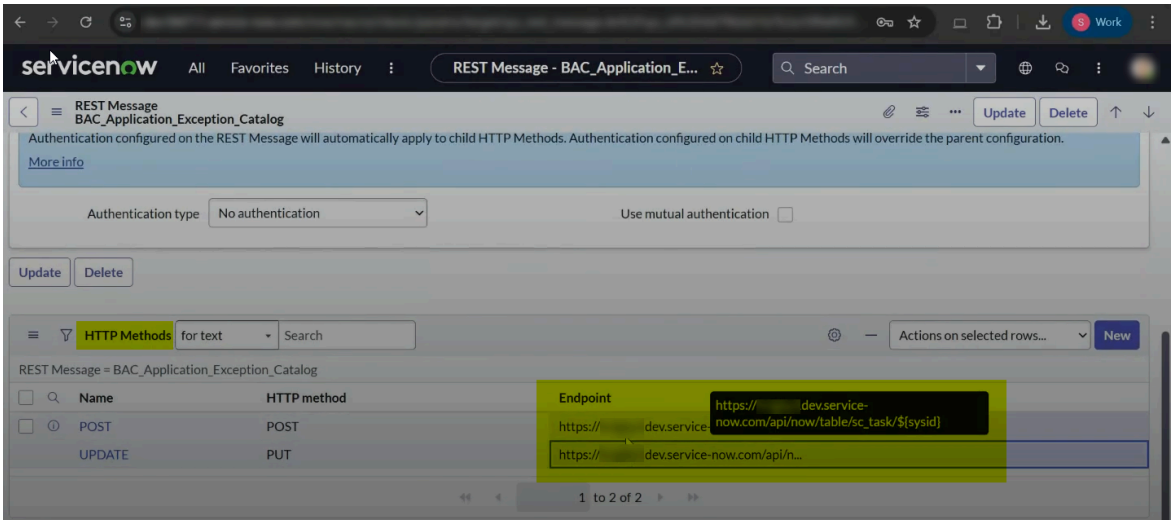


15. On the **REST Message BAC_Application_Exception_Catalog** screen, update the **Endpoint** field with the URL of the customers ServiceNow™ instance.

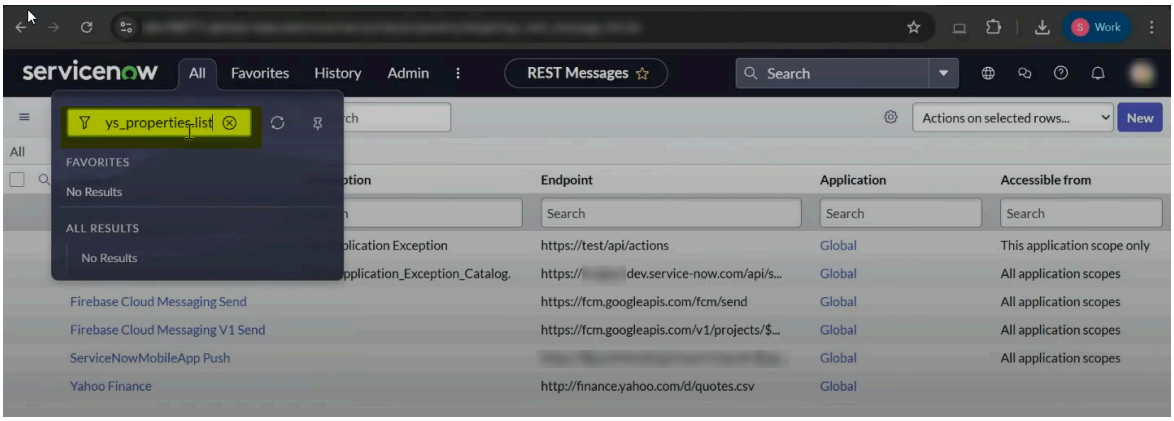


This endpoint URL is ServiceNow™ instance where you wish to generate the exception requests raised by the desktop users of Application Control.

16. Scroll down on the same screen and update the **Endpoint** column for the post and put methods in the **HTTP Methods** section.

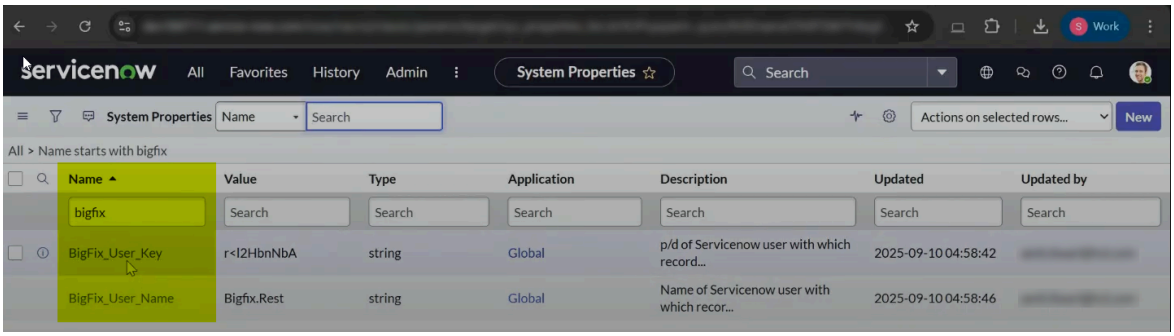


17. Next, configure the **sys_properties.list** property. To do so, browse back to the **All** tab and search for `sys_properties.list` property.



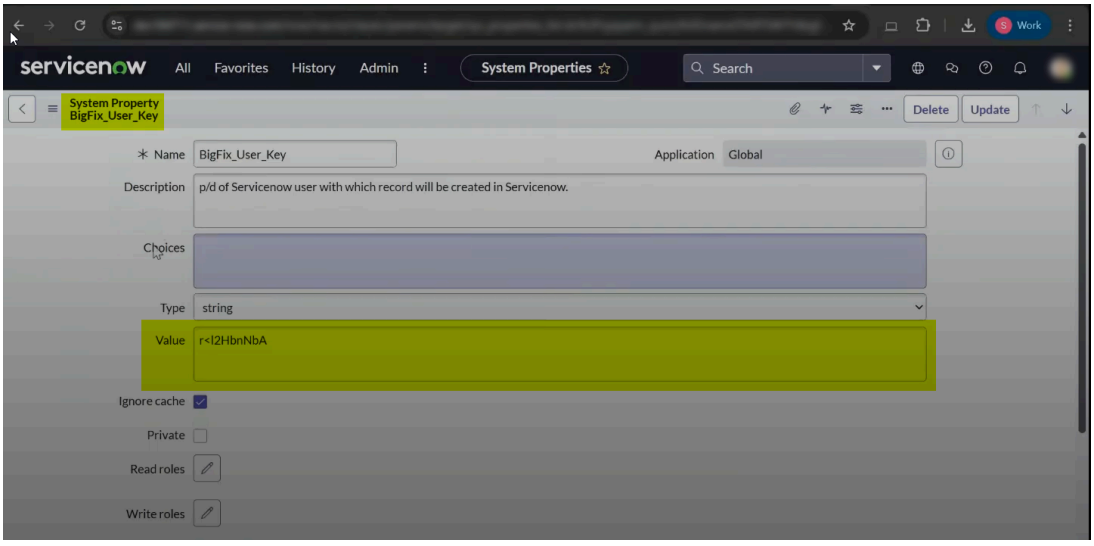
18. **Note:** The ServiceNow™ user (with exception manager role or persona), must have **ITIL** and **REST Service** roles assigned to it before you proceed to update the properties in this step.

On the **System Properties** screen, search using the `BigFix` keyword in the **Name** column.

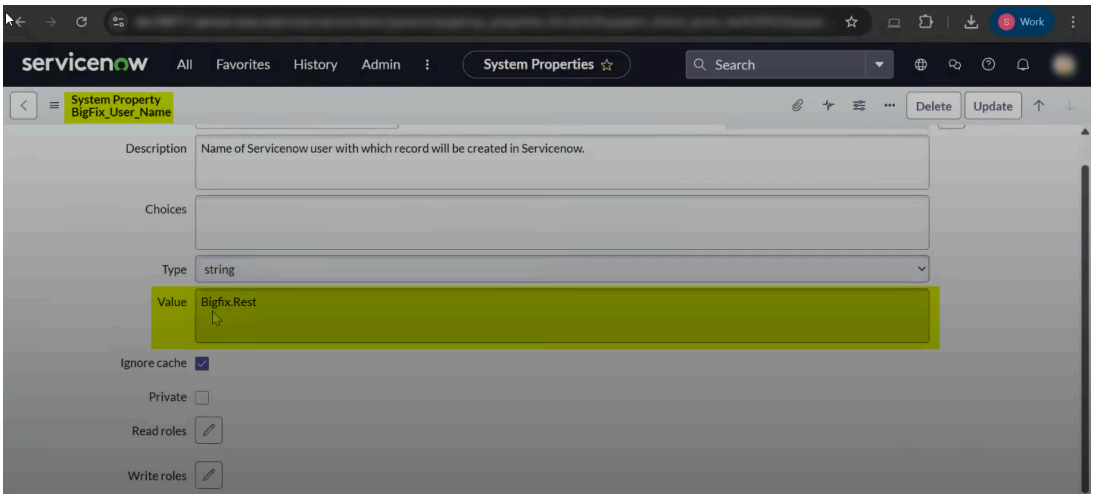


This search will result in two BigFix® properties: **BigFix_User_Key** & **BigFix_User_Name**.

a. **BigFix_User_Key** is the password of the ServiceNow™ user (user with the exception manager role or persona).



b. **BigFix_User_Name** is the user name of the ServiceNow™ user (user with the exception manager role or persona).



Set Global Policy

Learn how to reset the Application Control policy on target endpoints to its original default state. This task removes all custom-defined rules, establishing a clean security baseline and ensuring that only explicitly allowed applications are permitted.

Learn how to reset the Application Control policy on target endpoints to its original default state.

This task allows an administrator to reset the Application Control policy on target endpoints to its original default state. By running this action, you will be able to remove all custom-defined rules and restore the policy to the initial configuration created during the agent's installation.

Warning: Running this task will permanently delete all the existing custom application control rules from the `bes_bac.pol` file on the selected endpoints. This action is irreversible.

Note: Proceed only if you want to revert the endpoints to a factory default security policy.

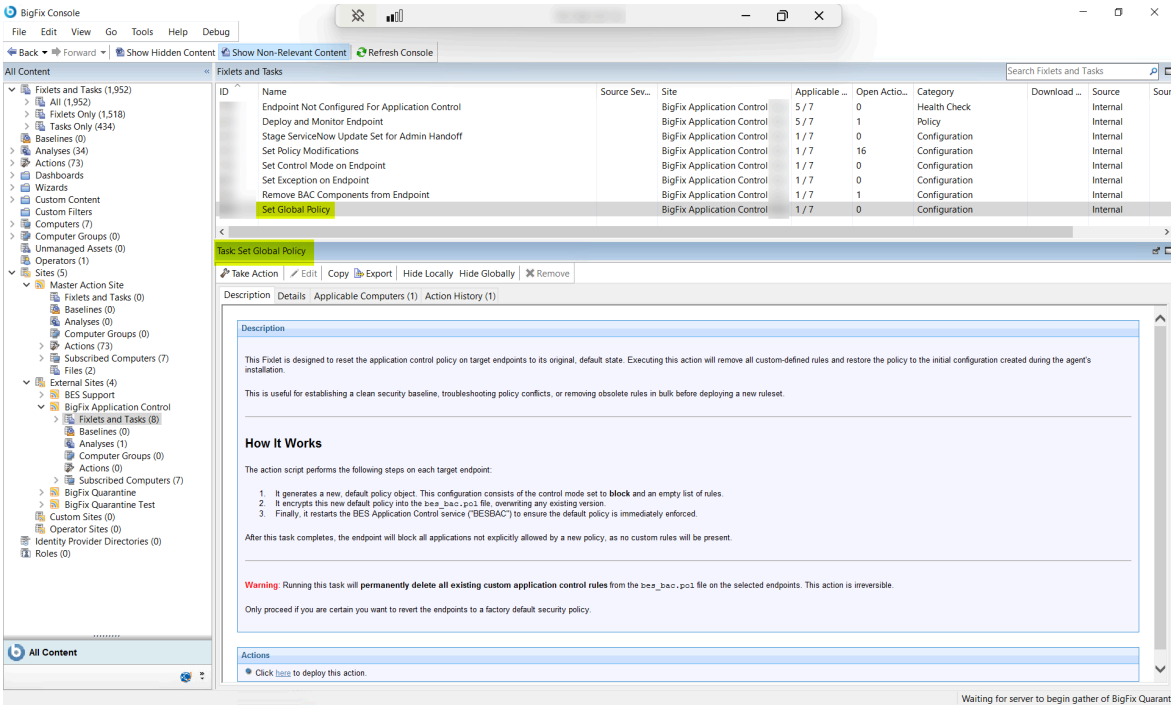
This task is useful for establishing a clean security baseline, troubleshooting policy conflicts, or removing obsolete rules in bulk before deploying a new ruleset.

This task's action script performs the following steps on each target endpoint:

1. It generates a new default policy object. This policy configuration consists of the control mode set to block and an empty list of rules.
2. It encrypts the new default policy into the `bes_bac.pol` file, overwriting any existing versions.
3. Lastly, it restarts the BES Application Control service (BESBAC) to ensure the default policy is immediately enforced.

After this task completes, the endpoint will block all applications not explicitly allowed by a new policy, as no custom rules are present.

1. From the **Fixlets and Tasks** pane, select **Task: Set Global Policy**.



2. Select the **Take Actions** tab and select the endpoints on which you want to apply this task.
3. Click **OK**.

Remove BigFix® Application Control from an Endpoint

This topic provides instructions for administrators to remove Application Control from target endpoints using the Task: Remove BAC Components from Endpoints. This process involves stopping the BAC service, deleting associated files, and cleaning user profiles.

Learn how to remove BigFix Application Control from managed endpoints.

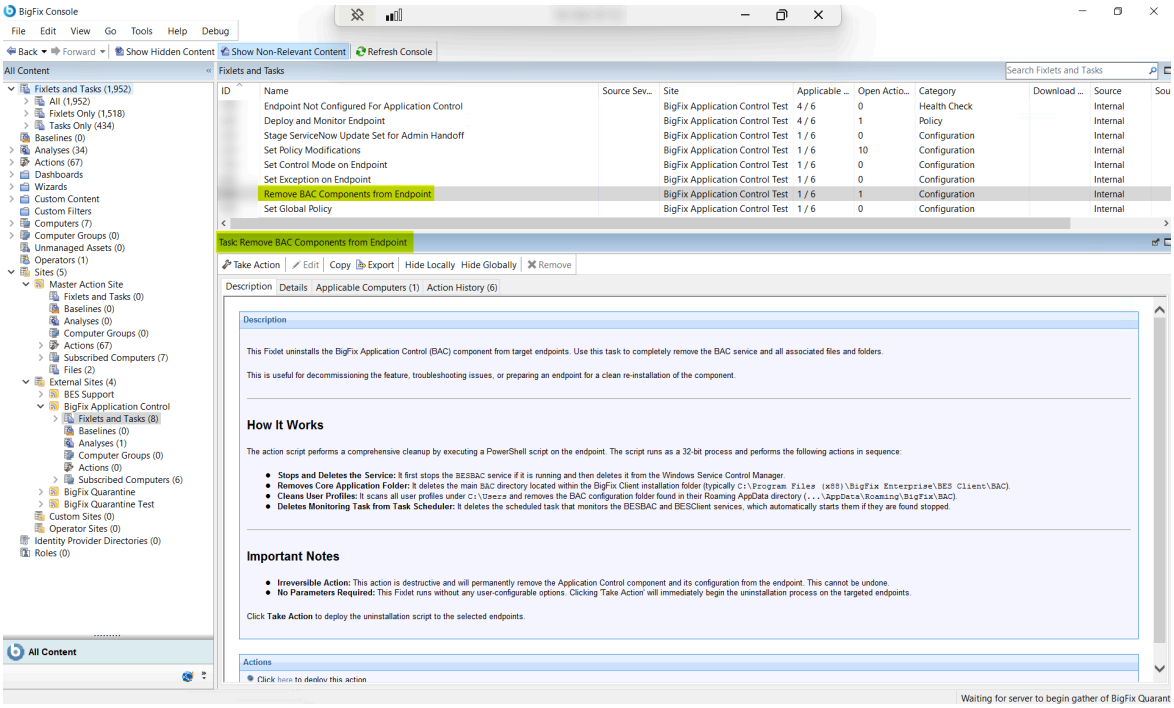
As an administrator, you can remove or uninstall BigFix Application Control from target endpoints. This task removes the BAC service and all associated files and folders from the target endpoints.

You use the **Task: Remove BAC Components from Endpoints** for uninstalling **Application Control**. This task performs the following actions:

1. Stops and deletes the BESBAC service from Windows™ Service Control Manager.
2. Removes the BAC directory located in the BigFix Client installation folder.
3. Scans and cleans user profiles by removing the BAC folder from their Roaming AppData directory.
4. Deletes the task that monitors BESBAC and `BESClient` services.

Follow the steps below to configure the watcher service refresh interval:

1. From the **Fixlets and Tasks** pane, select **Task: Remove BAC Components from Endpoint**.



2. Select the **Take Actions** tab and select the endpoints from which you want to remove BigFix Application Control.
3. Click **OK**.

Chapter 4. Support

For more information about this product, see the following resources:

- BigFix Support Portal
- BigFix Developer
- BigFix Playlist on YouTube
- BigFix Tech Advisors channel on YouTube
- BigFix Forum

Notices

This information was developed for products and services offered in the US.

HCL may not offer the products, services, or features discussed in this document in other countries. Consult your local HCL representative for information on the products and services currently available in your area. Any reference to an HCL product, program, or service is not intended to state or imply that only that HCL product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any HCL intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-HCL product, program, or service.

HCL may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

HCL
330 Potrero Ave.
Sunnyvale, CA 94085
USA
Attention: Office of the General Counsel

For license inquiries regarding double-byte character set (DBCS) information, contact the HCL Intellectual Property Department in your country or send inquiries, in writing, to:

HCL
330 Potrero Ave.
Sunnyvale, CA 94085
USA
Attention: Office of the General Counsel

HCL TECHNOLOGIES LTD. PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some jurisdictions do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. HCL may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-HCL websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this HCL product and use of those websites is at your own risk.

HCL may use or distribute any of the information you provide in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

HCL
330 Potrero Ave.
Sunnyvale, CA 94085
USA
Attention: Office of the General Counsel

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by HCL under terms of the HCL Customer Agreement, HCL International Program License Agreement or any equivalent agreement between us.

The performance data discussed herein is presented as derived under specific operating conditions. Actual results may vary.

Information concerning non-HCL products was obtained from the suppliers of those products, their published announcements or other publicly available sources. HCL has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-HCL products. Questions on the capabilities of non-HCL products should be addressed to the suppliers of those products.

Statements regarding HCL's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to actual people or business enterprises is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to HCL, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. HCL, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided "AS IS," without warranty of any kind. HCL shall not be liable for any damages arising out of your use of the sample programs.

Each copy or any portion of these sample programs or any derivative work must include a copyright notice as follows:
© (your company name) (year).
Portions of this code are derived from HCL Ltd. Sample Programs.

Trademarks

HCL Technologies Ltd. and HCL Technologies Ltd. logo, and hcl.com are trademarks or registered trademarks of HCL Technologies Ltd., registered in many jurisdictions worldwide.

Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Other product and service names might be trademarks of HCL or other companies.

Terms and conditions for product documentation

Permissions for the use of these publications are granted subject to the following terms and conditions.

Applicability

These terms and conditions are in addition to any terms of use for the HCL website.

Personal use

You may reproduce these publications for your personal, noncommercial use provided that all proprietary notices are preserved. You may not distribute, display or make derivative work of these publications, or any portion thereof, without the express consent of HCL.

Commercial use

You may reproduce, distribute and display these publications solely within your enterprise provided that all proprietary notices are preserved. You may not make derivative works of these publications, or reproduce, distribute or display these publications or any portion thereof outside your enterprise, without the express consent of HCL.

Rights

Except as expressly granted in this permission, no other permissions, licenses or rights are granted, either express or implied, to the publications or any information, data, software or other intellectual property contained therein.

HCL reserves the right to withdraw the permissions granted herein whenever, in its discretion, the use of the publications is detrimental to its interest or, as determined by HCL, the above instructions are not being properly followed.

You may not download, export or re-export this information except in full compliance with all applicable laws and regulations, including all United States export laws and regulations.

HCL MAKES NO GUARANTEE ABOUT THE CONTENT OF THESE PUBLICATIONS. THE PUBLICATIONS ARE PROVIDED "AS-IS" AND WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE.