Application Control User's Guide

Special notice

Before using this information and the product it supports, read the information in Notices *(on page xli)*.

Edition notice

This edition applies to BigFix version 10 and to all subsequent releases and modifications until otherwise indicated in new editions.

Contents

Chapter 1. Overview **5**

Chapter 2. What's new in this release **7**

Chapter 3. Features added in previous releases **9**

Chapter 4. Application Control Persona's **11**

Chapter 5. System Architecture **12**

Chapter 6. Migrating from Application Control v1.0.0 to v2.0.0 ..... **15**

Chapter 7. Administering Application Control v2.0.0 ..... **16**

Creating & Setting-up Self Signed Certificate on Endpoint 17

Deploying Default Microsoft Base Policy 19

Deploying Custom Base Policy 21

Deploying Supplemental Policy on Endpoint 24

Refreshing Self-Signed Certificate & Updating Deployed Policies Signers on Endpoint 26

Refreshing Thumbprint of Deployed Policies Signers on Endpoint 28

Enforcing Secure ACL on BAC Folder on Endpoint 30

Generating Blocked WDAC Event Logs on Endpoint 32

Removing (Base/Supplemental) Policy from Endpoint 34

Removing WDAC Components from Endpoint 36

Viewing Endpoint Details using BigFix® Web Reports 38

Notices xli

Index .....

Chapter 1. Overview

Set a secure environment by using Application Control.

BigFix® Application Control is a security solution designed to manage which software can run on Windows devices within BigFix environments in an organization. It utilizes Windows Defender Application Control (WDAC) as the chosen enforcement engine to apply policies at the kernel level, preventing unauthorized software execution through kernel-level enforcement. It is a lightweight, native enforcement system designed for comprehensive management of application execution across enterprise endpoints. Following is a more detailed breakdown of its core components and how they function:

1. **Core Security Mechanism: WDAC Integration**

   The solution's strength lies in its use of Windows Defender Application Control (WDAC).

   - **Kernel-level Enforcement:** Unlike standard software that runs in "user mode," WDAC operates within the Windows kernel. This means the security checks happen at the deepest layer of the operating system.
   - **Allowlisting vs. Blocklisting:**
     - **Allowlisting:** A "Zero Trust" approach where only approved applications can run; everything else is blocked by default.
     - **Blocklisting:** Specific known-malicious or unwanted programs are banned, while others are permitted.

2. **Centralized Management & Deployment**

   BigFix acts as the "brain" for these Windows security features, allowing IT teams to manage everything from one place.

   - **The BigFix Console:** Instead of manually configuring every computer, administrators use the central BigFix console to create rules (policies) and push them out to thousands of endpoints simultaneously.
   - **Policy Management:** This includes defining which softwares are safe and which are restricted based on the inputs (like file hash, file name, file path, or publisher) provided.

Table 1. BigFix Application Control v2.0.0 Summary Table

Feature	Benefit
WDAC Engine	Provides high-level security that is difficult for malware to disable.
Kernel Enforcement	Stops unauthorized code before it can even start.
BigFix Console	Enables massive scalability for enterprise 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 for the future.

Chapter 2. What's new in this release of Application Control

A summary of new or changed features and enhancements included in BigFix Application Control v2.0.0

BigFix Application Control v2.0.0

New features that are introduced in Application Control v2.0.0

This release focuses on providing a robust, stable, and secure foundation for application control.

WDAC Base Policy Deployment

Deploy Microsoft-provided WDAC base policies to Windows endpoints.

Policies are deployed and activated using BigFix Fixlets.

Supplemental Policy Deployment

Deploy WDAC supplemental policies to endpoints with an active base policy.

Centralized Policy Management

Manage WDAC policies from the BigFix Console.

Support for publisher, file hash, file name, and file path rules.

Support for Audit and Enforcement modes.

Monitoring and Reporting and Audited Application Blocks

Collect and report applications that would be blocked in Audit mode.

Validate application impact before enforcement.

Blocked Application Reporting

Report blocked application execution events in Enforcement mode.

Includes application name, file path, hash, publisher, rule, and time stamp.

Events aggregated across endpoints to identify frequently blocked applications.

Identify impacted endpoints and analyze block patterns.

Active Policy Monitoring

View active WDAC policies on endpoints.

Includes base and supplemental policies and enforcement mode.

Verify policy enforcement and ensure compliance across endpoints.

Deployment Status Monitoring

Track policy deployment status across endpoints.

Identify failed or incomplete deployments.

Policy Management and Policy Removal

Remove WDAC base or supplemental policies from endpoints for rollback or recovery.

Security

Policies are securely signed to ensure integrity.

Role-based access control for policy operations.

Performance and Scalability

Support for large-scale deployments.

Minimal impact on endpoint performance during enforcement.

All policies (Base & Supplemental) are applied without reboot.

Additional information about this release

Published Site and Component Versions:

- Application Control site version: 2

Application Control Documentation links:

- https://help.hcl-software.com/bigfix/11.0/lifecycle/lifecycle_application_control.html
- https://help.hcl-software.com/bigfix/10.0/lifecycle/lifecycle_application_control.html

Chapter 3. Features added in previous releases

In this section, you can find the feature updates from the previous versions.

The following features were released with ACv1.0.0

Features that are introduced in Application Control V1.0.0

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, enabling IT administrators to enforce application usage policies with real-time monitoring and exception management capabilities.

This release focuses on providing a robust, stable, and secure foundation for application control.

Centralized Policy and Rule Management

Configure and deploy the solution from the BigFix console. Create powerful Allow Rules (for default-deny policies) or Block Rules (for default-allow policies) to control application execution. Rules can also include time constraints to grant temporary access.

Bulk Ruleset Management

Easily upload a CSV file containing a set of rules to apply a baseline policy across all subscribed computers.

Endpoint Visibility

See the effective control policy (the complete set of rules) for any endpoint directly from the BigFix Console. Approved exceptions can be viewed using BigFix® Web Reports.

Real-time Block Notifications

When a process is blocked, a notification utility instantly appears, informing the user that the application is not permitted to run.

Application Control Policy

The collection of individual rules and CSV rulesets that are applied to an endpoint to restrict or allow application execution.

Seamless Exception Request Work-flow

The notification utility allows users to request a temporary exception. They can provide a business justification and a desired expiration date, which is then sent directly to ServiceNow to create an exception request ticket.

For Security and Performance

Endpoint Policy Encryption Ensures Secure Monitoring and Immutable Rules

The effective policy on the endpoint is encrypted, ensuring that a user, even one with administrative privileges cannot modify the rules.

Lightweight Endpoint Service

A compiled C# *watcher service* enforces policies in real-time with minimal CPU and memory overhead, ensuring no impact on user productivity.

Log Retention

Endpoint logs are stored for 10 days to provide an audit trail of local activity.

This release contains the following key features:

Table 2. Key Features Application Control Release V1.0.0

Features	Description
Compliance Enforcement	Block unauthorized applications to meet corporate and regulatory requirements.
Policy Deployment	Administrators can add rules to block or allow apps using file paths or registry rules.
Process Monitoring	The Process Monitoring service on endpoints polls for policies and enforces them in real-time. When a blocked app is accessed, it is terminated, a notification is shown, and a log entry is created.
Exception Request Handling	Allow temporary, audited access to blocked applications with proper approval through your ITSM system.

ServiceNow Integration Workflow

Application Control integrates with ServiceNow to manage the exception Lifecycle:

1. **Setup**: A BigFix operator installs the Application Control UpdateSet XML in ServiceNow.
2. **Request**: The endpoint utility calls a ServiceNow REST API to create an exception request when a user submits one. Distributed Denial-of-Service (DDoS) protection is active, rate-limiting requests to 60 per hour.
3. **Approval**: The exception manager approves or denies the request within ServiceNow.
4. **Fulfillment**: Upon approval, ServiceNow calls the BigFix Action API to create and deploy a temporary allow rule to the specific endpoint. The ServiceNow ticket is then updated with a "fulfilled" status.

Additional information about this release

Published Site Versions:

Site Name	Site Version
Application Control	1.0.0

Chapter 4. Application Control Persona’s

This document outlines the various user persona's associated with the BigFix console, including the Security Administrator, IT Administrator, SOC Analyst, and End User.

In the following points each persona is defined with its responsibilities and interactions within the system, providing clarity on user responsibilities in managing and utilizing the solution.

Security Administrator

Defines security posture, creates allow/block policies, ensures compliance.

IT Administrator:

Deploys policies to endpoints, manages agent health, handles first-level support.

SOC Analyst:

Monitors blocked events and investigates potential threats via dashboards.

End User:

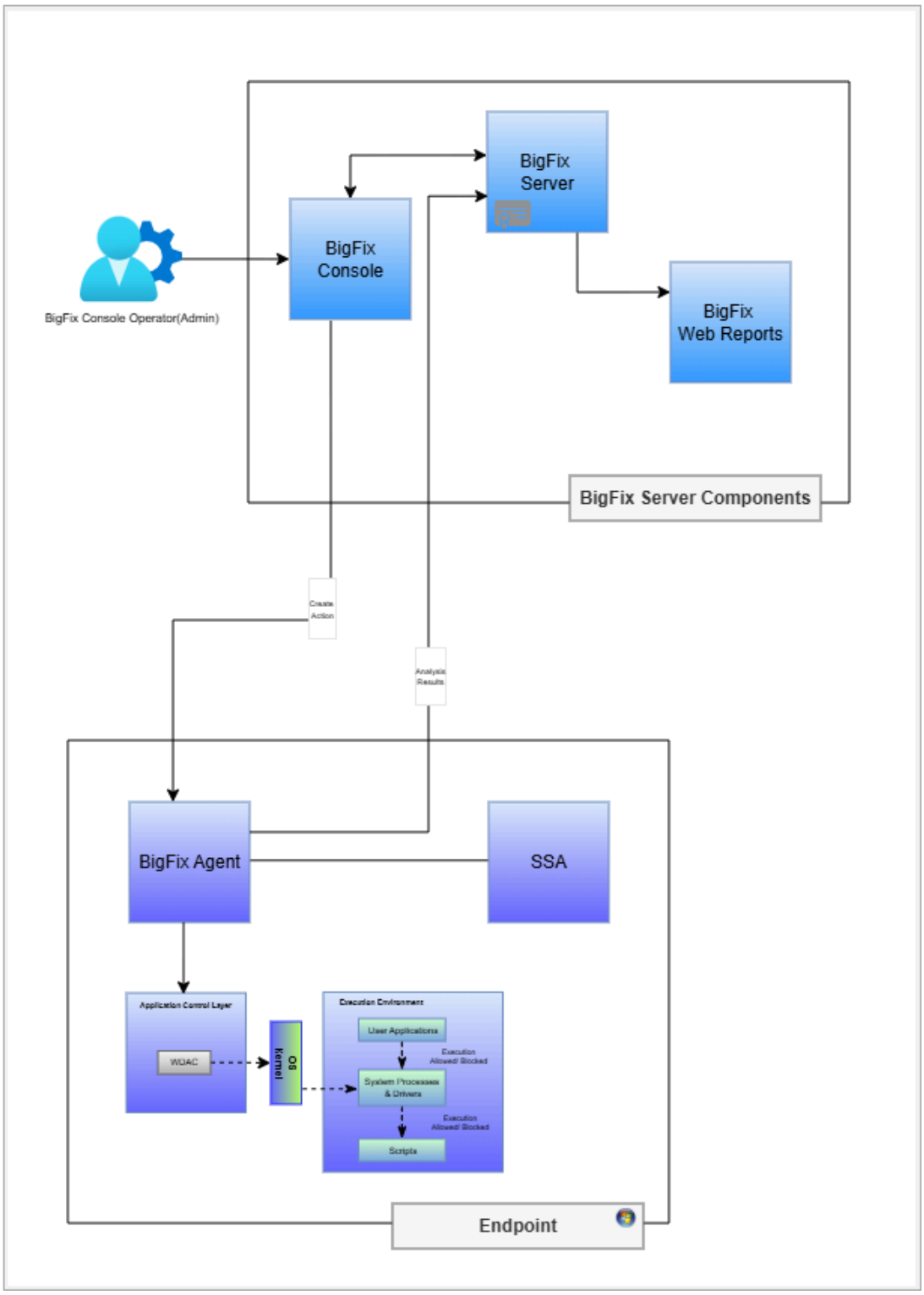
Uses the solution with clear block messages and simple exception requests.

Chapter 5. System Architecture

The system architecture 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 other components.

The system architecture diagram illustrates the interaction between BigFix Server components and BigFix endpoints. 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.

  - **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 administrative report(s) that are shown for Application Control:

    - Effective Policy on Endpoint

- **Endpoints**

  On the endpoints the BigFix agent is installed which communicates with Application Control Layer to enforce allowlisting or blocklisting of applications using kernel-based WDAC.

WDAC Enforcement Model: The Application Control policy is authored in XML, then compiled to binary, and then is digitally signed. The digitally signed certificate is then deployed to `<EFI System Partition>\EFI\Microsoft\Boot\CiPolicies\Active\`. The OS kernel validates the policy and only the allowlisted applications are allowed to execute.

Chapter 6. Migrating from Application Control v1.0.0 to Application Control v2.0.0

Learn how to migrate from Application Control v1.0.0 to Application Control v2.0.0.

As BigFix Application Control v2.0.0 is the only currently supported version of Application Control, it is strongly recommended that you migrate to Application Control v2.0.0. This migration replaces the Application Control v1.0.0 *custom BAC rule engine* with Application Control v2.0.0 *WDAC based enforcement*. Existing allow rules are recreated as **Supplemental Policies**. This migration is a one-time, non-reversible per endpoint without redeployment process.

Migration Flow Summary

Step 1: Export AC v1.0.0 Rules → **Step 2:** Remove AC v1.0.0 solution from endpoints → **Step 3:** Create & setup self-signed certificate → **Step 4:** Deploy AC v2.0.0 base policy → **Step 5:** Create supplemental policies → **Step 6:** Monitor via web reports

 **Remember:**

- ◦ Migration is a **one-time** process.
  ◦ Base policy once set **cannot be switched**.
  ◦ Supplemental policies only extends the allowlist.
  ◦ WDAC uses a **default deny** enforcement model.
  ◦ Block rules are not migrated.
  ◦ Application Control supports only one base policy (MVP).

Refer to Migrating from Application Control v1.0.0 to Application Control v2.0.0 topic for more details.

Chapter 7. Administrating Application Control v2.0.0

Users with an administrator persona can perform the tasks mentioned in this chapter in Application Control v2.0.0.

All the tasks described in this section are to be performed by users with administrator role for installing, configuring, and removing BigFix Application Control v2.0.0.

The following tasks are covered under this topic:

- **Create & Setup Self-Signed Certificate on Endpoint v2.0**:

  This task generates and configures a self-signed code-signing certificate on the endpoint for use with Windows Defender Application Control (WDAC).

- **Deploy Default Microsoft Base Policy v2.0**:

  This task deploys a signed Windows Defender Application Control (WDAC) Base Policy on an endpoint using a secure and controlled workflow. The policy is selected from a list of Microsoft-recommended baseline policies and applied as the system's active base policy.

- **Deploy Custom Base Policy v2.0**:

  This task deploys a Custom Windows Defender Application Control (WDAC) Base Policy on the endpoint. The raw XML configuration for the policy must be provided before taking action.

- **Deploy Supplemental Policy on Endpoint v2.0**:

  This task creates and deploys a signed Windows Defender Application Control (WDAC) supplemental policy on the endpoint using a controlled and secure approach. The supplemental policy is generated as a separate policy file and linked to an existing base policy using the provided Base Policy GUID.

- **Refresh Self-Signed Certificate and Update Deployed Policies Signers on Endpoint v2.0**:

  This task automates the end-to-end renewal, signing, and deployment of Windows Defender Application Control (WDAC) policies to ensure policies remain active and securely signed.

- **Refresh Thumbprint of Deployed Policies Signers on Endpoint v2.0**:

  This task automates the taking of the thumbprint of the new certificates and then signs them to ensure policies remain active and securely signed.

- **Enforce Secure ACL on BAC Folder on Endpoint v2.0**:

  This task secures the BigFix Application Control (BAC) directory by enforcing strict access control and ownership settings.

- **Generate Blocked WDAC Event Logs on Endpoint v2.0**:

  This task extracts Windows Defender Application Control (WDAC) / App Control block events from endpoint event logs for both audit and enforced modes, and generates a structured JSON report for analysis.

- **Remove (Base/Supplemental) Policy from Endpoint v2.0**:

  This task manages Windows Defender Application Control (WDAC) policies on the endpoint by supporting both supplemental policy removal and a full base policy reset using a controlled and safe approach.

- **Remove WDAC Components from Endpoint v2.0**:

  This task removes all the associated files and folders related to Windows Defender Application Control (WDAC).

Creating & Setting-up Self Signed Certificate on Endpoint

Use this task to generate and configure a self-signed code-signing certificate on the endpoint for use with Windows Defender Application Control (WDAC).

The task performs the following:

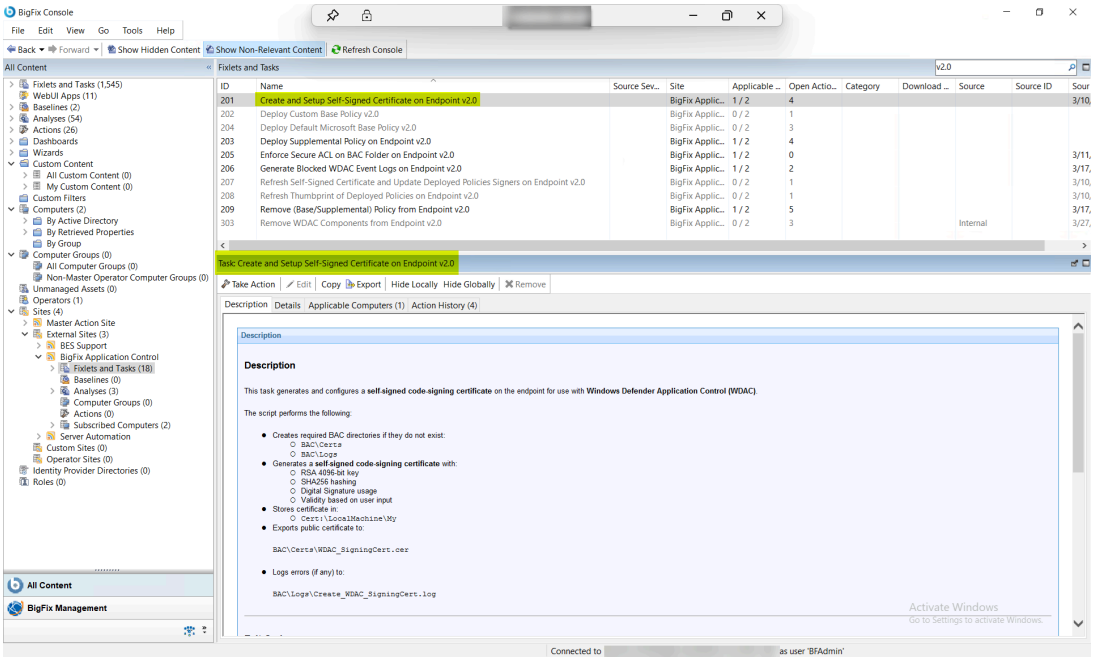
- Creates the following required BAC directories if they do not exist:
  - `BAC\Certs`
  - `BAC\Logs`
- Generates a self-signed code-signing certificate with:
  - RSA 4096-bit key
  - SHA256 hashing
  - Digital Signature usage
  - Validity based on user input
- Stores the certificate at the `Cert:\LocalMachine\My` location.
- Exports the public certificate to the `BAC\Certs\WDAC_SigningCert.cer` folder.
- Logs errors (if any) to the `BAC\Logs\Create_WDAC_SigningCert.log` location.

Refer to the table below to know more about the task's exit code.

Table 3. Exit Codes Table

Exit Code	Meaning
0	Success
10	BAC directory creation failure
11	Certificate directory creation failure
12	Log directory creation failure
20	Certificate creation failure
30	Certificate export failure

Figure 2. Task: Setup and Create Self-Signed Certificate



1. In the BigFix Console, navigate to **All Content > BigFix Application Control > Fixlets and Tasks**.
2. From the **Fixlets and Tasks** pane, select **Task: Setup and Create Self-Signed Certificate on Endpoint v2.0**.
3. From the **Task: Setup and Create Self-Signed Certificate on Endpoint v2.0** pane, under **Configuration Options**, enter the following information:

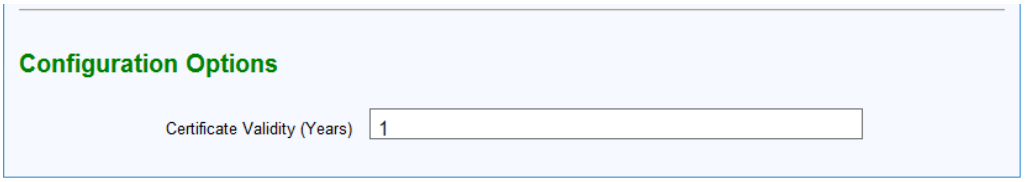


Table 4. Task: Setup and Create Self-Signed Certificate on Endpoint v2.0 Configuration Options

Field Name	Description
Certificate Validity (Years)	Number of years for which the newly generated certificate will be valid.

4. From the **Task: Setup and Create Self-Signed Certificate on Endpoint v2.0** 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**.

A successful execution of this task results in the following outcomes:

- A self-signed WDAC certificate is created on the endpoint.
- The certificate is available in the `LocalMachine` store.

- The public certificate is exported to the `BAC` folder.
- A certificate is ready for WDAC policy signing and deployment.

Deploying Default Microsoft Base Policy

Use this task to deploy a signed Windows Defender Application Control (WDAC) Base Policy on the endpoint using a secure and controlled workflow. This policy is selected from a list of Microsoft-recommended baseline policies and are applied as the endpoint's active base policy.

This deployment ensures that the policy is trusted, enforced, and persisted at the firmware level by placing it in the EFI partition. This enables strong application control, protecting the system from unauthorized or untrusted code execution.

The task performs the following actions:

- Allows the selection of a Microsoft WDAC base policy template from the predefined options.
- Dynamically downloads only the selected policy file using secure hash validation (SHA1/SHA256).
- Copies the selected XML policy to the working directory.
- Initializes or replaces the existing base policy with a new policy id.
- Converts the policy from XML format to binary `*.cip` format.
- Signs the policy using a trusted code-signing certificate.
- Validates the signed output to ensure integrity.
- Mounts the EFI system partition.
- Deploys the signed policy to `EFI\Microsoft\Boot\CiPolicies\Active` location.
- Triggers a policy refresh (if supported) or applies on reboot.
- Logs all execution details (success/failure) to `BAC\Logs\Deploy_WDAC_BasePolicy.log` location.

Refer to the table below to know more about the task's exit code.

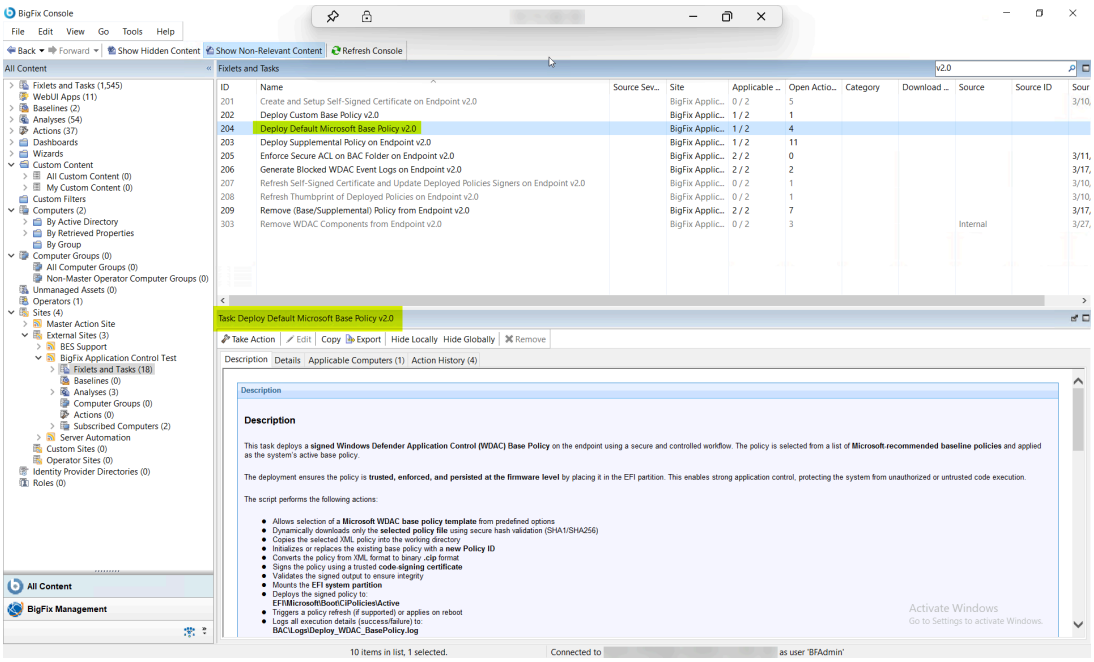
Table 5. Exit Codes Table

Exit Code	Meaning	Description
0	Success	The WDAC base policy was successfully processed, signed, and deployed.
10	Working directory creation failed	The BAC working directory could not be created or accessed.
11	Log directory creation failed	The logging directory could not be created, preventing execution tracking.
12	Policy directory creation failed	The policy storage directory could not be initialized.
20	Template missing	The selected WDAC policy template file was not found or failed to download.

Table 5. Exit Codes Table (continued)

Exit Code	Meaning	Description
30	Policy processing failure	Error occurred during policy preparation, version, or rule configuration.
40	Binary conversion failure	Failed to convert the WDAC policy from XML format to binary (.cip).
50	Signing failure	The policy signing process failed or the signed output was not generated correctly.
60	Deployment failure	Failed to mount the EFI partition or copy the policy to the target location.
70	Policy refresh failure	The policy refresh process failed after deployment. A reboot may be required.

Figure 3. Task: Deploy Default Microsoft Base Policy



1. In the BigFix Console, navigate to **All Content > BigFix Application Control > Fixlets and Tasks**.
2. From the **Fixlets and Tasks** pane, select **Task: Deploy Default Microsoft Base Policy v2.0**.
3. From the **Task: Deploy Default Microsoft Base Policy v2.0** pane, under **Configuration Options** select one of the following policy options:

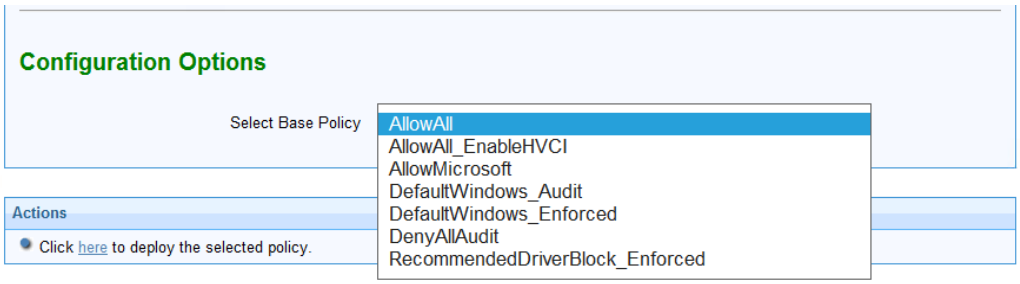


Table 6. Task: Deploy Default Microsoft Base Policy v2.0 Configuration Options

Field Name	Options	Description
Select Base Policy	AllowAll	Permissive policy (allows all applications)
	AllowAll_EnableHVCI	Permissive policy with HVCI support
	AllowMicrosoft	Allows only Microsoft-signed binaries
	DefaultWindows_Audit	Default Microsoft policy in audit mode
	DefaultWindows_Enforced	Default Microsoft enforced policy (recommended baseline)
	DenyAllAudit	Blocks all applications in audit mode
	RecommendedDriverBlock_Enforced	Blocks known vulnerable drivers

4. From the **Task: Deploy Default Microsoft Base Policy v2.0** 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**.

A successful execution of this task results in the following outcomes:

- The selected WDAC base policy is successfully deployed to the system.
- The policy becomes the active enforcement policy for Application Control.
- The system enforces or audits applications based on the selected policy type.
- The policy persists across reboots via EFI deployment.
- Execution logs become available for audit and troubleshooting.

Deploying Custom Base Policy

Use this task to deploy a Custom Windows Defender Application Control (WDAC) Base Policy on the endpoint. You must provide the raw XML configuration for the policy before taking action.

This deployment ensures that the custom policy is trusted, enforced, and persists at the firmware level by placing it in the EFI partition. The script also automatically handles version increments and injects necessary rules to ensure the BigFix client and deployment tools remain operational.

The task performs the following actions:

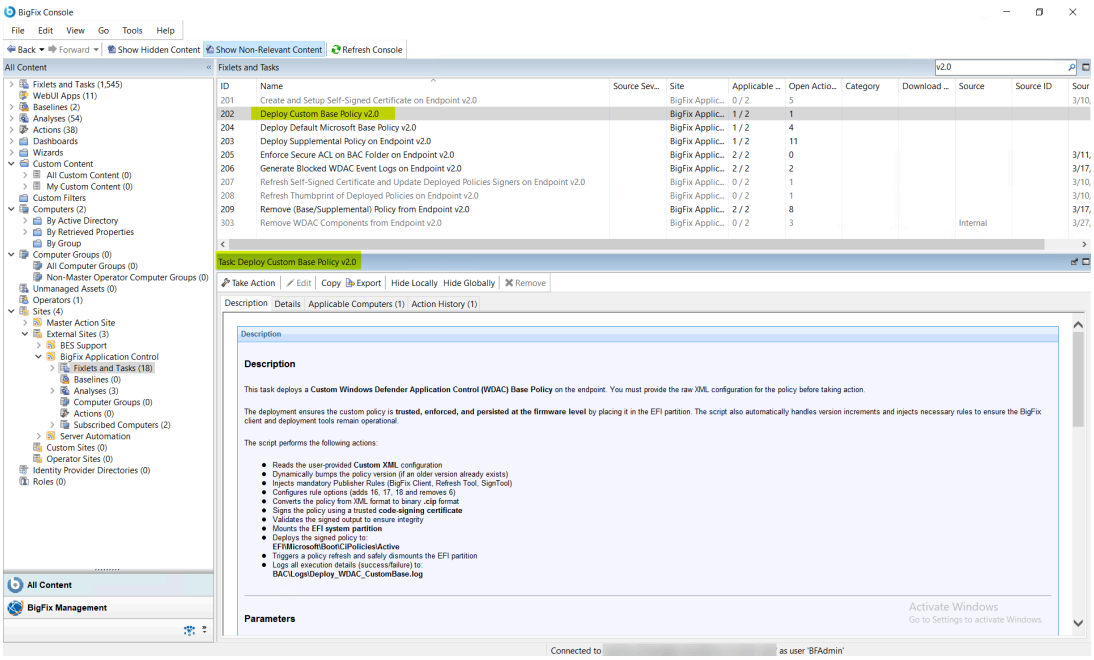
- Reads the user-provided Custom XML configuration.
- Dynamically bumps the policy version (if an older version already exists).
- Injects mandatory publisher rules (BigFix Client, Refresh Tool, SignTool).
- Configures rule options (adds 16, 17, 18 and removes 6).
- Converts the policy from XML format to binary `*.cip` format.
- Signs the policy using a trusted code-signing certificate.
- Validates the signed output to ensure integrity.
- Mounts the EFI system partition.
- Deploys the signed policy to `EFI\Microsoft\Boot\CiPolicies\Active` loaction.
- Triggers a policy refresh and safely dismounts the EFI partition.
- Logs all execution details (success/failure) to the `BAC\Logs\Deploy_WDAC_CustomBase.log` location.

Refer to the table below to know more about the task's exit code.

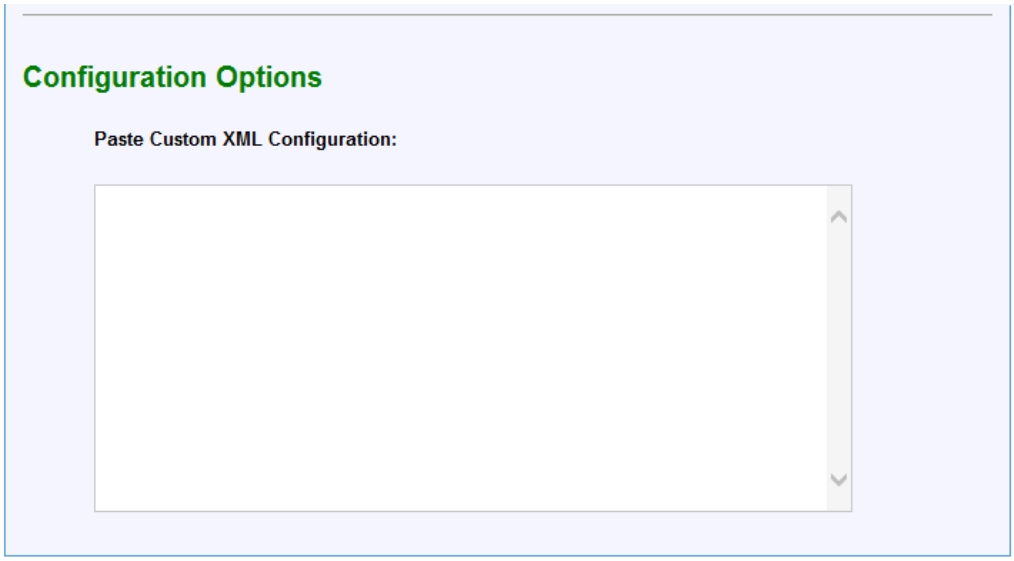
Table 7. Exit Codes Table

Exit Code	Meaning	Description
0	Success	The WDAC base policy was successfully processed, signed, and deployed.
10	Working directory creation failed	The BAC working directory could not be created or accessed.
11	Log directory creation failed	The logging directory could not be created, preventing execution tracking.
12	Policy directory creation failed	The policy storage directory could not be initialized.
30	Policy processing failure	Error occurred during policy preparation, version bumping, or rule injection.
40	Binary conversion failure	Failed to convert the WDAC policy from XML format to binary (.cip).
50	Signing failure	The policy signing process failed or generated an invalid signature.
60	Deployment failure	Failed to mount the EFI partition or copy the policy to the target location.
70	Policy refresh failure	The policy refresh process or EFI dismount failed.

Figure 4. Task: Deploy Custom Base Policy



1. In the BigFix Console, navigate to **All Content > BigFix Application Control > Fixlets and Tasks**.
2. From the **Fixlets and Tasks** pane, select **Task: Deploy Custom Base Policy v2.0**.
3. From the **Task: Deploy Custom Base Policy v2.0** pane, under **Configuration Options**, paste the raw XML configuration for your base policy into the provided text area.



4. From the **Task: Deploy Custom Base Policy v2.0** 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**.

A successful execution of this task results in the following outcomes:

- The custom WDAC base policy is successfully deployed to the system.
- The system enforces or audits applications based on the provided XML logic.
- The policy persists across reboots via EFI deployment
- Execution logs become available for audit and troubleshooting.

Deploying Supplemental Policy on Endpoint

Use this task to create and deploy a signed Windows Defender Application Control (WDAC) supplemental policy on the endpoint using a controlled and secure approach. This supplemental policy is generated as a separate policy file and is linked to an existing base policy using the provided base policy GUID.

The task performs the following actions:

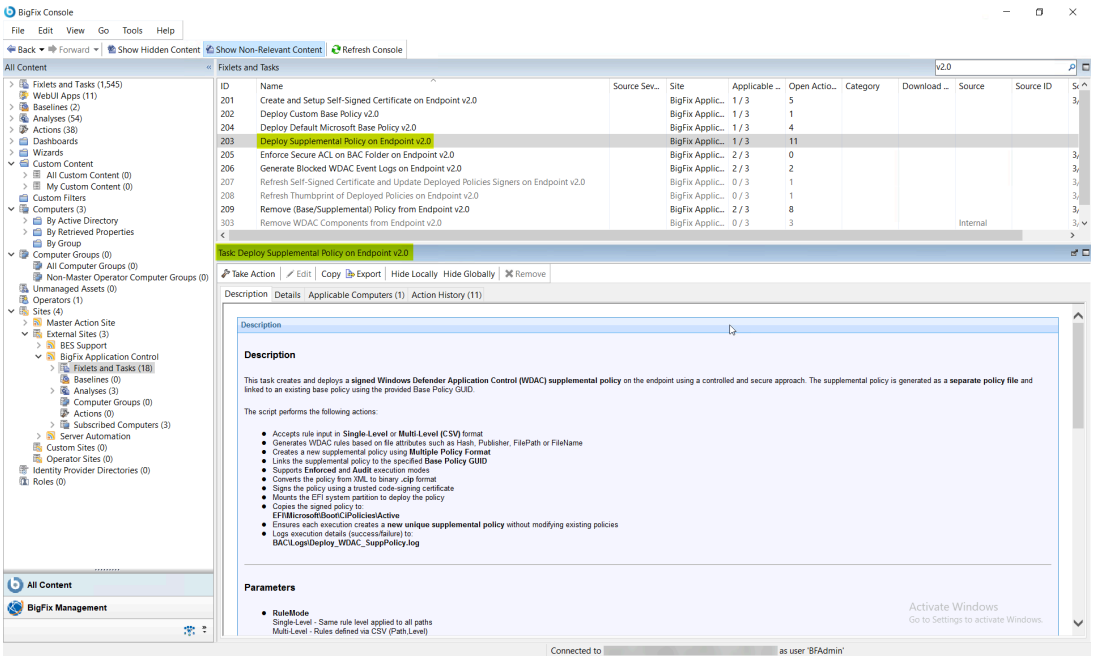
- Accepts the rule input in either **Single-Level** or **Multi-Level** (CSV) format.
- Generates WDAC rules based on file attributes such as hash, publisher, file path or file name.
- Creates a new supplemental policy using multiple policy format.
- Links the newly created supplemental policy to the specified base policy GUID.
- Supports enforced and audit execution modes.
- Converts the policy from XML to binary `*.cip` format.
- Signs the policy using a trusted code-signing certificate.
- Mounts the EFI system partition to deploy the policy.
- Copies the signed policy to the `EFI\Microsoft\Boot\CiPolicies\Active` location.
- Ensures each execution creates a new unique supplemental policy without modifying existing policies.
- Logs execution details (success/failure) to the `BAC\Logs\Deploy_WDAC_SuppPolicy.log` location.

Refer to the table below to know more about the task's exit code.

Table 8. Exit Codes Table

Exit Code	Meaning
0	Success
20	Missing base policy GUID
30	No valid rules generated
40	Signing failure or invalid signed output

Figure 5. Task: Deploy Supplemental Policy on Endpoint



1. In the BigFix Console, navigate to **All Content > BigFix Application Control > Fixlets and Tasks**.
2. From the **Fixlets and Tasks** pane, select **Task: Deploy Supplemental Policy on Endpoint v2.0**.
3. From the **Task: Deploy Supplemental Policy on Endpoint v2.0** pane, under **Configuration Options**, paste the raw XML configuration for your base policy into the provided text area.

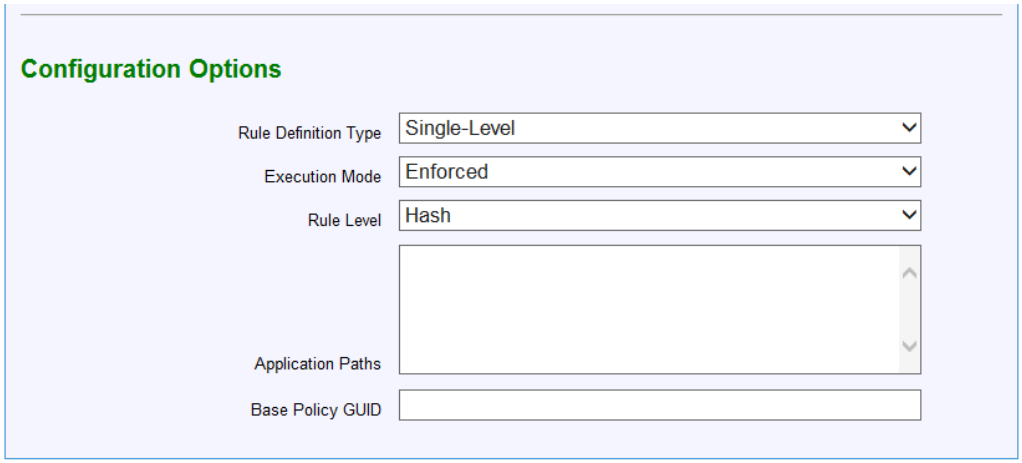


Table 9. Task: Deploy Supplemental Policy on Endpoint v2.0 Configuration Options

Field Name	Options	Description
Rule Definition Type	Single-Level	Same rule level applied to all paths
	Multi-Level	Rules defined via CSV (path, level)
Execution Mode	Enforced	Policy is enforced

Field Name	Options	Description
	Audit	Policy is applied in audit mode
Rule Level	Hash	Applicable only in Single-Level mode (Hash, Publisher, FilePath, FileName)
	Publisher	
	FilePath	
	FileName	
Application Paths	N/A	Text box. List of file paths (newline or comma separated) for Single-Level mode only
CSV Rules	N/A	Text box. CSV input for Multi-Level mode in the format: Path, Rule Level
Base Policy GUID	N/A	Text field. Required. Specifies the GUID of the base policy to be supplemented.

4. From the **Task: Deploy Supplemental Policy on Endpoint v2.0** 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**.

A successful execution of this task results in the following outcomes:

- A new WDAC supplemental policy is created and deployed.
- The policy is linked to the specified base policy.
- Existing policies remain unchanged.
- The endpoint enforces or audits rules based on the selected mode.

Refreshing Self-Signed Certificate & Updating Deployed Policies Signers on Endpoint

Use this task to automate the end-to-end renewal, signing, and deployment of Windows Defender Application Control (WDAC) policies to ensure policies remain active and securely signed.

The task follows the below listed workflow:

1. **Setup**: Initializes logging and ensures that the required BAC directories exist.
2. **Certificate Rotation**: Checks if the current WDAC signing certificate expires within 30 days. If yes, this task generates a new 4096-bit RSA self-signed certificate.
3. **XML Processing**: Scans for XML policies, automatically increments their version numbers, and updates the signer rules to trust the current certificate.

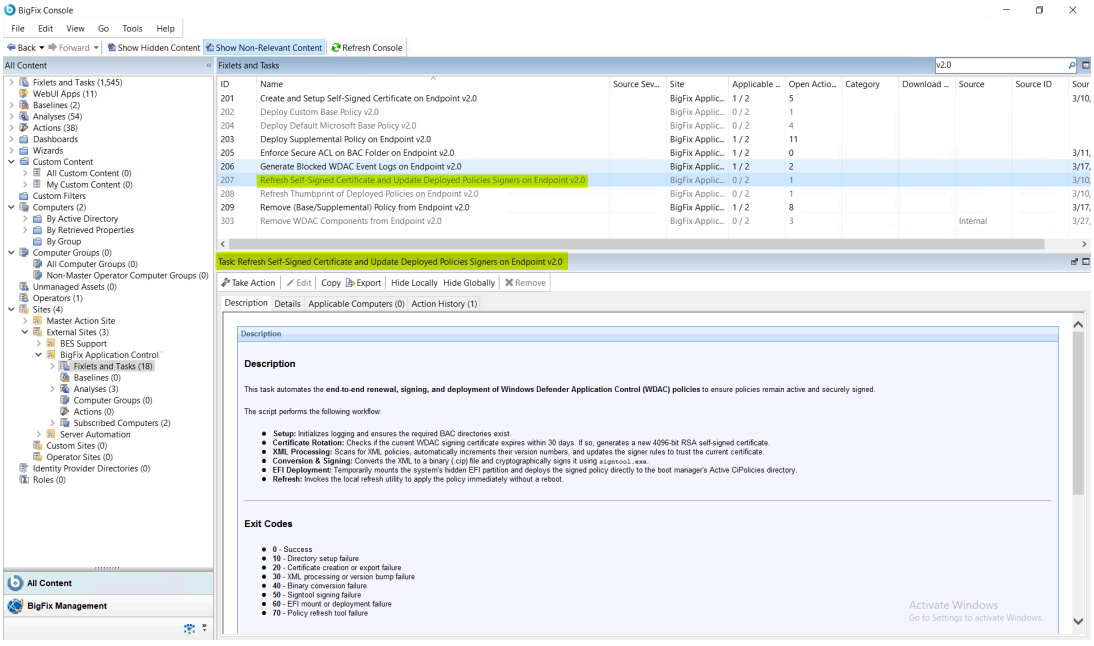
4. **Conversion & Signing**: Converts the XML to a binary `*.cip` file and cryptographically signs it using the `signtool.exe`.
5. **EFI Deployment**: Temporarily mounts the system's hidden EFI partition and deploys the signed policy directly to the boot manager's `Active CiPolicies` directory.
6. **Refresh**: Invokes the local refresh utility to apply the policy immediately without a reboot.

Refer to the table below to know more about the task's exit code.

Table 10. Exit Codes Table

Exit Code	Meaning
0	Success
10	Directory setup failure
20	Certificate creation or export failure
30	XML processing or version bumping failure
40	Binary conversion failure
50	Signtool signing failure
60	EFI mount or deployment failure
70	Policy refresh tool failure

Figure 6. Task: Refresh Self-Signed Certificate and Update Deployed Policies Signers on Endpoint



1. In the BigFix Console, navigate to **All Content > BigFix Application Control > Fixlets and Tasks**.
2. From the **Fixlets and Tasks** pane, select **Task: Refresh Self-Signed Certificate and Update Deployed Policies Signers on Endpoint v2.0**.
3. From the **Task: Refresh Self-Signed Certificate and Update Deployed Policies Signers on Endpoint v2.0** pane, under **Configuration Options**, enter the following information:

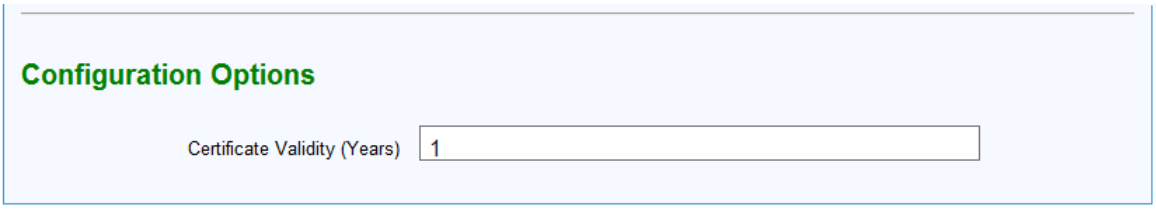


Table 11. Task: Refresh Self-Signed Certificate and Update Deployed Policies Signers on Endpoint v2.0 Configuration Options

Field Name	Description
Certificate Validity (Years)	Number of years for which the newly generated certificate will be valid.

4. From the **Task: Refresh Self-Signed Certificate and Update Deployed Policies Signers on Endpoint v2.0** 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**.

Note: Once this task is triggered, it remains as an open action and runs on the system whenever the system becomes relevant. Only an administrator can stop this task.

A successful execution of this task results in the following outcomes:

- WDAC signing certificate is rotated (if within 30 days of expiration).
- Local XML policies are updated with incremented version numbers and new signer rules.
- Cryptographically signed binary (*.cip) policies are successfully deployed to the EFI partition.
- System application control policies are immediately refreshed and enforced.
- A system reboot is required for the changes to take effect.

Refreshing Thumbprint of Deployed Policies Signers on Endpoint

Use this task to automate the end-to-end renewal, signing, and deployment of Windows Defender Application Control (WDAC) policies to ensure policies remain active and securely signed.

The task follows the below listed workflow:

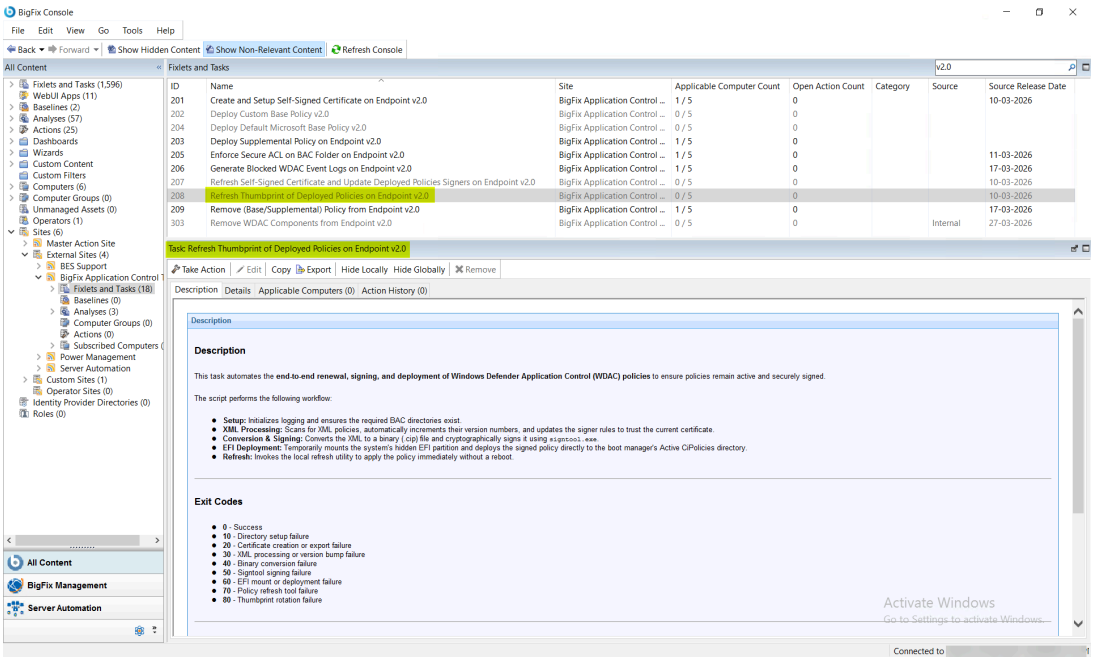
1. **Setup**: Initializes the logging and ensures that the required BAC directories exist.
2. **XML Processing**: Scans for the XML policies, automatically increments their version numbers, and updates the signer rules to trust the current certificate.
3. **Conversion & Signing**: Converts the XML to a binary (`*.cip`) file and cryptographically signs it using `signtool.exe`.
4. **EFI Deployment**: Temporarily mounts the system's hidden EFI partition and deploys the signed policy directly to the boot manager's `Active CiPolicies` directory.
5. **Refresh**: Invokes the local refresh utility to apply the policy immediately without a reboot.

Refer to the table below to know more about the task's exit code.

Table 12. Exit Codes Table

Exit Code	Meaning
0	Success
10	Directory setup failure
20	Certificate creation or export failure
30	XML processing or version bumping failure
40	Binary conversion failure
50	Signtool signing failure
60	EFI mount or deployment failure
70	Policy refresh tool failure
80	Thumbprint rotation failure

Figure 7. Task: Refresh Thumbprint of Deployed Policies Signers on Endpoint



1. In the BigFix Console, navigate to **All Content > BigFix Application Control > Fixlets and Tasks**.
2. From the **Fixlets and Tasks** pane, select **Task: Refresh Thumbprint of Deployed Policies Signers on Endpoint v2.0**.
3. From the **Task: Refresh Thumbprint of Deployed Policies Signers on Endpoint v2.0** pane, click the **Applicable Computers(n)** tab and view the endpoints on which you want to run the task.
4. Select the **Take Actions** tab and select the endpoints on which you want to apply this installer task.
5. Click **OK**.

Note: Once this task is triggered, it remains as an open action and runs on the system whenever the system becomes relevant. Only an administrator can stop this task.

A successful execution of this task results in the following outcomes:

- Local XML policies are updated with incremented version numbers and new signer rules.
- Cryptographically signed binary (*.cip) policies are successfully deployed to the EFI partition.
- System application control policies are immediately refreshed and enforced.

Enforcing Secure ACL on BAC Folder on Endpoint

Use this task to secure the BigFix Application Control (BAC) directory by enforcing strict access control and ownership settings.

The task performs the following actions:

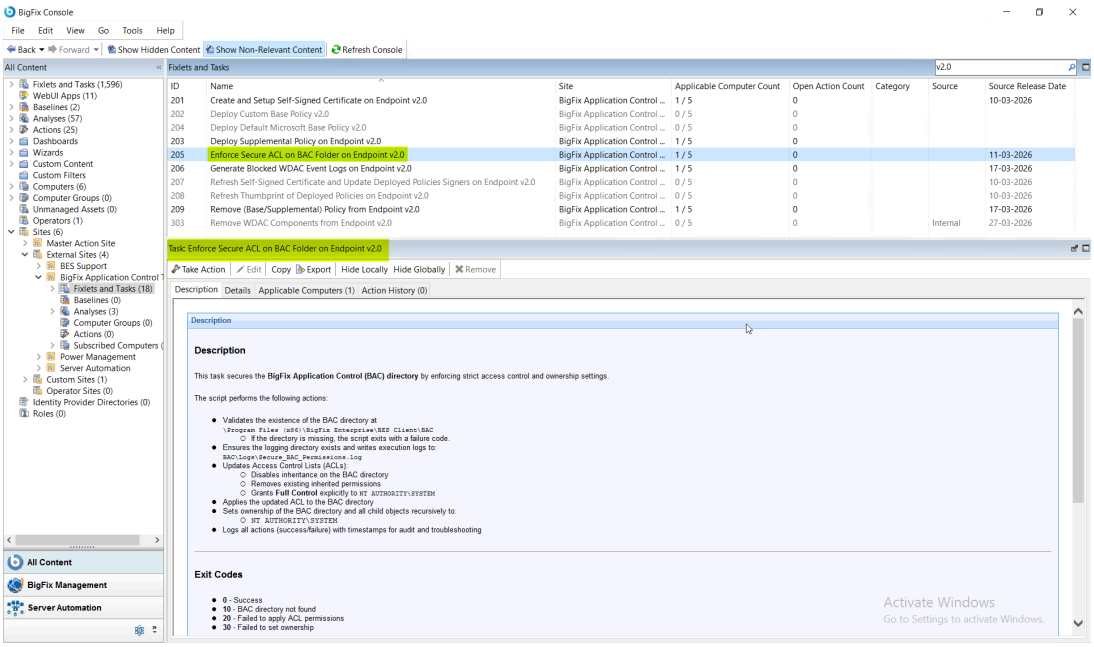
- Validates the existence of the BAC directory at the `\Program Files (x86)\BigFix Enterprise\BES Client\BAC` location. If the directory is missing, the task exits with a failure code.
- Ensures the logging directory exists and writes execution logs to the `BAC\Logs\Secure_BAC_Permissions.log` location.
- Updates Access Control Lists (ACLs):
    - Disables inheritance on the BAC directory.
    - Removes any existing inherited permissions.
    - Grants full control explicitly to `NT AUTHORITY\SYSTEM`.
- Applies the updated ACL to the BAC directory.
- Sets ownership of the BAC directory and all child objects recursively to `NT AUTHORITY\SYSTEM`.
- Logs all actions (success/failure) with timestamps for audit and troubleshooting.

Refer to the table below to know more about the task's exit code.

Table 13. Exit Codes Table

Exit Code	Meaning
0	Success
10	BAC directory not found
20	Failed to apply ACL permissions
30	Failed to set ownership

Figure 8. Task: Enforce Secure ACL on BAC Folder on Endpoint



1. In the BigFix Console, navigate to **All Content > BigFix Application Control > Fixlets and Tasks**.
2. From the **Fixlets and Tasks** pane, select **Task: Enforce Secure ACL on BAC Folder on Endpoint v2.0**.
3. From the **Task: Enforce Secure ACL on BAC Folder on Endpoint v2.0** pane, click the **Applicable Computers(n)** tab and view the endpoints on which you want to run the task.
4. Select the **Take Actions** tab and select the endpoints on which you want to apply this installer task.
5. Click **OK**.

> **Note:** Once this task is triggered, it remains as an open action and runs on the system whenever the system becomes relevant. Only an administrator can stop this task.

A successful execution of this task results in the following outcomes:

- The BAC directory is fully secured.
- Only the SYSTEM account has full control.
- Ownership is standardized across all files and sub folders.
- Unauthorized or inherited permissions are removed.

Generating Blocked WDAC Event Logs on Endpoint

Use this task to extract Windows Defender Application Control (WDAC) / App Control block events from the endpoint's event logs for both audit and enforced modes and generate a structured JSON report for analysis.

The task performs the following actions:

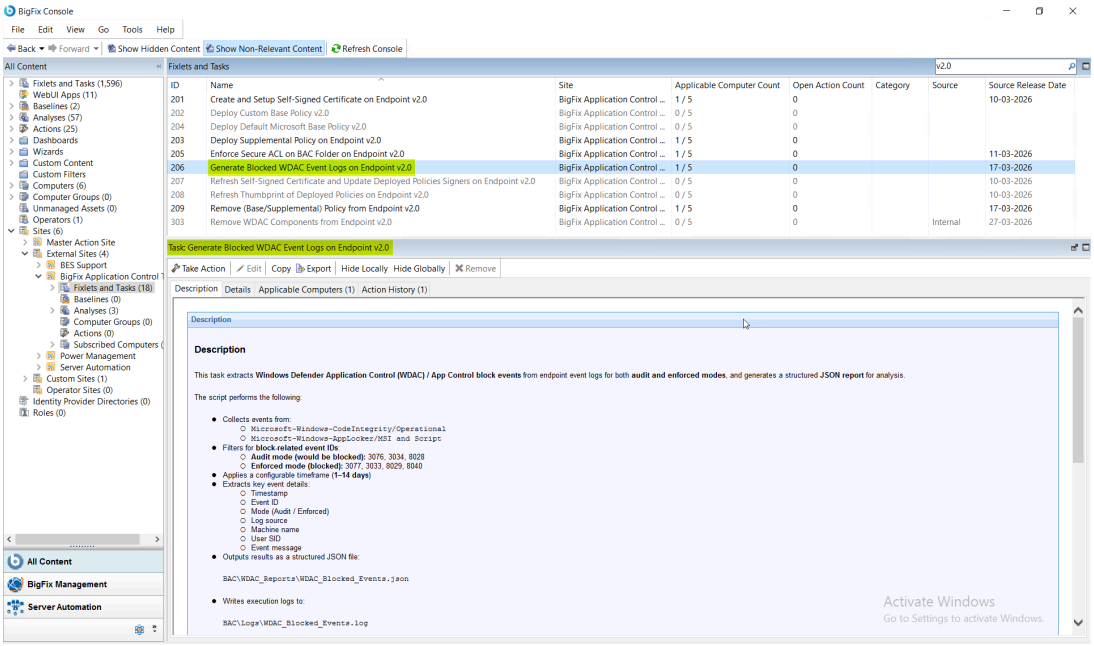
- Collects events from:
  - `Microsoft-Windows-CodeIntegrity/Operational`
  - `Microsoft-Windows-AppLocker/MSI and Script`
- Filters for block-related event IDs:
  - Audit mode (would be blocked): 3076, 3034, 8028
  - Enforced mode (blocked): 3077, 3033, 8029, 8040
- Applies a configurable time frame of 1 to 14 days.
- Extracts the following key event details:
  - Timestamp
  - Event ID
  - Mode (Audit / Enforced)
  - Log source
  - Machine name
  - User SID
  - Event message
- Outputs the results as a structured JSON file to `BAC\WDAC_Reports\WDAC_Blocked_Events.json` file.
- Writes the execution logs to the `BAC\Logs\WDAC_Blocked_Events.log` file.

Refer to the table below to know more about the task's exit code.

Table 14. Exit Codes Table

Exit Code	Meaning
0	Success
10	Invalid time frame
20	BAC path not found
30	Event query failure
40	No events found
50	Report generation failure

Figure 9. Task: Generate Blocked WDAC Event Logs on Endpoint



1. In the BigFix Console, navigate to **All Content > BigFix Application Control > Fixlets and Tasks**.
2. From the **Fixlets and Tasks** pane, select **Task: Generate Blocked WDAC Event Logs on Endpoint v2.0**.
3. From the **Task: Generate Blocked WDAC Event Logs on Endpoint v2.0** pane, under **Configuration Options**, enter the following information:

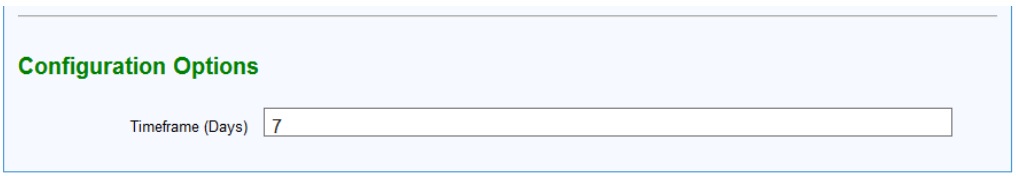


Table 15. Task: Generate Blocked WDAC Event Logs on Endpoint v2.0 Configuration Options

Field Name	Description
Timeframe (Days)	Number of days for which the event logs will be generated.

4. From the **Task: Generate Blocked WDAC Event Logs on Endpoint v2.0** 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**.

A successful execution of this task results in the following outcomes:

- WDAC block events, both audit and enforced are extracted.
- Clean, structured JSON report is generated in the BAC folder.
- Data ready for ingestion into dashboards, analysis, or for BigFix® reporting.

Removing (Base/Supplemental) Policy from Endpoint

Use this task to manage Windows Defender Application Control (WDAC) policies on the endpoint by supporting both supplemental policy removal and full base policy reset using a controlled and safe approach.

The task performs the following actions:

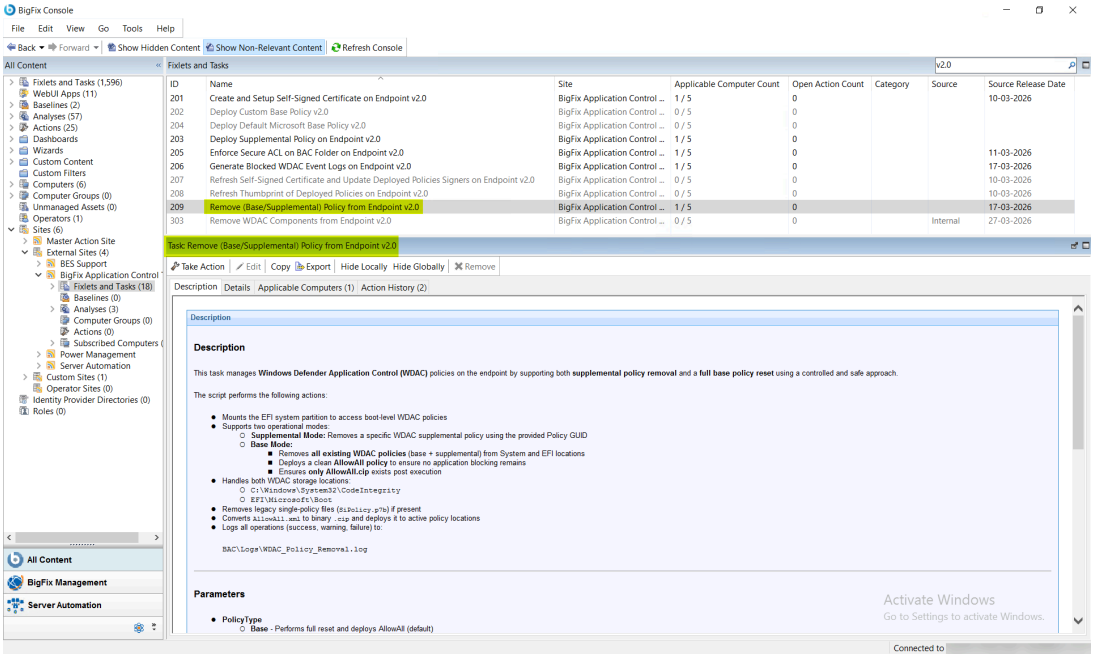
- Mounts the EFI system partition to access the boot-level WDAC policies.
- Supports the following two operational modes:
  - **Supplemental Mode**: Removes a specific WDAC supplemental policy using the provided Policy GUID.
  - **Base Mode**:
    - Removes all the existing WDAC policies (base as well as supplemental) from System and EFI locations.
    - Deploys a clean `AllowAll` policy to ensure no application blocking exists.
    - Ensures only `AllowAll.cip` exists post this task execution.
- Handles both the WDAC storage locations:
  - `C:\Windows\System32\CodeIntegrity`
  - `EFI\Microsoft\Boot`
- Removes legacy single-policy files (like `SiPolicy.p7b`) if present.
- Converts the `AllowAll.xml` to binary `*.cip` and deploys it to the active policy locations.
- Logs all the operations (success, warning, failure) in the `BAC\Logs\WDAC_Policy_Removal.log` file.

Refer to the table below to know more about the task's exit code.

Table 16. Exit Codes Table

Exit Code	Meaning
0	Success
10	Invalid input parameters
20	BAC path not found
30	EFI mount failure
40	Policy removal failure
50	AllowAll.xml not found
60	AllowAll deployment failure

Figure 10. Task: Remove (Base/Supplemental) Policy from Endpoint



1. In the BigFix Console, navigate to **All Content > BigFix Application Control > Fixlets and Tasks**.
2. From the **Fixlets and Tasks** pane, select **Task: Remove (Base/Supplemental) Policy from Endpoint v2.0**.
3. From the **Task: Remove (Base/Supplemental) Policy from Endpoint v2.0** pane, under **Configuration Options**, enter the following information:

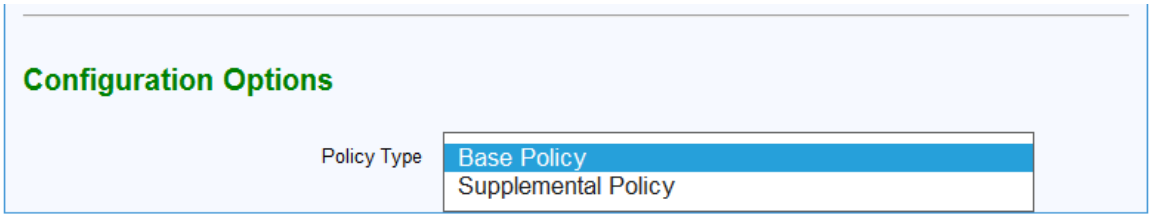


Table 17. Task: Remove (Base/Supplemental) Policy from Endpoint v2.0 Configuration Options

Field Name	Options	Description
Policy Type	Base	Performs full reset and deploys AllowAll (default).
	Supplemental	Removes only a specific supplemental policy.
PolicyId		Required only when the policy type is Supplemental. Specifies the GUID of the policy to be removed.

4. From the **Task: Remove (Base/Supplemental) Policy from Endpoint v2.0** 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**.

A successful execution of this task results in the following outcomes:

- In Supplemental mode, only the specified policy is removed.
- In Base mode, all WDAC policies are removed and replaced with AllowAll.
- System remains stable with a valid WDAC configuration.
- A system reboot is required for changes to take effect.

Removing WDAC Components from Endpoint

Use this task to remove all the associated files and folders related to Windows Defender Application Control (WDAC) from an endpoint.

The task performs the following actions:

- Mounts the EFI system partition to access the boot-level WDAC policies.
- Removes the AllowAll base policy from the endpoint (EFI).
- Uninstalls the SDK, including SignTool.exe.
- Deletes the BAC folder from the endpoint.
- Logs all operations (success, warning, failure) to the `BAC\Logs\WDAC_Cleanup.log` file.

Refer to the table below to know more about the task's exit code.

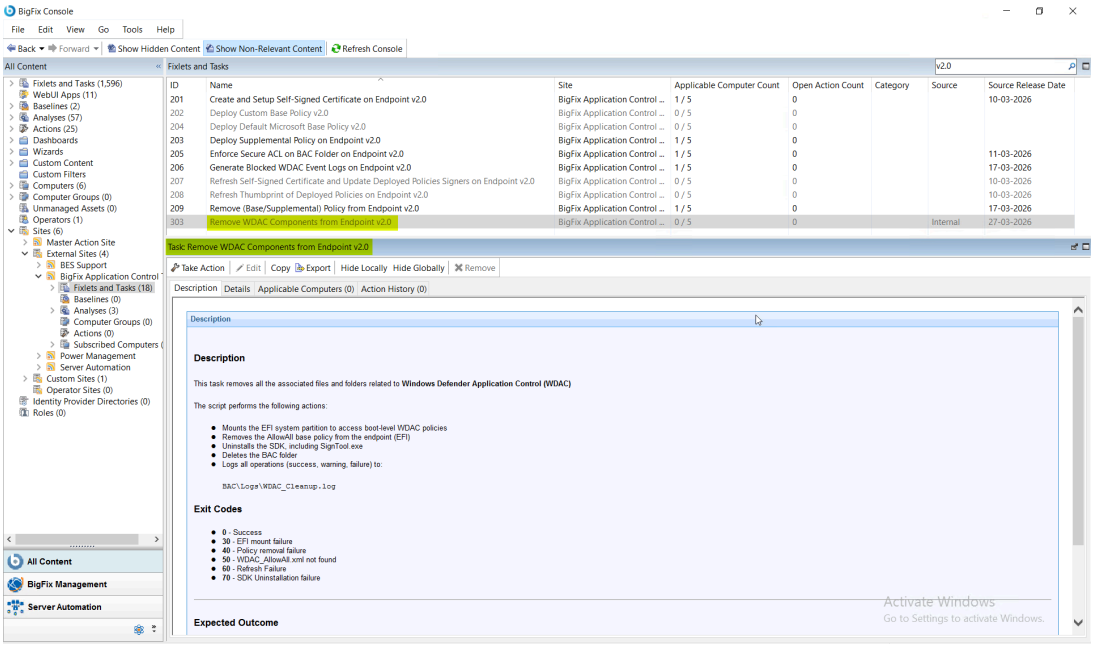
Table 18. Exit Codes Table

Exit Code	Meaning
0	Success

Table 18. Exit Codes Table (continued)

Exit Code	Meaning
30	EFI mount failure
40	Policy removal failure
50	WDAC_AllowAll.xml file not found.
60	Refresh failure
70	SDK un-installation failure

Figure 11. Task: Remove WDAC Components from Endpoint



1. In the BigFix Console, navigate to **All Content > BigFix Application Control > Fixlets and Tasks**.
2. From the **Fixlets and Tasks** pane, select **Task: Remove WDAC Components from Endpoint v2.0**.
3. From the **Task: Remove WDAC Components from Endpoint v2.0** pane, click the **Applicable Computers(n)** tab and view the endpoints on which you want to run the task.
4. Select the **Take Actions** tab and select the endpoints on which you want to apply this installer task.
5. Click **OK**.

A successful execution of this task results in the following outcomes:

- Removes all the associated Application Control files and folders from the endpoint.
- A system reboot is required for the changes to take effect.

Viewing Endpoint Details using BigFix® Web Reports

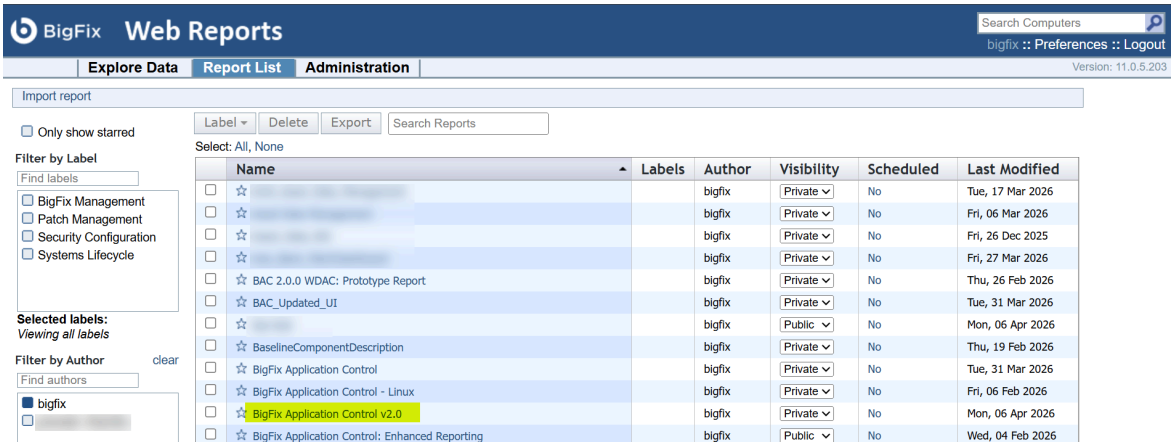
As an administrator, you can utilize BigFix Web Reports to view a comprehensive, read-only overview of all enterprise endpoints with the application installed. This topic outlines the steps to access and navigate the various tabs that display managed devices, blocklisted applications, allowlisted applications,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

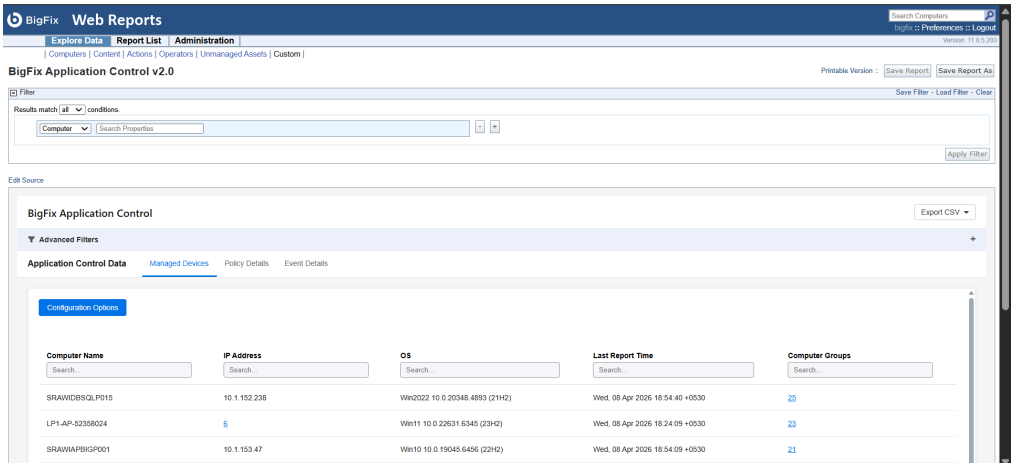
Follow the steps below to view details from BigFix Web Reports:

1. Login to **BigFix Web Reports**.
2. On the **Web Reports** home page, select the **Report List** tab and click **BigFix Application Control v2.0**.



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

Figure 12. 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.

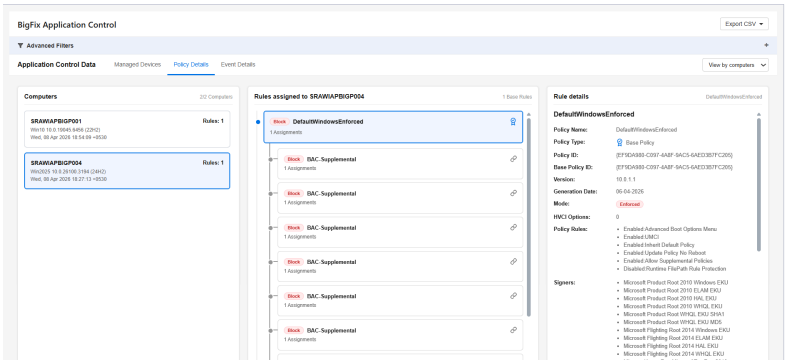
- **Export CSV**

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

b. **Policy Details**

This tab will display the list of managed devices with rules assigned to them. Select an endpoint or device name from the **Computers** column and the **Rules assigned to <device_name>** column will display all the rules assigned to the endpoint. Selecting a specific rule from it will populate the **Rule details** column.

Figure 13. Policy Details screen

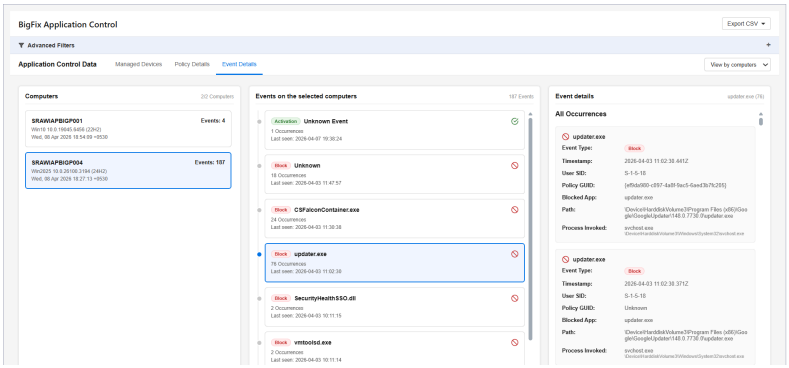


c. **Event Details**

This tab will display the list managed devices with all the events executed on them. Select an endpoint or device name from the **Computers** column and the **Events on the**

selected computers column will list all the events of the endpoint. Selecting a specific event from it will populate the **Event details** column.

Figure 14. Event Details screen



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.