

**BigFix Compliance
Configuration Management
(SCM) for Console User Guide**



Special notice

Before using this information and the product it supports, read the information in [Notices \(on page 107\)](#).

Edition notice

This edition applies to BigFix version 11 and to all subsequent releases and modifications until otherwise indicated in new editions.

Contents

Chapter 1. Setting up Configuration Management.....	7
System requirements	8
Standards.....	8
Chapter 2. Using checks and checklists.....	10
Check Fixlets.....	10
Modifying check parameters.....	13
Activating Measured Value Analyses.....	13
Creating and Managing Custom Checklists.....	14
Creating custom checklists.....	14
Customizing content.....	15
Using the Synchronize Custom Checks wizard.....	16
Scanning for out-of-date checks.....	16
Synchronizing out-of-date checks.....	17
Preserving custom remediation actions.....	17
Taking a remediation action.....	18
Chapter 3. Configuring Windows and Web Browser Checklist.....	19
Overview.....	19
What's new in Windows checklist.....	19
Available Windows and Web Browser checklist.....	20
Setup and configuration.....	21
Windows and Web browser Checklist Components.....	23
Deploy and Run task.....	23
Applicability Fixlets.....	27
Remediation.....	28
Measured Value Analysis.....	30
Using checks and checklists.....	31
Viewing check Fixlets from the HCL BigFix console.....	31
Chapter 4. Configuring Linux checklists.....	33
Overview.....	33
What's new in Linux checklist.....	33

Available Linux checklist.....	34
Setup and configuration.....	34
Checklist components.....	37
Deploy and Run task.....	39
Applicability Fixlets.....	45
Remediation.....	46
Measured Value Analysis.....	48
Using checks and checklists.....	49
Viewing check Fixlets from the HCL BigFix console.....	50
Chapter 5. Configuring Middleware Checklists.....	51
Overview.....	51
What's new in Middleware checklist.....	51
Available Middleware checklist.....	51
Setup and configuration.....	52
Middleware checklist components.....	54
Environment Setup Task.....	54
Applicability Fixlets.....	61
Remediation.....	63
Measured Value Analysis.....	66
Using checks and checklists.....	67
Viewing check Fixlets from the HCL BigFix console.....	67
Chapter 6. Configuring Unix checklists.....	69
Overview.....	69
What's new in Unix checklist.....	69
Available Unix checklist.....	69
Setup and configuration.....	70
Unix checklist components.....	72
Environment Setup Task.....	72
Applicability Fixlets.....	76
Remediation.....	78
Measured Value Analysis.....	80
Using checks and checklists.....	81

Viewing check Fixlets from the HCL BigFix console.....	82
Chapter 7. Importing SCAP content.....	83
Learning about SCAP.....	83
SCAP Checklists.....	86
Using the Import SCAP Content wizard.....	86
Using the Import SCAP 1.3 Content wizard.....	88
Using the Create SCAP Compatible Report wizard.....	95
Using the Create SCAP 1.3 Compatible Report wizard.....	97
Using OVALDI.....	102
Chapter 8. Configuration Management Reporting.....	103
Chapter 9. Frequently asked questions.....	104
Chapter 10. Support.....	106
Chapter 11. Notices.....	107

Chapter 1. Setting up Configuration Management

Follow these steps to set up your Configuration Management deployment.

Follow these steps to set up Configuration Management

1. Plan your Configuration Management deployment.
2. Subscribe to the external SCM sites.
3. Create custom sites or custom checklists.

Planning your Configuration Management deployment

Keep in mind the following steps as you plan your configuration management deployment.

1. Identify which computers will run the Configuration Management content.
2. Group the computers by operating system.
3. Create subgroups within each operating system that must comply with the different standards.

Subscribing to sites

Each Configuration Management checklist is provided as a single site and represents a single standard and platform. The content is continuously updated and automatically delivered when added to an BigFix deployment. Computers must be subscribed to the site to collect data from BigFix clients. This data is used for reporting and analysis.

The process of site subscription depends on the version of the BigFix console that you installed. For more information, see the [BigFix Configuration Guide](#).

Alternatively, an air-gap can be used to physically separate the BigFix server from the Internet Fixlet server. For more information, see [Installing in an Air-Gapped Network](#).

The Fixlets in this site can be used as-is or customized to meet your own security policies. Compliance calculations are evaluated locally on each endpoint, and the Configuration Management solution is scalable and can accommodate large numbers of computers.

You can choose to copy Configuration Management content to custom sites so you can customize the content.

Creating custom sites

As each Configuration Management checklist is provided as a single site, when you create a custom site, you are in effect, creating a custom checklist.

Use custom checklists to fine-tune the settings that are monitored in your deployment. You can customize Configuration Management parameters and exclude specific computers from an analysis. Custom checklists target specific sets of computers with tailored content with the use of the subscription mechanism.

Creating custom checklists involves the following steps

1. Create a custom checklist from an existing external checklist.
2. Customize Fixlets using built-in parameterization.
3. Subscribe the correct computers to the custom checklist.

You can use the Create Custom Checklist wizard to create new custom checklists that are based on your currently subscribed external checklists. For more information, see [Creating custom checklists \(on page 14\)](#).

System requirements

Set up your deployment according to the system requirements to successfully deploy Configuration Management.

Table 1. Supported components and system requirements to deploy Configuration Management

Components	Requirements
Supported browser versions	Internet Explorer 7.0 or later
HCL BigFix component versions	<ul style="list-style-type: none"> • Console 8.0 or later • Windows Client 8.0 • UNIX Client: <ul style="list-style-type: none"> ◦ Superseded version: HCL BigFix UNIX Client 7.2 ◦ Non-superseded version: HCL BigFix UNIX Client version 8.1.551.0

Standards

Security Configuration Management bases its checklist on various authority standards.

Center for Internet Security

The Center for Internet Security (CIS) guidelines recommends technical control rules and values that are applicable to network devices, operating systems, software applications, and middleware applications. CIS guidelines are consensus-based and are used by the US government and businesses in various industries.

The CIS guidelines are distributed for free in PDF formats and are also available in Extensible Configuration Checklist Description Format (XCCDF) for CIS Security Benchmark members. XCCDF is an XML-based language that is used for benchmark assessment tools and custom scripts.

For more information about CIS, see <https://www.cisecurity.org/>.

Defense Information System Agency Security Technical Implementation Guidelines

The Defense Information Systems Agency (DISA) releases the Security Technical Implementation Guidelines (STIG). STIG provides recommendations for secure installation, configuration, and

maintenance of software, hardware, and information systems. STIG is one of the basis of configuration standards that the US Department of Defense uses.

For more information about DISA and STIG, see <http://www.disa.mil/>.

Federal Desktop Core Configuration

The Federal Desktop Core Configuration (FDCC) is a set of security settings that were recommended by the National Institute of Standards and Technology (NIST). FDCC was replaced by the United States Government Configuration Baseline (USGCB).

Payment Card Industry Data Security Standard

The Payment Card Industry Data Security Standard (PCI DSS) is a baseline of technical and organizational requirements that are related to the Payment Card Industry.

You must establish a secure payments environment throughout your organization to achieve PCI DSS compliance. SCM enforces security configurations for endpoints and servers in your organization, and can help your organization protect endpoints meet security compliance for PCI DSS.

By complying with the PCI DSS standards you ensure that cardholder data and sensitive authentication data are secure and well protected from malicious users and attacks. The PCI DSS applies to all entities involved in payment card processing and requires continuous compliance with the security standards and best practices set by the PCI Security Standards Council.

For more information about PCI DSS, see the PCI Security Standards Council website at www.pcisecuritystandards.org/security_standards/ and the [Payment Card Industry Data Security Standard \(PCI DSS\) User's Guide](#).

United States Government Configuration Baseline

The United States Government Configuration Baseline (USGCB) provides guidance for security configuration of Information Technology products that are deployed by US government federal agencies. USGCB addresses the following platforms Microsoft's Windows 7, Windows 7 Firewall, Windows Vista, Windows Vista Firewall, Windows XP, Windows XP Firewall, Internet Explorer 7, Internet Explorer 8, and Red Hat Enterprise Linux 5.

USGCB replaced the Federal Desktop Core Configuration (FDCC).

For more information about USGCB, see <http://usgcb.nist.gov/>.

Chapter 2. Using checks and checklists

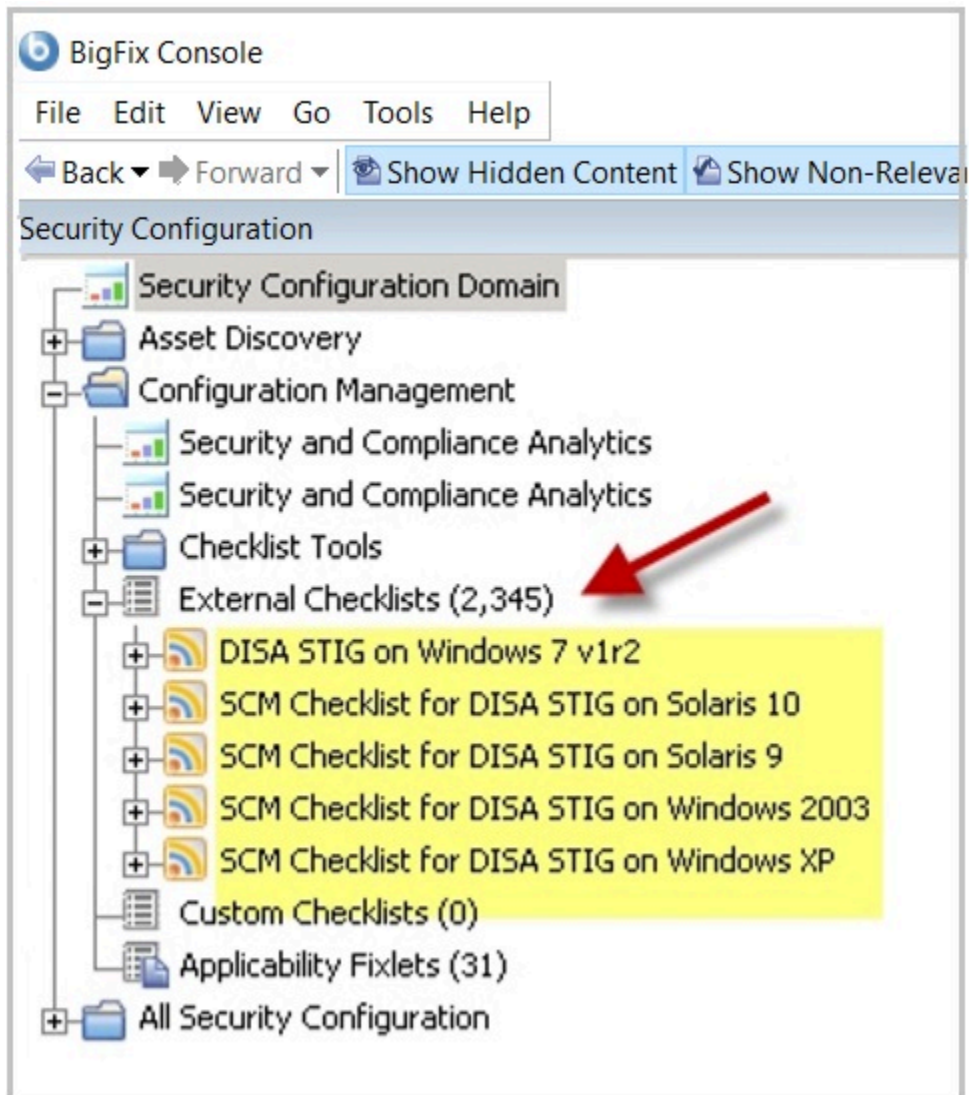
Check Fixlets in Configuration Management checklists assess an endpoint against a configuration standard. Many check Fixlets have a corresponding analysis, sometimes referred to as *measured values*, which report the value of the element that the check Fixlet evaluates.

Check Fixlets

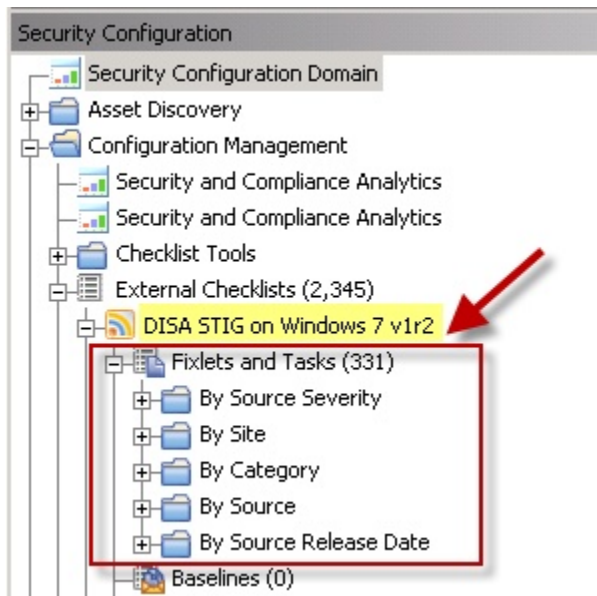
A check Fixlet becomes relevant when a client computer is out of compliance with a configuration standard. By viewing the Configuration Management Fixlets, you can identify non-compliant computers and the corresponding standards.

To start using the Configuration Management checklists, obtain a masthead for the appropriate Configuration Management site and open it within the BigFix console. When the site has been gathered in the console, follow the steps below to view the checks:

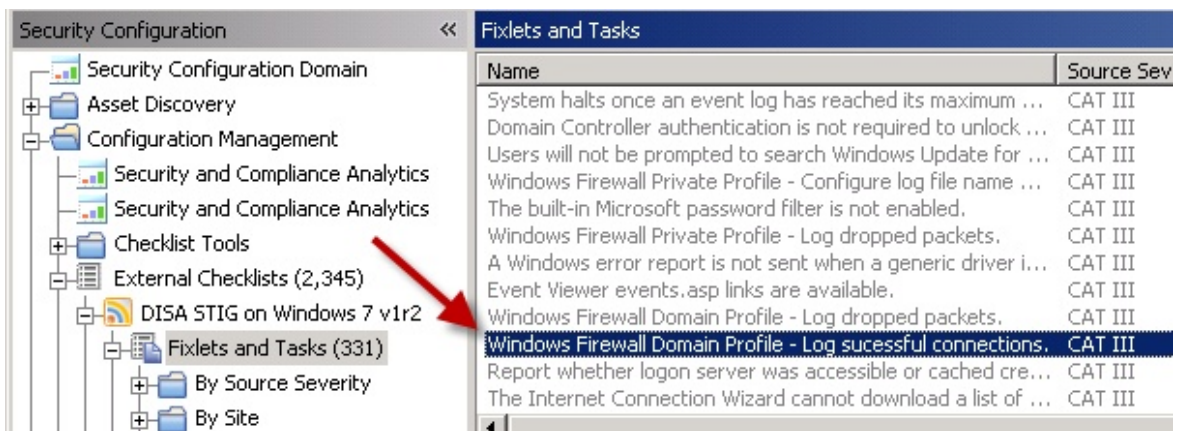
1. Select a Configuration Management checklist from the navigation tree.



2. Expand a checklist and click *Fixlets and Tasks*.



3. Click one of the Fixlets displayed in the list. The Fixlet opens with the following tabs: *Description*, *Details*, *Applicable Computers*, and *Action History*. Click the *Description* tab to view the text describing this Fixlet.



The Fixlet window typically contains a description of the check, options to customize the configuration setting, and a related Action to remediate one or more systems to the expected configuration value.

Fixlet: Windows Firewall Domain Profile - Log successful connections.

Take Action Edit Copy Export Hide Locally Hide Globally Remove

Description Details Applicable Computers (0) Action History (0)

Description

Windows Firewall Domain Profile - Log successful connections.

This check enables logging of successful connections for a domain connection.

Source ID 5.462	Source Severity CAT III	DISA Group Title Windows FW Domain - Log Successful Connections	DISA IA Controls ECSC-1
DISA Rule ID SV-25229r1_rule	DISA Responsibility System Administrator	DISA Valid (STIG-ID) V-17427	DISA Documentable Not available

DISA Check Content
If the following registry value does not exist or is not configured as specified, then this is a finding:

The Fixlet is applicable to a subset of endpoints on your network. The size of that subset is shown in the Applicable Computers tab.

Fixlet: Windows Firewall Domain Profile - Log successful connections.

Take Action Edit Copy Export Hide Locally Hide Globally Remove

Description Details Applicable Computers (0) Action History (0)



Note: UNIX controls provide custom parameterization, but through a different mechanism.

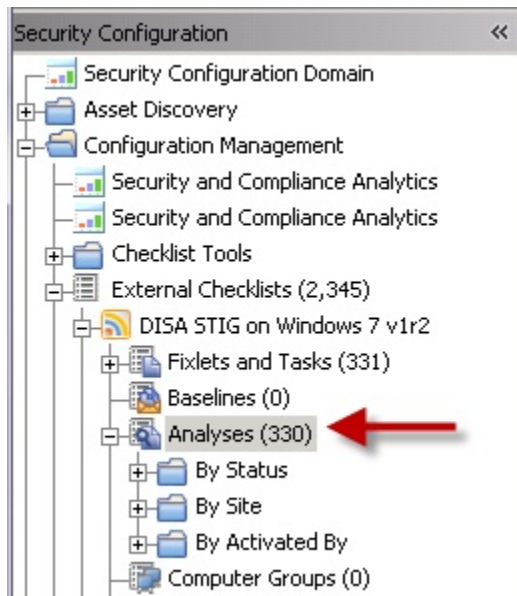
Modifying check parameters

In addition to monitoring compliance status and remediating settings that are out of compliance, you can also modify the parameters used in determining the compliance of the checks. For example, you can set the minimum password length on an endpoint to 14 characters. You can customize the password-length parameter to your specific policy.

Activating Measured Value Analyses

Click the Analyses subnode within a checklist to find measured value analyses.

In addition to check Fixlets, some checklists include analyses that provide the actual values of the items being checked. Measured values are retrieved using analysis properties. You can find measured value analyses by clicking the Analyses subnode within any checklist.



Note: For best performance, only activate the analyses that you need for your deployment. Only activated analyses are visible in SCA.

Creating and Managing Custom Checklists

The ability to customize Configuration Management parameters and exclude specific computers from an analysis gives you control over your security status. However, you can also use custom checklists to fine-tune the settings monitored in your deployment. Custom checklists target specific sets of computers with tailored content using the subscription mechanism. This allows statistics to be gathered with finer granularity. To create your own checklist with custom sites, perform the following steps.

- Step 1: Create a custom checklist from an existing external checklist
- Step 2: Customize Fixlets using built-in parameterization
- Step 3: Subscribe the proper computers to the custom checklist

Creating custom checklists

Use this wizard to create custom checklists.

You must be subscribed to the SCM Reporting external site.

1. From the **Security Configuration Domain**, go to **Configuration Management > Checklist Tools > Create Custom Checklist**.

Create Custom Checklist

This wizard will assist you in creating a new custom checklist based on one or more of your currently subscribed external checklists.

New checklist name: 9 characters remaining

(2 checks selected out of 326 displayed)

Select target platform: ☐ AIX 5.3 ☐ AIX 6.1 ☐ Red Hat 3 ☐ Red Hat 4 ☐ Red Hat 5 ☐ Red Hat 6

External checklist to copy checks from:

<input type="checkbox"/>	Check Name	Source ID	Source Severity	Source Checklist
<input type="checkbox"/>	/profile PATH - AIX 5.3-6.1	CIS-1.7.1	Level-1	CIS Checklist for AIX 5.3 and 6.1
<input checked="" type="checkbox"/>	/audit - group owner - AIX 5.3-6.1	CIS-2.11.5.2	Level-1	CIS Checklist for AIX 5.3 and 6.1
<input checked="" type="checkbox"/>	/audit - owner - AIX 5.3-6.1	CIS-2.11.5.1	Level-1	CIS Checklist for AIX 5.3 and 6.1
<input type="checkbox"/>	/audit - permissions - AIX 5.3-6.1	CIS-2.11.5.3	Level-1	CIS Checklist for AIX 5.3 and 6.1
<input type="checkbox"/>	/etc/environment PATH - AIX 5.3-6.1	CIS-1.7.2	Level-1	CIS Checklist for AIX 5.3 and 6.1

Staged List: The following checks will be copied to your new checklist (including any necessary measured value analyses and/or applicability fixlets):

<input checked="" type="checkbox"/>	Check Name	Source ID	Source Severity	Source Checklist
<input checked="" type="checkbox"/>	/audit - group owner - AIX 5.3-6.1	CIS-2.11.5.2	Level-1	CIS Checklist for AIX 5.3 and 6.1
<input checked="" type="checkbox"/>	/audit - owner - AIX 5.3-6.1	CIS-2.11.5.1	Level-1	CIS Checklist for AIX 5.3 and 6.1

2 total checks will be copied to the new checklist

2. Enter the name of the new checklist.
3. Select the target platform.
4. Click the drop-down menu to select which external checklist you copy the checks from. As you select the checks, they are shown in the staged list at the lower part of the window.
5. Optional: Click the **Activate Measured Value analyses after copying** check box to activate all analyses that were copied.
6. Click **Create Checklist**.

The console begins copying the checks in the selected lists into your new custom checklist. The process might take several minutes, depending on the number and size of the checklists selected.



Note: Use care when you subscribe computers to custom checklists. Custom checklists do not support site relevance, which protects you from bad subscriptions.

Customizing content

Now that you have a custom checklist populated with content copied from external checklists, you can configure your checklist by any of the following means:

- Configure check parameters to control remediation
- Delete unwanted or unnecessary checks



Note: In Console versions 8.0 and later, subscribing computers to a custom checklist site is handled in the same way as with External checklist subscriptions.

Using the Synchronize Custom Checks wizard

Use the SCM Synchronize Custom Checks wizard to update any custom checks in your deployment whose external sources have since been updated by HCL. You can use any additional functionality or bug fixes that may have been provided by HCL (in the form of external site updates) since the custom copies were made.

To synchronize a custom checklist, you must have the latest version of the Create Custom Checklist wizard (SCM Reporting version 36 or later). The latest version of the wizard adds required metadata to the copied checks that allows the sync wizard to determine whether the current external source has been modified since the copy was made.

- First time SCM user

If your Endpoint Manager deployment does not have any custom checklists that were created prior to the release of the sync wizard, any custom checklists you create from now on will be compatible with the Synchronize Custom Checks wizard.

- Existing SCM user and you used the previous version of the Create Custom Checklist wizard

If you already have one or more custom checklists created with an older version of the Create Custom Checklist wizard, you will have to first recreate these and any other custom checklists that you wish to have synchronizing abilities using the latest version of the Create Custom Checklist wizard.



Note: SCM user should have **Can Submit Queries** permission and **Can use REST API** privilege set to **Yes** to trigger the sync wizard operation.

Scanning for out-of-date checks

You can make basic global scans or detailed targeted scans for out-of-date checks.

The custom checklist that you will synchronize must be created with the latest version of the Create Custom Checklist wizard (SCM Reporting version 36 or later).

This wizard scans all SCM custom checklists for external updates, and displays the checklists that need an update or synchronization in the table. Please note that this scan will not detect checks that have been added to or removed from an external site.

The detailed targeted scan requires the user to select a source checklist (external) and a destination checklist (custom) before performing the scan. This scan does a limited scan that performs a comparison of the source and destination checklists to determine whether or not there are any: out of date custom checks, newly added external checks, or recently removed external checks.

This scan is designed for use only in cases where the user intends to maintain an up-to-date copy of an entire external checklist. If the destination was not originally created as a copy of the source, the results of this scan may be confusing and/or misleading; however, there are no hard restrictions to this end, and the user may perform a detailed targeted scan comparison between any external and custom checklist pair.

1. Select the appropriate tab.
 - Basic Global Scan
 - Detailed Targeted Scan
 - a. Select the source from the external checklists.
 - b. Select the destination of the custom checklist.
 - c. Option: Click the **Only show** drop-down menu to select from the filter choices.
2. Click **Scan** to scan for out-of-sync checks.

Synchronizing out-of-date checks

Custom parameterizations will be automatically preserved.

1. From the Out of Sync Checks window, select the checkboxes in the left-most column.
2. Click **Synchronize** in upper left corner. A progress indicator box displays the percentage complete and an estimated remaining time to complete the synchronization operation. You can also cancel the operation at any time from this window.



Note: The synchronization process can take a number of seconds per check. Keep in mind when synchronizing large sets of checks at a time.

Preserving custom remediation actions

Follow these steps to preserve manually edited remediation action scripts for checks in your custom checklists.

Normally, synchronizing a custom check overwrites the existing remediation action, if there are any, with the latest from the external source. However, if you manually edited the remediation action script for checks in your custom checklists, you can preserve this custom action after synchronizing.

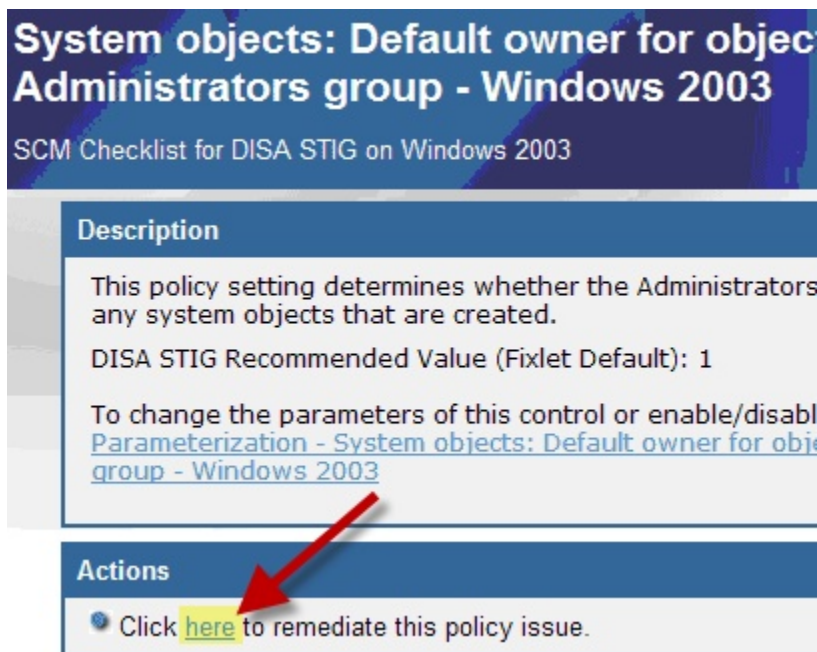


Note: Preserving a custom action in this way prohibits this check from receiving updates and bug fixes to the remediation action portion of the check. This option is only suggested for cases in which the user is sure that the action of the source check is either missing or incorrect, or if your security policy calls for remediating the check in a custom manner.

1. From the **Synchronize Custom Checks** wizard, click the name of the custom check. The corresponding Fixlet opens.
2. Click **Edit** at the upper part of the Fixlet window. In the window that opens, click the **Actions** tab.
3. Select the wanted action in the first list. In most cases, there is only one.
4. Add `// SCMSyncManager: NO_SYNC` to the first line of the **Action Script** text box.

Taking a remediation action

Many Fixlet controls have built-in Actions to remediate an issue. To start the remediation process, click the link in the Actions box.



The Take Action dialog opens, where you can target the computers that you want to remediate. For more information about the Take Action dialog, see the [BigFix Console Operator's Guide](#).

A remediation action typically sets a value in a file or in the Windows registry. Most UNIX remediations run the `runme.sh` file for the appropriate check. This action applies the recommended value shipped with the product or the customized parameter you set according to your own corporate policy.

After you have targeted a set of endpoints, click **OK** and enter your Private Key Password to send the action to the appropriate endpoints. While the actions are run on the endpoints and the setting is remediated, you can watch the progress of the actions in the console.

When every endpoint in a deployment is brought into compliance, the check Fixlet is no longer relevant and is removed from the list of relevant Fixlets. Although the Fixlets are no longer listed, they continue checking for computers that deviate from the specified level of compliance. To view them, click the "Show Non-Relevant Content" tab at the top of the console window.

Chapter 3. Configuring Windows and Web Browser Checklist

The Configuration Management checklists for the Windows™ and Web Browser systems are delivered as a set of Fixlets and tasks that can help you find the information you need to manage your deployment.

A checklist for configuring the Windows™ and Web Browser settings and web browsers to ensure optimal performance, security, and compatibility with applications.

Overview

You can configure the Windows™ and the Web Browser checklists for the Windows™ operating system and web browsers.

The Windows™ and Web Browser checklists in BigFix effectively meet the requirements outlined in the CIS and DISA checklists, with a strong emphasis on compliance monitoring.

Many Windows™ and the Web Browser checks include built-in remediation. However, a smaller portion of some Windows™ and the Web Browser checks allow auditing of non-default values. If customization is available for a specific check, input fields will be present on the **Description tab** of the Fixlet®. You can simply modify the relevant field to the desired audit value and click the **Apply** button.

What's new in Windows checklist

HCL BigFix Compliance Windows™ and the Web Browser checklist provide additional support and enhancements in the recent update.

Several checks have been improved by adding a **pending restart** feature. This feature operates as follows:

- For checks that require an OS reboot, the action results will now display "Pending Restart" instead of "Fixed."

Figure 1. Pending start

Baseline Component Applicability		Action History (1)	User Management Rights (1)	Role Management Rights (0)
State	Status	Name		Site
Open	Pending Restart	Simple TCP/IP Services must not be installed on the sy...		DISA STIG Checklis...

- The check will remain relevant for those endpoints until they are rebooted.
- After the endpoint is rebooted, the action results will display as "Fixed," and the check will be marked as compliant.

For a detailed list of releases, see the [Windows and Web Browser Checklist Release Notes](#).

Universal Checklist

The Universal Checklist for Windows Server is a single, unified checklist designed to simplify compliance management for all supported Windows Server versions (2016, 2019, 2022, and 2025). This beta release integrates

all security checks from the CIS and DISA benchmarks, allowing you to apply consistent security configurations across your entire server environment with one action.

What's Changing

- **A Single Checklist Model:** You will now manage and deploy one checklist for the entire Windows Server platform, rather than one for each OS version and benchmark.

What Stays the Same

- **Custom Checklist Creation:** Your workflow for creating custom checklists is not changing. You can still use the **Create Custom Checklist** wizard with the content from this new Universal Checklist.
- **Parameterization:** The ability to parameterize checks, where applicable, remains unchanged from the existing process.
- **Checklist-Level Reporting:** For this beta phase, you will find the compliance score for the Universal Checklist in the same location as your other checklists: **SCA > Reports > Checklists** section. Or you can access the same data by running the existing compliance reports in Web Reports (https://<bigfix_server_name>:8083/webreports).



Important: It is important to note that this report shows the overall compliance for the general-purpose Universal Checklist itself and is not a substitute for a benchmark-specific (e.g., CIS or DISA) report.

- **Availability of Individual CIS/DISA Checklists:** This Universal Checklist is for general purpose use. To generate specific CIS or DISA compliance reports, you must continue to use the individual CIS and DISA checklists, which will still be delivered through the existing method.

Available Windows and Web Browser checklist

The Windows™ and Web Browser checklists are commonly used to ensure systems are secure, optimized, and compliant with best practices.

Below are the Windows™ and Web Browser checklists available in the License dashboard:

Table 2. Windows and Web Browser checklists

CIS Checklists	DISA STIG Checklists	Universal Checklists
Windows	Windows	Windows Server
Web Browser	Web Browser	

To get more details of Windows and Web Browser checklists, refer to the [Windows and Web Browser Checklist](#).

Setup and configuration

Create custom copies of the Windows™ and Web browser checklist content if you want to modify the checks based on a specific corporate policy. Use the Create Custom Checklist wizard to create copies of the Windows™ and Web browser checklists and save them in a custom site.

You must subscribe to the SCM Reporting external site.

You can use custom checklists to fine-tune your ability to customize Configuration Management parameters, which gives you control over your security status. Custom checklists target specific sets of computers with tailored content using the subscription mechanism. This allows statistics to be gathered with finer granularity. For more information, see [Modifying check parameters \(on page 29\)](#).

Setting up your Configuration Management checklist for Windows™ and Web browser checklist involves two basic steps:

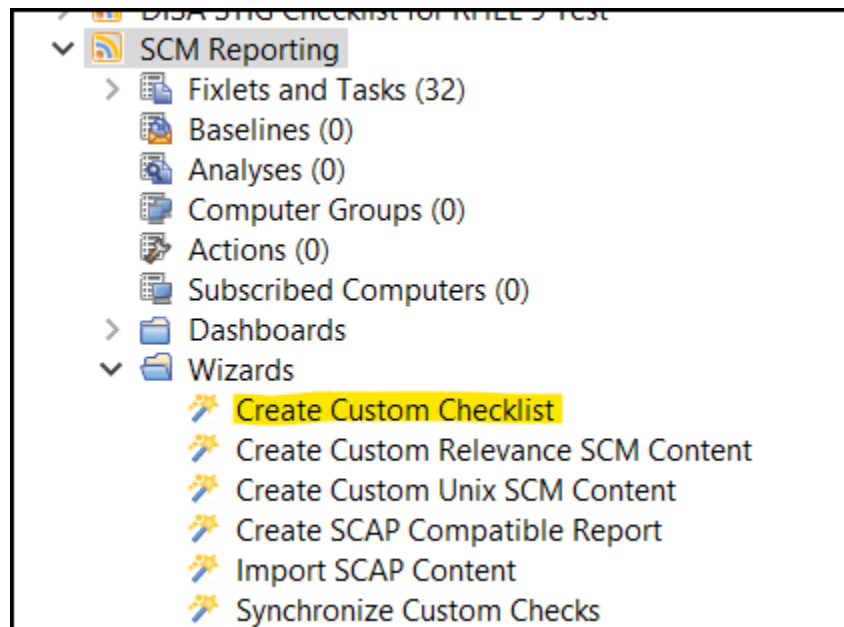
Creating your checklist:

- Creating custom checklists by using the Create Custom Checklist wizard:
 1. From the Security Configuration Domain, go to **Configuration Management > Checklist Tools > Create Custom Checklist**.
 2. Enter the name of the new checklist.
 3. Select the target platform.
 4. Click the drop-down menu to select which external checklist you copy the checks from. As you select the checks, they are shown in the staged list at the lower part of the window.
 5. Click the **Activate Measured Value analyses after copying** check box to activate all analyses that were copied.
 6. Click **Create Checklist**.

The console begins copying the checks in the selected lists into your new custom checklist. The process might take several minutes, depending on the number and size of the checklists selected.

Use the **Create Custom Checklist** wizard located in the **SCM Reporting** site under the wizard section.

Figure 2. Create custom checklist



- Creating custom checklists manually:

1. Select **Tools > Create Custom Site**.
2. You are prompted for a name for your custom site. Enter a name and click **OK**.
3. From the Domain panel, find your site under **Sites > Custom** and click it to describe your site.
From the **Details** tab, enter a description of your site. From the **Domain** pull-down menu, select a Domain to house your site.
4. From the **Computer Subscriptions** tab, indicate which subset of your BigFix client computers you want to subscribe to this site.
5. From the **Operator Permissions** tab, you can grant specific access permissions to specific operators.
6. Click the **Save Changes** button above the work area to complete the description of your site. You must enter your password to propagate your new custom site.

Subscribe computers to the custom checklist.



Note: Custom checklists do not support site relevance, so take extra precaution when you subscribe computers to custom checklists.

Figure 3. Create custom checklist

Create Custom Checklist

This wizard will assist you in creating a new custom checklist based on one or more of your currently subscribed external checklists.

New checklist name: DISA_Win 202219 characters remaining

(212 checks selected out of 212 displayed)

External checklist to copy checks from: DISA STIG Checklist for Windows 2022

Search

<input checked="" type="checkbox"/>	Check Name	Source ID	Source Severity	Source Checklist
<input checked="" type="checkbox"/>	Windows Server 2022 Application Compatibility P...	No CCEs provided	low	DISA STIG Checklist for Windows 2022
<input checked="" type="checkbox"/>	Windows Server 2022 must be configured to en...	No CCEs provided	medium	DISA STIG Checklist for Windows 2022
<input checked="" type="checkbox"/>	Windows Server 2022 must be configured to au...	No CCEs provided	medium	DISA STIG Checklist for Windows 2022
<input checked="" type="checkbox"/>	Windows Server 2022 must not have the TFTP C...	No CCEs provided	medium	DISA STIG Checklist for Windows 2022
<input checked="" type="checkbox"/>	Windows Server 2022 create global objects user...	No CCEs provided	medium	DISA STIG Checklist for Windows 2022
<input checked="" type="checkbox"/>	Windows Server 2022 permissions for the Applic...	No CCEs provided	medium	DISA STIG Checklist for Windows 2022
<input checked="" type="checkbox"/>	Windows Server 2022 maximum password age m...	No CCEs provided	medium	DISA STIG Checklist for Windows 2022
<input checked="" type="checkbox"/>	Windows Server 2022 Deny log on as a service ...	No CCEs provided	medium	DISA STIG Checklist for Windows 2022
<input checked="" type="checkbox"/>	Windows Server 2022 must have the Server Me...	No CCEs provided	medium	DISA STIG Checklist for Windows 2022
<input checked="" type="checkbox"/>	Windows Server 2022 must not save passwords ...	No CCEs provided	medium	DISA STIG Checklist for Windows 2022

Staged List: The following checks will be copied to your new checklist (including any necessary measured value analyses and/or applicability fixlets):

<input checked="" type="checkbox"/>	Check Name	Source ID	Source Severity	Source Checklist
<input checked="" type="checkbox"/>	Windows Server 2022 Application Compatibility Pr...	No CCEs provided	low	DISA STIG Checklist for Windows 2022
<input checked="" type="checkbox"/>	Windows Server 2022 must be configured to ena...	No CCEs provided	medium	DISA STIG Checklist for Windows 2022
<input checked="" type="checkbox"/>	Windows Server 2022 must be configured to aud...	No CCEs provided	medium	DISA STIG Checklist for Windows 2022
<input checked="" type="checkbox"/>	Windows Server 2022 must not have the TFTP C...	No CCEs provided	medium	DISA STIG Checklist for Windows 2022
<input checked="" type="checkbox"/>	Windows Server 2022 create global objects user ...	No CCEs provided	medium	DISA STIG Checklist for Windows 2022
<input checked="" type="checkbox"/>	Windows Server 2022 permissions for the Applic...	No CCEs provided	medium	DISA STIG Checklist for Windows 2022
<input checked="" type="checkbox"/>	Windows Server 2022 maximum password age mu...	No CCEs provided	medium	DISA STIG Checklist for Windows 2022
<input checked="" type="checkbox"/>	Windows Server 2022 Deny log on as a service u...	No CCEs provided	medium	DISA STIG Checklist for Windows 2022
<input checked="" type="checkbox"/>	Windows Server 2022 must have the Server Mes...	No CCEs provided	medium	DISA STIG Checklist for Windows 2022

212 total checks will be copied to the new checklist

Activate Measured Value analyses after copying ☒

Create Checklist

Windows and Web browser Checklist Components

The Windows™ and Web browser checklist components ensure that the system is systematically reviewed and remains operational, secure, and compliant.

Deploy and Run task

Deploy and Run tasks are a crucial part of the checklist, especially for checks where continuous monitoring is not feasible.

These tasks are prerequisite actions that must be executed on the target endpoints before accurate compliance results can be reported. The task includes all the necessary action scripts and should be performed periodically (e.g., once per day) to update the compliance data collected for the Fixlets listed in the Deploy and Run Task description tab.

Figure 4. List of Fixlets depend on the Deploy and run tasks

10852 Deploy and Run - Microsoft Windows Server 2022

10832 Applicability - Microsoft Windows Server 2022

10750 Applicability - HKU

9774 (L2) Ensure 'Turn on Responder (RSPNDR) driver' is set to 'Disabled' N/A

Task: Deploy and Run - Microsoft Windows Server 2022

Take Action Edit Copy Export Hide Locally Hide Globally Remove

Description Details Applicable Computers (1) Action History (0)

Deploy and Run - Microsoft Windows Server 2022

The following Fixlets require prerequisite actions to be taken on the target endpoints before their compliance results can be reported accurately. This Task contains all the required action as a periodic action (e.g. reapplying once per day) to update the collected compliance data.

- (L1) Ensure 'Network access: Allow anonymous SID/Name translation' is set to 'Disabled'
- (L1) Ensure 'Store passwords using reversible encryption' is set to 'Disabled'
- (L1) Ensure 'Password must meet complexity requirements' is set to 'Enabled'

Actions

Click [here](#) to deploy this action.

Windows checklists require you to run the Deploy and Run tasks to populate the necessary properties on the endpoints, enabling relevance evaluation.

The site includes all required action scripts. When scheduled or executed, it runs all the scripts and stores the results under the BigFix folder structure: C:\Program Files (x86)\BigFix Enterprise\BES Client__BESData__SCMData.



Note: For more details about the folder structure and its output, refer to the [Understanding the output of deploy and Run task \(on page 26\)](#) section.



Note: You do not need to complete this task if your checklist does not include these checks.

The check Fixlets from these sites will only display current results once the Deploy and Run tasks are completed. If you are using any mixed content sites, schedule the periodic execution of the Deploy and Run Task.

1. From the **Security Configuration** domain, navigate to **All Security Configuration > Sites > External Sites**.
2. Select a checklist and click **Fixlets and Tasks**.
3. In the List panel, locate and click the **Deploy and Run Task**.

Figure 5. Deploy and Run Task in the CIS Checklist Windows 2022 DC

Fixlets and Tasks

Search Fixlets and Tasks

ID	Name	Source Sev...	Site	Applicable ...	Open Actio
214129...	Deploy and Run - Microsoft Windows Server 2022		CIS Checklist ...	0 / 0	0
214120...	Applicability - Microsoft Windows Server 2022		CIS Checklist ...	0 / 0	0
150386	Applicability - HKU		CIS Checklist ...	0 / 0	0
147789	(1.2) Ensure "Turn on BitLocker (BSMNDP) driver" is set to "Disabled"	N/A	CIS Checklist	0 / 0	0

Task: Deploy and Run - Microsoft Windows Server 2022

Take Action

Edit

Copy

Export

Hide Locally

Hide Globally

Remove

Description

Details

Applicable Computers (0)

Action History (0)

Description

Deploy and Run - Microsoft Windows Server 2022

The following Fixlets require prerequisite actions to be taken on the target endpoints before their compliance results can be reported accurately. This Task contains all the required action scripts. It should be taken as a periodic action (e.g. reapplying once per day) to update the collected compliance data.

- (L1) Ensure 'Network access: Allow anonymous SID/Name translation' is set to 'Disabled'
- (L1) Ensure 'Store passwords using reversible encryption' is set to 'Disabled'
- (L1) Ensure 'Password must meet complexity requirements' is set to 'Enabled'

Actions

Click [here](#) to deploy this action.

4. Click **Take Action** to deploy the task, or click the appropriate link in the Actions box.
5. Select the appropriate endpoints in your environment.
6. Click the **Execution** tab.

Figure 6. Take Action - Execution tab

Take Action

Name: Create in domain:

Preset: ☐ Show only personal presets

Target Execution Users Messages Offer Post-Action Applicability Success Criteria Action Script

Constraints

☐ Starts on at

☒ Ends on at

☐ Run between and

☐ Run only on

☐ Run only when

Behavior

☐ On failure, retry times

☒ Wait between attempts

☐ Wait until computer has rebooted

☐ Reapply this action

☒ whenever it becomes relevant again

☐ while relevant, waiting between reapplications

☒ Limit to reapplications

☐ Start client downloads before constraints are satisfied

☐ Stagger action start times over minutes to reduce network load

7. Set the Deploy and Run Task to run daily and click **OK**.

8. Once the task is complete, refresh the endpoints.

The Deploy and Run Task will update the reports in the **Security and Compliance Analytics console** (now known as **BigFix Compliance Analytics**) with the latest results. To ensure that you get the most current content, run this task on the endpoint before initiating an import. For automatic daily imports to BigFix Compliance Analytics, scheduling more than one run of the Deploy and Run Task action is unnecessary.

Understanding the output of deploy and Run task

With Windows content, endpoint scans are accomplished by a series of Windows powershell scripts that provide greater accessibility to Windows system administrators.

In BigFix, Fixlets continuously evaluate conditions on each endpoint, displaying results in the console when their relevance clauses of the Fixlets evaluate to true or false. For Windows systems, the "Deploy and Run Task" within a

Security Checklist initiates a scan of the endpoints. This scan can be executed on an ad hoc basis whenever a scan is required or configured as a recurring policy from the console.

The endpoint scan is carried out by various Windows powershell scripts available within the Deploy and Run tasks. These scripts write the information to an output file, which is then used by the corresponding Fixlet checks for evaluation. Once the results files are written to disk, the Fixlets read the output and display the results in the console.

After executing the Deploy and Run task from the Security Checklist, the scripts run and store the results under the directory: `C:\Program Files (x86)\BigFix Enterprise\BES Client__BESData__SCMData`, which contains several components as detailed below:

Table 3. Deploy and Run task result file structure

CIS_secpol.txt	This output file stores security policies of particular CIS Fixlets.
DISA_secpol.txt	This output file stores security policies of particular DISA Fixlets.
Universal_secpol.txt	This output file stores security policies of particular Universal Checklist Fixlets.

Applicability Fixlets

Learn about concepts and the work process in Configuration Management.

Each Windows™ and Web browser checklist includes Applicability Fixlets based on the checklist requirements. For example, in the **DISA STIG Checklist Windows 2022**, the following Applicability Fixlets are available:

- Applicability - HKU
- Applicability - Microsoft Windows Server 2022
- Applicability - Windows Domain Controller
- Applicability - Windows Domain Member or Standalone Server
- Applicability - Windows Domain Member Server
- Applicability - Windows Not Server Core Installation

These Fixlets work with HCL BigFix Compliance to determine whether endpoints subscribed to the checklist meet the required conditions. A Fixlet is relevant only for applicable endpoints and remains irrelevant otherwise. To optimize performance, site subscriptions should be limited to applicable endpoints.



Note: The number of Applicability Fixlets may vary depending on checklist requirements.

Omit List in applicability Fixlets

The Omit List in applicability Fixlets is a predefined list of checks that are excluded from the evaluation process.

In the **Applicability – Microsoft Windows Server 2022**, we include the Omit List, which specifies checks that are not supported from the benchmark. These omitted checks typically require human interaction or have technical limitations that prevent automated evaluation.

Figure 7. Omit list from the DISA Checklist for Windows 2022

Fixlet: Applicability - Microsoft Windows Server 2022																																															
Take Action Edit Copy Export Hide Locally Hide Globally Remove																																															
Description Details Applicable Computers (0) Action History (0)																																															
Applicability – Microsoft Windows Server 2022 <p>This fixlet is used in connection with HCL BigFix Compliance to determine whether endpoints subscribed to the current checklist meet the following condition: Microsoft Windows Server 2022. This fixlet will be relevant for applicable endpoints and not relevant otherwise. Endpoint subscription to applicable endpoints.</p> <p>There may be nearly identical applicability fixlets included within a checklist in cases where the conditions for applicability are related but different.</p> <p>Details of DISA STIG Checklist for Microsoft Windows 2022.</p> <p>Total number of checks: 273 Number of checks supported: 212 Number of checks not supported: 61</p> <p>List of checks not supported from Microsoft Windows 2022 due to the requirement of human interaction / technical limitations</p> <table> <thead> <tr> <th>XCCE Rule ID</th><th>DISA Valid (STIG-ID)</th><th>Reason</th></tr> </thead> <tbody> <tr> <td>xcce_mil.disa.stig_rule_SV-254299r991558_rule</td><td>V-254299</td><td>Require Human Interaction- Related to permission to authorized users</td></tr> <tr> <td>SV-254261r991589_rule</td><td>V-254261</td><td>Software certificate related and due to potential performance impact</td></tr> <tr> <td>SV-254246r991589_rule</td><td>V-254246</td><td>Require Human Interaction, Trusted Platform Module (TPM) configuration required</td></tr> <tr> <td>SV-254283r991589_rule</td><td>V-254283</td><td>Require Human Interaction, Configuration of UEFI firmware to run in UEFI mode required instead of Legacy BIOS mode</td></tr> <tr> <td>SV-254284r991589_rule</td><td>V-254284</td><td>Require Human Interaction, Required to Enable Secure Boot in the system firmware</td></tr> <tr> <td>SV-254266r1000134_rule</td><td>V-254266</td><td>Require Human Interaction, Installation DoD-approved ESS software required</td></tr> <tr> <td>SV-254245r958808_rule</td><td>V-254245</td><td>Require Human Interaction, Related to configuration of whitelisting applications</td></tr> <tr> <td>SV-254267r958364_rule</td><td>V-254267</td><td>Require Human Interaction, Related to removal of temporary user accounts</td></tr> <tr> <td>SV-254260r958524_rule</td><td>V-254260</td><td>Require Human Interaction, Related to non system-created file shares</td></tr> <tr> <td>SV-254268r958508_rule</td><td>V-254268</td><td>Require Human Interaction, Related to removal/disable of emergency accounts</td></tr> <tr> <td>SV-254282r991589_rule</td><td>V-254282</td><td>Require Human Interaction, Related to removal of Orphaned security identifiers (SIDs). Depends upon organization</td></tr> <tr> <td>SV-254263r991589_rule</td><td>V-254263</td><td>Require Human Interaction, Related to installation of host based firewall</td></tr> <tr> <td>SV-254240r991589_rule</td><td>V-254240</td><td>Require Human Interaction, Need to define policy and exception</td></tr> <tr> <td>SV-254343r991589_rule</td><td>V-254343</td><td>Require Human Interaction, Related to Virtualization Based Security (VBS) and DMA Protection requires a CPU that supports input/output memory management unit (IOMMU)</td></tr> </tbody> </table>			XCCE Rule ID	DISA Valid (STIG-ID)	Reason	xcce_mil.disa.stig_rule_SV-254299r991558_rule	V-254299	Require Human Interaction- Related to permission to authorized users	SV-254261r991589_rule	V-254261	Software certificate related and due to potential performance impact	SV-254246r991589_rule	V-254246	Require Human Interaction, Trusted Platform Module (TPM) configuration required	SV-254283r991589_rule	V-254283	Require Human Interaction, Configuration of UEFI firmware to run in UEFI mode required instead of Legacy BIOS mode	SV-254284r991589_rule	V-254284	Require Human Interaction, Required to Enable Secure Boot in the system firmware	SV-254266r1000134_rule	V-254266	Require Human Interaction, Installation DoD-approved ESS software required	SV-254245r958808_rule	V-254245	Require Human Interaction, Related to configuration of whitelisting applications	SV-254267r958364_rule	V-254267	Require Human Interaction, Related to removal of temporary user accounts	SV-254260r958524_rule	V-254260	Require Human Interaction, Related to non system-created file shares	SV-254268r958508_rule	V-254268	Require Human Interaction, Related to removal/disable of emergency accounts	SV-254282r991589_rule	V-254282	Require Human Interaction, Related to removal of Orphaned security identifiers (SIDs). Depends upon organization	SV-254263r991589_rule	V-254263	Require Human Interaction, Related to installation of host based firewall	SV-254240r991589_rule	V-254240	Require Human Interaction, Need to define policy and exception	SV-254343r991589_rule	V-254343	Require Human Interaction, Related to Virtualization Based Security (VBS) and DMA Protection requires a CPU that supports input/output memory management unit (IOMMU)
XCCE Rule ID	DISA Valid (STIG-ID)	Reason																																													
xcce_mil.disa.stig_rule_SV-254299r991558_rule	V-254299	Require Human Interaction- Related to permission to authorized users																																													
SV-254261r991589_rule	V-254261	Software certificate related and due to potential performance impact																																													
SV-254246r991589_rule	V-254246	Require Human Interaction, Trusted Platform Module (TPM) configuration required																																													
SV-254283r991589_rule	V-254283	Require Human Interaction, Configuration of UEFI firmware to run in UEFI mode required instead of Legacy BIOS mode																																													
SV-254284r991589_rule	V-254284	Require Human Interaction, Required to Enable Secure Boot in the system firmware																																													
SV-254266r1000134_rule	V-254266	Require Human Interaction, Installation DoD-approved ESS software required																																													
SV-254245r958808_rule	V-254245	Require Human Interaction, Related to configuration of whitelisting applications																																													
SV-254267r958364_rule	V-254267	Require Human Interaction, Related to removal of temporary user accounts																																													
SV-254260r958524_rule	V-254260	Require Human Interaction, Related to non system-created file shares																																													
SV-254268r958508_rule	V-254268	Require Human Interaction, Related to removal/disable of emergency accounts																																													
SV-254282r991589_rule	V-254282	Require Human Interaction, Related to removal of Orphaned security identifiers (SIDs). Depends upon organization																																													
SV-254263r991589_rule	V-254263	Require Human Interaction, Related to installation of host based firewall																																													
SV-254240r991589_rule	V-254240	Require Human Interaction, Need to define policy and exception																																													
SV-254343r991589_rule	V-254343	Require Human Interaction, Related to Virtualization Based Security (VBS) and DMA Protection requires a CPU that supports input/output memory management unit (IOMMU)																																													

Remediation

Most Windows™ and Web browser checks include built-in remediation capabilities. However, a smaller subset of Windows™ and Web browser audit checks allows customization to audit a non-default value.

If a Windows™ and Web browser audit check supports customization, the **Description tab** of the Fixlet will contain **one or more input fields** for user-defined values.

Remediating configuration settings

Windows™ and Web browser checklists support remediation, allowing console operators to resolve vulnerabilities with a single action. A remediation action can only be executed on an endpoint where the Fixlet is relevant.

You can audit, assess, and remediate configuration settings using **Security and Compliance Analytics (SCA)**, now known as **BigFix Compliance Analytics**. For Fixlet checks that support automatic remediation, a **action button** appears within the relevant Fixlet. Remediation actions can only be applied to relevant and selected endpoints.



Note: Not all Fixlets include a remediation action.



Note: If an external global policy is enabled, any local endpoint changes will be overwritten. In such cases, remediation must be performed using the external global policy solution.

1. Navigate to the **Security Configuration Domain > All Security Configuration > Fixlets and Tasks**.
2. Expand the sub-folders to locate the desired Fixlet.
3. Open the Fixlet, click the **Description** tab, and scroll down to the **Actions** box.
4. Click the link in the **Actions** box to remediate the specified policy issue.

Figure 8. Check containing an action for remediation

Fixlet: Windows Server 2022 password history must be configured to 24 passwords remembered.

Take Action | Edit | Copy | Export | Hide Locally | Hide Globally | Remove

Description | Details | Applicable Computers (0) | Action History (0)

er_2022_STIG

OVAL Definitions
 oval:mil.disa.stig.windows2022.def:254288, oval:mi
 l.disa.stig.defs:def:253300

CPEs
 cpe:/o:microsoft:windows_server_2022:-

Check compliance: Condition 1

Condition 1:
 PasswordHistorySize
 Details: security_database('PasswordHistorySize')
 Compliant if: values.oval?(:all, :at_least_one_exists) {[s] s.to_i >= input.to_i }
 Default value: 24

Desired value:

Click "Save" to update this check.
Note: Only a custom copy of this check can be configured.

Save

Actions
 Click [here](#) to remediate local policy for this setting.

5. Set your parameters in the **Take Action** dialog and click **OK**.

Modifying check parameters

In addition to monitoring compliance status and remediating non-compliant settings, you can modify configuration settings to align with your organization's policies.

To adjust the desired value of a check parameter in the Fixlet check description, you must first create a custom site. For details on custom sites, refer to creating custom checklists. Since parameters are stored as site settings, the same check can be parameterized differently across sites containing a copy of the check.



Note: Not all checks in custom sites can be parameterized.

Certain Fixlet checks allow you to specify a more restrictive value than the default specified by the Windows™ and Web browser checklist, providing greater flexibility to customize security policies to meet the specific requirements.

1. Open the Fixlet check and navigate to the **Description** tab.
2. Scroll down to the **Parameters** section and enter the desired value.

Figure 9. Setting up Parameterization for Fixlets

Fixlet: Windows Server 2022 must have the built-in Windows password complexity policy enabled.

Take Action | Edit | Copy | Export | Hide Locally | Hide Globally | Remove

Description | Details | Applicable Computers (0) | Action History (0)

Check compliance: Condition 1

Condition 1: System access test (PasswordComplexity)
 Details: system_access("PasswordComplexity")
 Compliant if: values.oval?(:all, :at_least_one_exists) {[s] s.to_b == input.to_b }
 Default value: 1

Following are possible values for this parameter (there may be others):

Value	Description
0	disabled
1	enabled

Desired value:

Click "Save" to update this check.
Note: Only a custom copy of this check can be configured.

Save

3. Click **Save**.
4. Deploy the Fixlet.

Measured Value Analysis

Many check Fixlets have a corresponding analysis, often referred to as "measured values", which report the value of the element being evaluated by the check Fixlet.

Each computer reports its properties and analysis values, including active check measured values in your deployment. These results are aggregated by the BigFix Compliance Analytics server and enhanced with computer properties and analysis values, providing both compliance overviews and detailed result lists.

Steps to activate measured values:

- Expand the checklist.
- Navigate to the **Analysis** section.
- In the right-hand panel, select all the analyses.
- Right-click and select **Activate Analysis**.

Figure 10. Non-Activated Measured Value Analyses

Analyses				
Status	Name	Site	Applicable Com	
Not Activated	Measured values - Windows Server 2022 account lockout duration must be configured to 15 minutes or greater.	DISA STIG Checklis...	0	
Not Activated	Measured values - Windows Server 2022 Act as part of the operating system user right must not be assigned to any ...	DISA STIG Checklis...	0	
Not Activated	Measured values - Windows Server 2022 Add workstations to domain user right must only be assigned to the Admini...	DISA STIG Checklis...	0	
Not Activated	Measured values - Windows Server 2022 administrator accounts must not be enumerated during elevation.			
Not Activated	Measured values - Windows Server 2022 Allow log on locally user right must only be assigned to the Administr...			
Not Activated	Measured values - Windows Server 2022 Allow log on through Remote Desktop Services user right must only b			
Not Activated	Measured values - Windows Server 2022 Application Compatibility Program Inventory must be prevented from			
Analysis: Measured values - Windows Server 2022 Access this computer from the network user right must only be assigned to the Admin				
<div><div><div><div><div></div><div>Activate</div></div><div><div></div><div>Deactivate</div></div><div><div></div><div>Edit</div></div><div><div></div><div>Export</div></div><div><div></div><div>Hide Locally</div></div><div><div></div><div>Hide Globally</div></div><div><div></div><div>Remove</div></div></div></div></div>				
Description		Details	Applicable Computers (0)	
<div><div><div><div><div></div><div>Applicable Computers (0)</div></div></div></div></div>		Computer Name	IP Address	OS

Open

Copy Text

Copy Text with Headers

Select All

Globally Hide

Globally Unhide

Locally Hide

Locally Unhide

Activate

Deactivate

Add Comment...

Edit...

Remove

Export

Create New Analysis...

Figure 11. Activated Measured Value Analyses

Analyses							Search Analyses
Status	Name	Site	Applicable Comput...	Activated By	Time Activated		
Activated Globally	Measured values - Windows Server 2022 Act as part of the operating system user right must not be assigned to any ...	DISA STIG Checklis...	0	bigfix	3/22/2025 3:54:28...		
Activated Globally	Measured values - Windows Server 2022 Add workstations to domain user right must only be assigned to the Admini...	DISA STIG Checklis...	0	bigfix	3/22/2025 3:54:28...		
Activated Globally	Measured values - Windows Server 2022 administrator accounts must not be enumerated during elevation.	DISA STIG Checklis...	0	bigfix	3/22/2025 3:54:28...		
Activated Globally	Measured values - Windows Server 2022 Allow log on locally user right must only be assigned to the Administrators ...	DISA STIG Checklis...	0	bigfix	3/22/2025 3:54:28...		
Activated Globally	Measured values - Windows Server 2022 Allow log on through Remote Desktop Services user right must only be assi...	DISA STIG Checklis...	0	bigfix	3/22/2025 3:54:28...		
Activated Globally	Measured values - Windows Server 2022 Application Compatibility Program Inventory must be prevented from colle...	DISA STIG Checklis...	0	bigfix	3/22/2025 3:54:28...		
Activated Globally	Measured values - Windows Server 2022 Application event log size must be configured to 32768 KB or greater.	DISA STIG Checklis...	0	bigfix	3/22/2025 3:54:28...		
Analysis: Measured values - Windows Server 2022 Act as part of the operating system user right must not be assigned to any groups or accounts.							
<div><div><div><div><div><div></div></div></div><div><div>Activate</div></div></div><div><div><div></div></div></div><div><div>Deactivate</div></div></div><div><div><div></div></div></div><div><div>Edit</div></div></div> <div><div><div></div></div></div> <div><div>Export</div></div> <div><div><div></div></div></div> <div><div>Hide Locally</div></div> <div><div><div></div></div></div> <div><div>Hide Globally</div></div> <div><div><div></div></div></div> <div><div>Remove</div></div>							
Description Details Results Applicable Computers (0)							
<div><div><div><div><div><div></div></div></div><div><div>Applicable Computers (0)</div></div></div></div><div><div><div>Computer Name</div><div>IP Address</div><div>OS</div><div>CPU</div><div>Last Report Time</div><div>Locked</div><div>BES Relay S...</div><div>Relay</div><div>User Na</div></div></div></div>							

Using checks and checklists

The check Fixlets in Configuration Management checklists evaluate an endpoint against a defined configuration standard. Many of these check Fixlets have a corresponding analysis, often referred to as "measured values", which reports the value of the element being assessed by the check Fixlet.

Viewing check Fixlets from the HCL BigFix console

A check Fixlet becomes relevant when a client computer is out of compliance with a configuration standard. By reviewing the **Configuration Management Fixlets**, Console Operators can identify non-compliant computers and the corresponding standards.

To access the check Fixlets, subscribe to the **Windows™** and **Web browser** checklist Fixlet sites.

Steps to view the check Fixlets in the HCL BigFix Console:

1. From the **Security Configuration** domain, navigate to **All Security Configuration > Sites > External Sites**.
2. Expand the checklist you want to view.
3. Click **Fixlets and Tasks** to open the Fixlets and Tasks section.
4. Click on one of the Fixlets displayed in the list.

The Fixlet opens with the following tabs: **Description**, **Details**, **Applicable Computers**, and **Action History**.

5. Click the **Description** tab to view details about the Fixlet.

The Fixlet applies to a subset of endpoints on your network, and the size of that subset is shown in the **Applicable Computers** tab.

The description typically includes information about the check, the rationale, and guidelines for remediation actions. If the Fixlet is relevant, you need to take the action listed in the **Remediation** section of the description to address non-compliance. You can also access the associated analysis from this tab.

Chapter 4. Configuring Linux checklists

The Configuration Management checklists for Linux systems are delivered as a set of Fixlets and tasks that can help you find the information you need to manage your deployment.

These checklists help system administrators and IT professionals to efficiently manage and configure Linux systems in their environment.

These checklists typically include a series of actions or tasks that cover critical areas of system configuration, security, and compliance. The goal is to ensure that all systems are correctly set up, secure, and aligned with organizational or industry standards.

Overview

Learn about concepts and the work process in Linux checklists.

You can configure Linux checklists for all major Linux distributions, including Red Hat Linux, CentOS, Oracle Linux, Debian, Ubuntu, Rocky Linux, and SUSE Linux.

The Linux™ checklist in BigFix effectively meets the requirements outlined in the CIS and DISA checklists for these distributions, with a strong emphasis on compliance monitoring.

Most of the Linux™ audit checks come with built-in remediation. However, a smaller subset of audit checks allows for flexibility in auditing non-default values. If customization is available for a particular audit check, you will find corresponding input fields in the **Description tab** of the Fixlet®. You can easily adjust the field to your desired audit value and then click **Save** to apply the changes.

What's new in Linux checklist

HCL BigFix Compliance Linux checklist provides additional support and enhancement in the recent update.

The **HCL BigFix Compliance Linux checklist** has received additional support and enhancements in the recent update.

As part of the Linux checklist, we are in the process of eliminating the dependency on the SQLite package in the **Deploy and Run** tasks.

Several checks have been improved by adding a **pending restart** feature. This feature operates as follows:

- For checks that require an OS reboot, the action results will now display "Pending Restart" instead of "Fixed."

Figure 12. Pending start

Send Refresh		
Relevant Baselines (0)	Baseline Component Applicability	Action History (1)
Time Issued ^	Status	Name
11/28/2024 3:16:35 AM	Pending Restart	OL 8 must generate audit records for any use of the "unix_chkpwd" command.

- The check will remain relevant for those endpoints until they are rebooted.
- After the endpoint is rebooted, the action results will display as “Fixed”, and the check will be marked as compliant.

For a detailed list of releases, see the [Linux Checklist Release Notes](#).

Available Linux checklist

Linux checklists are commonly used to ensure systems are secure, optimized, and compliant with best practices.

Below are the Linux checklists available in the License dashboard:

Table 4. Linux checklist

CIS Checklists	DISA STIG Checklists
Amazon Linux	Oracle Linux
Centos	Centos
Debian	RHEL
Rocky Linux	Suse
Distribution Independent Linux	Ubuntu
Ubuntu	
Oracle Linux	
RHEL	
Suse	

To get more details of Linux checklist, refer to the [Linux Checklist](#).

Setup and configuration

Create custom copies of the Linux checklist content if you want to modify the checks based on a specific corporate policy. You can manually create a custom site to host the Linux checklist or use the Create Custom Checklist wizard to create copies of the Linux checklist and save them in a custom site.

You must subscribe to the SCM Reporting external site.

You can use custom checklists to fine-tune your ability to customize Configuration Management parameters, which gives you control over your security status. Custom checklists target specific sets of computers with tailored content using the subscription mechanism. This allows statistics to be gathered with finer granularity. For more information, see [Modifying check parameters \(on page 47\)](#).

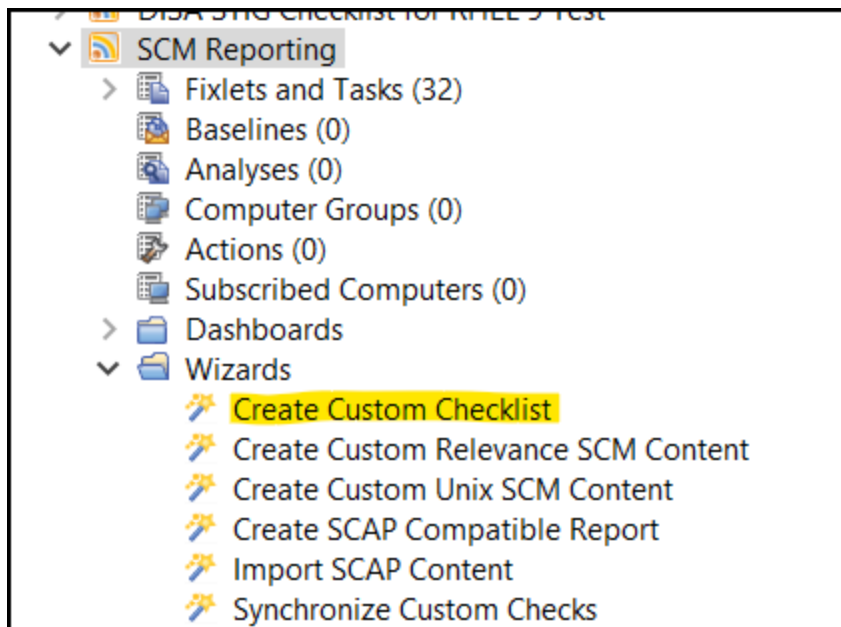
- Creating custom checklists by using the Create Custom Checklist wizard:

1. From the Security Configuration Domain, go to **Configuration Management > Checklist Tools > Create Custom Checklist**.
2. Enter the name of the new checklist.
3. Select the target platform.
4. Click the drop-down menu to select which external checklist you copy the checks from. As you select the checks, they are shown in the staged list at the lower part of the window.
5. Click the **Activate Measured Value analyses after copying** check box to activate all analyses that were copied.
6. Click **Create Checklist**.

The console begins copying the checks in the selected lists into your new custom checklist. The process might take several minutes, depending on the number and size of the checklists selected.

Use the **Create Custom Checklist** wizard located in the **SCM Reporting** site under the wizard section.

Figure 13. Create custom checklist



- Creating custom checklists manually:

1. Select **Tools > Create Custom Site**.
2. You are prompted for a name for your custom site. Enter a name and click **OK**.
3. From the Domain panel, find your site under **Sites > Custom** and click it to describe your site.
From the **Details** tab, enter a description of your site. From the **Domain** pull-down menu, select a Domain to house your site.
4. From the **Computer Subscriptions** tab, indicate which subset of your BigFix client computers you want to subscribe to this site.

- From the **Operator Permissions** tab, you can grant specific access permissions to specific operators.
- Click the **Save Changes** button above the work area to complete the description of your site. You must enter your password to propagate your new custom site.

Subscribe computers to the custom checklist.



Note: Custom checklists do not support site relevance, so take extra precaution when you subscribe computers to custom checklists.

Figure 14. Create custom checklist

Create Custom Checklist

This wizard will assist you in creating a new custom checklist based on one or more of your currently subscribed external checklists.

New checklist name:

External checklist to copy checks from: (252 checks selected out of 252 displayed)

Check Name	Source ID	Source Severity	Source Checklist
Ensure iptables is enabled and active	No CCEs provided	N/A	CIS Checklist for RHEL 8
Ensure nosuid option set on /dev/shm par...	No CCEs provided	N/A	CIS Checklist for RHEL 8
Ensure users' .netrc Files are not group o...	No CCEs provided	N/A	CIS Checklist for RHEL 8
Disable USB Storage	No CCEs provided	N/A	CIS Checklist for RHEL 8
Ensure nftables rules are permanent	No CCEs provided	N/A	CIS Checklist for RHEL 8
Ensure separate partition exists for /var/l...	No CCEs provided	N/A	CIS Checklist for RHEL 8
Ensure permissions on SSH private host k...	No CCEs provided	N/A	CIS Checklist for RHEL 8
Ensure users' dot files are not group or w...	No CCEs provided	N/A	CIS Checklist for RHEL 8
Ensure SSH LoginGraceTime is set to one ...	No CCEs provided	N/A	CIS Checklist for RHEL 8
Ensure minimum days between password ...	No CCEs provided	N/A	CIS Checklist for RHEL 8

Staged List: The following checks will be copied to your new checklist (including any necessary measured value analyses and/or applicability fixlets):

Check Name	Source ID	Source Severity	Source Checklist
Ensure password expiration is 365 days or...	No CCEs provided	N/A	CIS Checklist for RHEL 8
Ensure SSH warning banner is configured	No CCEs provided	N/A	CIS Checklist for RHEL 8
Ensure journald is configured to compress...	No CCEs provided	N/A	CIS Checklist for RHEL 8
Ensure iptables is enabled and active	No CCEs provided	N/A	CIS Checklist for RHEL 8
Ensure nosuid option set on /dev/shm par...	No CCEs provided	N/A	CIS Checklist for RHEL 8
Ensure users' .netrc Files are not group or...	No CCEs provided	N/A	CIS Checklist for RHEL 8
Disable USB Storage	No CCEs provided	N/A	CIS Checklist for RHEL 8
Ensure nftables rules are permanent	No CCEs provided	N/A	CIS Checklist for RHEL 8
Ensure separate partition exists for /var/l...	No CCEs provided	N/A	CIS Checklist for RHEL 8
Ensure permissions on SSH private host k...	No CCEs provided	N/A	CIS Checklist for RHEL 8

252 total checks will be copied to the new checklist

Activate Measured Value analyses after copying ☐ Create Checklist

- Run or Schedule your checklist:

- Schedule or run the **Deploy and Run Task**. Select the **Deploy and Run Task** and click the **Take Action** button.
- Set up or modify the global filesystem scan parameters.
- Specify the amount of points to skip during the filesystem scan.
- Choose the targeted computer or group of computers from the target section.
- Configure the execution criteria based on your environment and click "OK" to schedule or set up the Deploy and Run task.



Note: To get more details information about the file system scan option, see [Modifying global scan options \(on page 43\)](#) section.



Note: To get more details about the Deploy and Run tasks, see [Deploy and Run task details \(on page 39\)](#) section.

Checklist components

The Linux Checklist Components ensure that the system is systematically reviewed and remains operational, secure, and compliant.

Deploy and Run Task

Deploy and Run tasks are a crucial part of the checklist, especially for checks where continuous monitoring is not feasible.

These tasks are prerequisite actions that must be executed on the target endpoints before accurate compliance results can be reported. The task includes all the necessary action scripts and should be performed periodically (e.g., once per day) to update the compliance data collected for the Fixlets listed in the Deploy and Run Task description tab.

Figure 15. Deploy and run

Name	Source Sev...	Site	Applicabl
Applicability - CIS Red Hat Enterprise Linux 7 Benchmark - Filesystem Scan		CIS Checklist for RHEL 7	0 / 0
Deploy and Run CIS Red Hat Enterprise Linux 7		CIS Checklist for RHEL 7	0 / 0
Disable Automounting	N/A	CIS Checklist for RHEL 7	0 / 0

Task: Deploy and Run CIS Red Hat Enterprise Linux 7

Take Action
 Edit
 Copy
 Export
 Hide Locally
 Hide Globally
 Remove

Description Details Applicable Computers (0) Action History (0)

Description

The following Fixlets require prerequisite actions to be taken on the target endpoints before their compliance results can be reported accurately. This Task contains all the required action scripts. (e.g. reapplying once per day) to update the collected compliance data.

Note: sqlite3 package must be installed on the system.

The action will scan target endpoints to collect information on file attributes and store them under Bigfix data folder. It may take more time and space for the action to be completed under the end usual systems (e.g. a file server). Please review the options to exclude unnecessary filesystems from being scanned.

- [Ensure mounting of cramfs filesystems is disabled](#)
- [Ensure mounting of squashfs filesystems is disabled](#)
- [Ensure mounting of udf filesystems is disabled](#)
- [Ensure removable media partitions include noexec option](#)
- [Ensure nodev option set on removable media partitions](#)
- [Ensure nosuid option set on removable media partitions](#)
- [Ensure sticky bit is set on all world-writable directories](#)
- [Disable Automounting](#)
- [Disable USB Storage](#)
- [Disable the rhnsd Daemon](#)
- [Ensure filesystem integrity is regularly checked](#)
- [Ensure XD/NX support is enabled](#)
- [Ensure no unconfined services exist](#)
- [Ensure ntp is configured](#)
- [Ensure mail transfer agent is configured for local-only mode](#)
- [Ensure nfs-utils is not installed or the nfs-server service is masked](#)
- [Ensure rpcbind is not installed or the rpcbind services are masked](#)
- [Ensure rsync is not installed or the rsyncd service is masked](#)
- [Ensure wireless interfaces are disabled](#)
- [Ensure DCCP is disabled](#)
- [Ensure SCTP is disabled](#)
- [Ensure sctp is disabled or masked with firewall](#)

Linux checklists require you to run the Deploy and Run tasks to populate the necessary properties on the endpoints, enabling relevance evaluation. Execute this task when it appears as relevant and refresh the results on the endpoint.

For custom sites, spaces in the name are replaced with underscores, and the `CustomSite_` prefix is added. For example: `/var/opt/BESClient/___BESData/CustomSite_Checklist_for_RHEL7`.

The site includes all required action scripts. When scheduled or executed, it runs all the scripts and stores the results in `result.db` and `.out` files under the BigFix folder structure: `/var/opt/BESClient/___BESData/___SCMData/`.



Note: For more details about the folder structure and its output, refer to the [Understanding the output of deploy and Run task \(on page 42\)](#) section.



Note: You do not need to complete this task if your checklist does not include these checks.



Note: For some checklists, the SQLite package is required to make the Deploy and Run task relevant.

The check Fixlets from these sites will only display current results once the Deploy and Run tasks are completed. If you are using any mixed content sites, schedule periodic execution of the Deploy and Run Task.

1. From the **Security Configuration** domain, navigate to **All Security Configuration > Sites > External Sites**.
2. Select a checklist and click **Fixlets and Tasks**.
3. In the List panel, locate and click the **Deploy and Run Task**.

Figure 16. Deploy and Run

Name	Source Sev...	Site	Applicable ...	Open Actio...	Category	Down
Applicability - CIS Red Hat Enterprise Linux 7 Benchmark		CIS Checklist for RHEL 7	0 / 1	0		
Applicability - CIS Red Hat Enterprise Linux 7 Benchmark - Deploy and Run		CIS Checklist for RHEL 7	0 / 1	0		
Applicability - CIS Red Hat Enterprise Linux 7 Benchmark - Filesystem Scan		CIS Checklist for RHEL 7	0 / 1	0		
Deploy and Run CIS Red Hat Enterprise Linux 7		CIS Checklist for RHEL 7	1 / 1	0		
Ensure /dev/shm is a separate partition	N/A	CIS Checklist for RHEL 7	1 / 1	0	Configure /...	<no d

Task: Deploy and Run CIS Red Hat Enterprise Linux 7

Take Action | Edit | Copy | Export | Hide Locally | Hide Globally | Remove

Description | Details | Applicable Computers (1) | Action History (1)

Description

The following Fixlets require prerequisite actions to be taken on the target endpoints before their compliance results can be reported accurately. This Task contains all the required action scripts. It should be taken as a periodic action (e.g. read data).

The action will scan target endpoints to collect information on file attributes and store them under Bigfix data folder. It may take more time and space for the action to be completed under the endpoints which store more files than usual system unnecessary filesystems from being scanned.

- Ensure SELinux is not disabled in bootloader configuration
- Ensure SELinux policy is configured
- Ensure the SELinux mode is not disabled
- Ensure the SELinux mode is enforcing
- Ensure no unconfined services exist
- Ensure message of the day is configured properly
- Ensure local login warning banner is configured properly
- Ensure remote login warning banner is configured properly
- Ensure avahi-daemon services are not in use
- Ensure dhcp server services are not in use
- Ensure print server services are not in use
- Ensure rpcbind services are not in use
- Ensure rsync services are not in use
- Ensure telnet server services are not in use
- Ensure tftp server services are not in use
- Ensure web server services are not in use
- Ensure mail transfer agents are configured for local-only mode
- Ensure a single firewall configuration utility is in use
- Ensure firewall service enabled and running
- Ensure an rftables table exists

4. Click **Take Action** to deploy the task, or click the appropriate link in the Actions box.
5. Select the appropriate endpoints in your environment.
6. Click the **Execution** tab.

Take Action

Name: Create in domain:

Preset: ☐ Show only personal presets

Target Execution Users Messages Offer Post-Action Applicability Success Criteria Action Script

Constraints

☐ Starts on at

☒ Ends on at

☐ Run between and

☐ Run only on

☐ Run only when

Behavior

☐ On failure, retry times

☒ Wait between attempts

☐ Wait until computer has rebooted

☐ Reapply this action

☒ whenever it becomes relevant again

☐ while relevant, waiting between reapplications

☒ Limit to reapplications

☐ Start client downloads before constraints are satisfied

☐ Stagger action start times over minutes to reduce network load

7. Set the Deploy and Run Task to run daily and click OK.

8. Once the task is complete, refresh the endpoints.

The Deploy and Run Task will update the reports in the **Security and Compliance Analytics console** (now known as **BigFix Compliance Analytics**) with the latest results. To ensure you get the most current content, run this task on the endpoint before initiating an import. For automatic daily imports to BigFix Compliance Analytics, scheduling more than one run of the Deploy and Run Task action is unnecessary.



Note: Parameter changes will take effect only after the next run of the Deploy and Run Task.

Deploy and Run task

Deploy and Run tasks are a crucial part of the checklist, especially for checks where continuous monitoring is not feasible.

These tasks are prerequisite actions that must be executed on the target endpoints before accurate compliance results can be reported. The task includes all the necessary action scripts and should be performed periodically (e.g., once per day) to update the compliance data collected for the Fixlets listed in the Deploy and Run Task description tab.

Figure 17. Deploy and run

Name	Source Sev...	Site	Applicabl
Applicability - CIS Red Hat Enterprise Linux 7 Benchmark - Filesystem Scan		CIS Checklist for RHEL 7	0 / 0
Deploy and Run CIS Red Hat Enterprise Linux 7		CIS Checklist for RHEL 7	0 / 0
Disable Automounting	N/A	CIS Checklist for RHEL 7	0 / 0

Task: Deploy and Run CIS Red Hat Enterprise Linux 7

Take Action | Edit | Copy | Export | Hide Locally | Hide Globally | Remove

Description | Details | Applicable Computers (0) | Action History (0)

Description

The following Fixlets require prerequisite actions to be taken on the target endpoints before their compliance results can be reported accurately. This Task contains all the required action scripts (e.g. reapplying once per day) to update the collected compliance data.

Note: sqlite3 package must be installed on the system.

The action will scan target endpoints to collect information on file attributes and store them under BigFix data folder. It may take more time and space for the action to be completed under the end usual systems (e.g. a file server). Please review the options to exclude unnecessary filesystems from being scanned.

- Ensure mounting of cramfs filesystems is disabled
- Ensure mounting of squashfs filesystems is disabled
- Ensure mounting of udf filesystems is disabled
- Ensure removable media partitions include noexec option
- Ensure nodev option set on removable media partitions
- Ensure nosuid option set on removable media partitions
- Ensure sticky bit is set on all world-writable directories
- Disable Automounting
- Disable USB Storage
- Disable the rhnsd Daemon
- Ensure filesystem integrity is regularly checked
- Ensure XD/NX support is enabled
- Ensure no unconfined services exist
- Ensure ntp is configured
- Ensure mail transfer agent is configured for local-only mode
- Ensure nfs-utils is not installed or the nfs-server service is masked
- Ensure rpcbind is not installed or the rpcbind service is masked
- Ensure rsync is not installed or the rsyncd service is masked
- Ensure wireless interfaces are disabled
- Ensure DCCP is disabled
- Ensure SCTP is disabled
- Ensure sshd is either not installed or masked with firewalld

Linux checklists require you to run the Deploy and Run tasks to populate the necessary properties on the endpoints, enabling relevance evaluation. Execute this task when it appears as relevant and refresh the results on the endpoint.

For custom sites, spaces in the name are replaced with underscores, and the `CustomSite_` prefix is added. For example: `/var/opt/BESClient/___BESData/CustomSite_Checklist_for_RHEL7`.

The site includes all required action scripts. When scheduled or executed, it runs all the scripts and stores the results in `result.db` and `.out` files under the BigFix folder structure: `/var/opt/BESClient/___BESData/___SCMData/`.



Note: For more details about the folder structure and its output, refer to the [Understanding the output of deploy and Run task \(on page 42\)](#) section.



Note: You do not need to complete this task if your checklist does not include these checks.



Note: For some checklists, the SQLite package is required to make the Deploy and Run task relevant.

The check Fixlets from these sites will only display current results once the Deploy and Run tasks are completed. If you are using any mixed content sites, schedule periodic execution of the Deploy and Run Task.

1. From the **Security Configuration** domain, navigate to **All Security Configuration > Sites > External Sites**.
2. Select a checklist and click **Fixlets and Tasks**.
3. In the List panel, locate and click the **Deploy and Run Task**.

Figure 18. Deploy and run

The screenshot shows the 'Fixlets and Tasks' interface. At the top, there are navigation buttons: 'Forward', 'Show Hidden Content', 'Show Non-Relevant Content', and 'Refresh Console'. Below this is a table with columns: Name, Source Sev., Site, Applicable ..., Open Actio..., Category, and Down. The table lists several tasks, including 'Applicability - CIS Red Hat Enterprise Linux 7 Benchmark' and 'Deploy and Run CIS Red Hat Enterprise Linux 7'. The 'Deploy and Run CIS Red Hat Enterprise Linux 7' task is highlighted. Below the table, there are buttons for 'Take Action', 'Edit', 'Copy', 'Export', 'Hide Locally', 'Hide Globally', and 'Remove'. The 'Description' tab is selected, showing a detailed description of the task and a list of prerequisite actions.

Name	Source Sev.	Site	Applicable ...	Open Actio...	Category	Down
Applicability - CIS Red Hat Enterprise Linux 7 Benchmark		CIS Checklist for RHEL 7	0 / 1	0		
Applicability - CIS Red Hat Enterprise Linux 7 Benchmark - Deploy and Run		CIS Checklist for RHEL 7	0 / 1	0		
Applicability - CIS Red Hat Enterprise Linux 7 Benchmark - Filesystem Scan		CIS Checklist for RHEL 7	0 / 1	0		
Deploy and Run CIS Red Hat Enterprise Linux 7		CIS Checklist for RHEL 7	1 / 1	0		
Ensure /dev/shm is a separate partition	N/A	CIS Checklist for RHEL 7	1 / 1	0	Configure /...	<no d

Task: Deploy and Run CIS Red Hat Enterprise Linux 7

Description

The following Fixlets require prerequisite actions to be taken on the target endpoints before their compliance results can be reported accurately. This Task contains all the required action scripts. It should be taken as a periodic action (e.g. read data).

The action will scan target endpoints to collect information on file attributes and store them under Bigfix data folder. It may take more time and space for the action to be completed under the endpoints which store more files than usual system unnecessary filesystems from being scanned.

- Ensure SELinux is not disabled in bootloader configuration
- Ensure SELinux policy is configured
- Ensure the SELinux mode is not disabled
- Ensure the SELinux mode is enforcing
- Ensure no unconfined services exist
- Ensure message of the day is configured properly
- Ensure local login warning banner is configured properly
- Ensure remote login warning banner is configured properly
- Ensure xauth daemon services are not in use
- Ensure dhcp server services are not in use
- Ensure print server services are not in use
- Ensure rsync services are not in use
- Ensure telnet server services are not in use
- Ensure the server services are not in use
- Ensure web server services are not in use
- Ensure mail transfer agents are configured for local-only mode
- Ensure a single firewall configuration utility is in use
- Ensure firewall service enabled and running
- Ensure an authentic table exists

4. Click **Take Action** to deploy the task, or click the appropriate link in the Actions box.
5. Select the appropriate endpoints in your environment.
6. Click the **Execution** tab.

Take Action

Name: Create in domain:

Preset: ☐ Show only personal presets

Target Execution Users Messages Offer Post-Action Applicability Success Criteria Action Script

Constraints

☐ Starts on at

☒ Ends on at

☐ Run between and

☐ Run only on

☐ Run only when

Behavior

☐ On failure, retry times

☒ Wait between attempts

☐ Wait until computer has rebooted

☐ Reapply this action

☒ whenever it becomes relevant again

☐ while relevant, waiting between reapplications

☒ Limit to reapplications

☐ Start client downloads before constraints are satisfied

☐ Stagger action start times over minutes to reduce network load

7. Set the Deploy and Run Task to run daily and click OK.

8. Once the task is complete, refresh the endpoints.

The Deploy and Run Task will update the reports in the **Security and Compliance Analytics console** (now known as **BigFix Compliance Analytics**) with the latest results. To ensure you get the most current content, run this task on the endpoint before initiating an import. For automatic daily imports to BigFix Compliance Analytics, scheduling more than one run of the Deploy and Run Task action is unnecessary.



Note: Parameter changes will take effect only after the next run of the Deploy and Run Task.

Understanding the output of deploy and Run task

With Linux content, endpoint scans are performed using a series of Linux shell scripts, offering enhanced accessibility for Linux system administrators.

Unlike most BigFix content where Fixlets continuously evaluate conditions at each endpoint, Linux content utilizes a Deploy and Run task from the Security Checklist to initiate a scan on the endpoints. This scan can be executed on-demand whenever needed or scheduled as a recurring policy from the console.

The endpoint scan is carried out by various Linux shell scripts available within the Deploy and Run tasks. These scripts write the gathered information to an output file, which is then used by the corresponding Fixlet checks for evaluation. Once the results files are written to disk, the Fixlets read the output and display the results in the console.

After executing the Deploy and Run task from the Security Checklist, the scripts run and store the results under the directory: `/var/opt/BESClient/___BESData/___SCMData/`, which contains several components as detailed below:

Table 5. Deploy and Run task result file structure.

fileresults.db	Created upon successful completion of the Deploy and Run tasks, storing the results of the entire filesystem scan.
<HashValue>.out	Stores the results of a particular Fixlet audit script.
<HashValue>.out.err	Contains error outputs from a specific Fixlet audit script.
<HashValue>.out.metadata	Stores metadata related to a specific Fixlet audit script.
remediation.log	Logs the actions executed by the script.
remediation.log	Contains error logs related to the action script.
remediation.log.metadata	Stores metadata related to the action script.

Modifying global scan options

You can control the behavior of the global scan through the pop box on Deploy and Run in the Linux Checklists.

Linux™ content includes a global scan script part of the **Deploy and Run tasks** and that is used to do a full system scan. The results of this scan are used in several scripts. This script eliminates the need to run a full system scan multiple times when you are evaluating a set of checks on a single system. This feature allows Endpoint Manager to be more efficient and causes less impact on the system during a configuration scan.

Table 6. Parameters and their descriptions

Parameter	Description
EXCLUDEFS	<p>A list of specific file systems to exclude from scanning. This list must be a space-separated list of all the file system types to exclude from the search.</p> <p>By default, the global find script excludes the following file system types from its search:</p> <ul style="list-style-type: none"> • devpts • tmpfs • cdrfs • procfs • ctf • fd • hsfs • proc • mntfs • smbfs • iso9660 • nfs3 • nfs4 • nfs • msdos • nfsd • rpc_pipefs • binfmt_misc • sysfs • sharefs
EXCLUDEMOUNTS	<p>A list of specific mount points to exclude from scanning. This parameter must be defined as a space-separated list of all the file system mounts to exclude from the search. This prevents the shared file system from being scanned from multiple systems.</p> <p>For example, if several systems mount a shared directory on a Storage Area Network named /san, you might want to exclude them with a parameter such as: EXCLUDEMOUNTS="/san"</p> <p>By default, this parameter is not used and is represented as an empty value.</p>

Table 6. Parameters and their descriptions (continued)

Parameter	Description
EXCLUDEINODES	Threshold Inode count to skip file system during scan.

Action Parameter

Please enter a space separated list of filesystem types to skip during file scan, default is 'devpts tmpfs cdrfs procfs cifs fd hfs proc mntfs smbfs iso9660 nfs3 nfs4 nfs msdos nfsd rpc_pipefs binfmt_misc sysfs sharefs'.

3 nfs4 nfs msdos nfsd rpc_pipefs binfmt_misc sysfs sharefs

Ok Cancel

Action Parameter

Please enter a space separated list of mount points to skip during file scan, default is "".

Ok Cancel

To view the policies, click Reports > Policies.

Applicability Fixlets

Learn about concepts and the work process in Configuration Management.

Each Linux checklist includes three Applicability Fixlets, which are determined based on the checklist's requirements. Using the "CIS Red Hat Enterprise Linux 7" checklist as an example, the following Applicability Fixlets are included:

1. Applicability - CIS Red Hat Enterprise Linux 7 Benchmark - Filesystem Scan
2. Applicability - CIS Red Hat Enterprise Linux 7 Benchmark - Deploy and Run
3. Applicability - CIS Red Hat Enterprise Linux 7 Benchmark

These Applicability Fixlets work with HCL BigFix Compliance to evaluate whether the endpoints subscribed to the checklist meet the required conditions. Fixlets will be relevant for applicable endpoints and non-relevant for others. To ensure accurate evaluation, site subscriptions should be limited to applicable endpoints.



Note: The number of Applicability Fixlets may vary depending on the requirements of the specific checklist.

Omit List in applicability Fixlets

The Omit List in applicability Fixlets is a predefined list of checks that are excluded from the evaluation process.

In the **Applicability – CIS Red Hat Enterprise Linux 7 Benchmark**, the Omit List is used to specify: A list of checks from the benchmark that are not supported due to requirements for human interaction or technical limitations.

Figure 19. Omit list

Applicability – CIS Red Hat Enterprise Linux 7 Benchmark

This fixlet is used in connection with HCL BigFix Compliance to determine whether endpoints subscribed to the current checklist meet the following condition: CIS Red Hat Enterprise Linux 7 Benchmark. 1 fixlet will be relevant for applicable endpoints and not relevant otherwise. Effort should be made to limit site subscription to applicable endpoints.

There may be nearly identical applicability fixlets included within a checklist in cases where the conditions for applicability are related but different.

Checks not supported from CIS Red Hat Enterprise Linux 7 Benchmark

List of checks not supported from CIS Red Hat Enterprise Linux 7 due to the requirement of human interaction / technical limitations

Total number of checks: 306
Number of checks supported: 288
Number of checks not supported: 18

XCCDF Rule ID	Reason
"xccdf_org.cisecurity.benchmarks_rule_1.2.4_Ensure_package_manager_repositories_are_configured"	"Manual check"
"xccdf_org.cisecurity.benchmarks_rule_1.2.5_Ensure_updates_patches_and_additional_security_software_are_installed"	"Manual check"
"xccdf_org.cisecurity.benchmarks_rule_3.4.2.4_Ensure_network_interfaces_are_assigned_to_appropriate_zone"	"Manual check"
"xccdf_org.cisecurity.benchmarks_rule_3.4.2.3_Ensure_firewall_drops_unnecessary_services_and_ports"	"Manual check"
"xccdf_org.cisecurity.benchmarks_rule_3.4.3.6_Ensure_nftables_outbound_and_established_connections_are_configured"	"Manual check"
"xccdf_org.cisecurity.benchmarks_rule_3.4.4.2.2_Ensure_iptables_outbound_and_established_connections_are_configured"	"Manual check"
"xccdf_org.cisecurity.benchmarks_rule_3.4.4.3.2_Ensure_ip6tables_outbound_and_established_connections_are_configured"	"Manual check"
"xccdf_org.cisecurity.benchmarks_rule_3.4.4.3.3_Ensure_ip6tables_rules_exist_for_all_open_ports"	"Manual check"
"xccdf_org.cisecurity.benchmarks_rule_3.4.4.3.3_Ensure_ip6tables_firewall_rules_exist_for_all_open_ports"	"Manual check"
"xccdf_org.cisecurity.benchmarks_rule_5.1.1.5_Ensure_logging_is_configured"	"Manual check"
"xccdf_org.cisecurity.benchmarks_rule_6.1.13_Ensure_SUID_and_SGID_files_are_reviewed"	"Manual check"
"xccdf_org.cisecurity.benchmarks_rule_6.1.14_Audit_system_file_permissions"	"Manual check"
"xccdf_org.cisecurity.benchmarks_rule_5.1.3_Ensure_logrotate_is_configured"	"Manual check"
"xccdf_org.cisecurity.benchmarks_rule_5.1.1.5_Ensure_logging_is_configured"	"Manual check"
"xccdf_org.cisecurity.benchmarks_rule_3.4.3.2_Ensure_ip6tables_are_flushed_with_nftables"	"Manual check"
"xccdf_org.cisecurity.benchmarks_rule_5.1.2.6_Ensure_journal_log_rotation_is_configured_per_site_policy"	"Manual check"
"xccdf_org.cisecurity.benchmarks_rule_2.2.22_Ensure_only_approved_services_are_listening_on_a_network_interface"	"Manual check"
"xccdf_org.cisecurity.benchmarks_rule_1.2.1_Ensure_GPG_keys_are_configured"	"Manual check"

Activate W
Go to Settings

Remediation


Most Linux audit checks include built-in remediation capabilities. However, a smaller subset of Linux audit checks can be customized to audit non-default values.


If a Linux audit check supports customization, the **Description** tab of the Fixlet will display one or more input fields. These fields allow users to define specific values or parameters to tailor the check according to their requirements.

Remediating configuration settings

The Linux checklists provide remediation support, allowing console operators to address vulnerability issues with a single action. Remediation actions can only be executed on endpoints where the corresponding Fixlet is relevant.

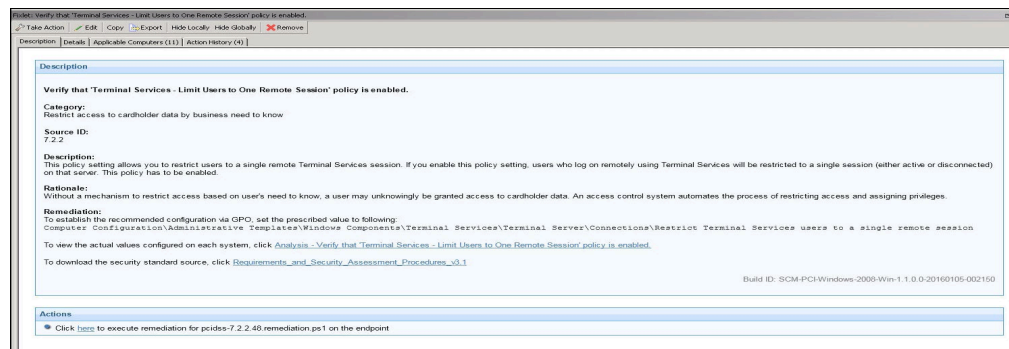
You can audit, assess, and remediate configuration settings using **Security and Compliance Analytics (SCA)**, now referred to as **BigFix Compliance Analytics**. For Fixlet checks that support automatic remediation, an action option is displayed in the relevant Fixlet. Remediation actions can only be taken on applicable and selected endpoints.

 **Note:** Not all Fixlets include a remediation action.

 **Note:** If an external global policy is enabled, any local endpoint changes will be overwritten. In such cases, remediation must be performed through the external global policy solution.

1. Navigate to the **Security Configuration Domain**: Go to **All Security Configuration > Fixlets and Tasks**.
2. Expand the sub-folders to locate the desired Fixlet.
3. Open the Fixlet, click the **Description** tab, and scroll down to the **Actions** box.
4. Click the link in the **Actions** box to remediate the specified policy issue.

Figure 20. Remediation



5. Set your parameters in the **Take Action** dialog and click **OK**.

Modifying check parameters

In addition to monitoring compliance status and remediating non-compliant settings, you can modify configuration settings to align with your organization's policies.

To adjust the desired value of a check parameter in the Fixlet check description, you must first create a custom site. For details on custom sites, refer to Creating Custom Checklists. Since parameters are stored as site settings, the same check can be parameterized differently across sites containing a copy of the check.



Note: Not all checks in custom sites can be parameterized.

Certain Fixlet checks allow you to specify a more restrictive value than the default specified by the Linux checklist, providing greater flexibility to tailor security policies to specific requirements.



Important: Custom parameterization may take a few minutes to process. Allow sufficient time between updating a parameter and executing the **Deploy and Run Task** for optimal results.



Note: Parameter changes will only take effect after running the Deploy and Run Task. For more details, see **Configuring Endpoints**.

1. Open the Fixlet check and navigate to the **Description** tab.
2. Scroll down to the **Parameters** section and enter the desired value.

Figure 21. Setting up Parameterization for Fixlets

Value	Description
600	10_minutes
900	15_minutes

Desired value:

Click "Save" to update this check.
Note: Only a custom copy of this check can be configured.

3. Click **Save**.
4. Deploy the Fixlet.

Measured Value Analysis

Many check Fixlets have a corresponding analysis, often referred to as "measured values", which report the value of the element being evaluated by the check Fixlet.

Each computer reports its properties and analysis values, including active check measured values in your deployment. These results are aggregated by the BigFix Compliance Analytics server and enhanced with computer properties and analysis values, providing both compliance overviews and detailed result lists.

Steps to activate measured values:

- Expand the checklist.
- Navigate to the **Analysis** section.
- In the right-hand panel, select all the analyses.
- Right-click and select **Activate Analysis**.

Figure 22. Measured value

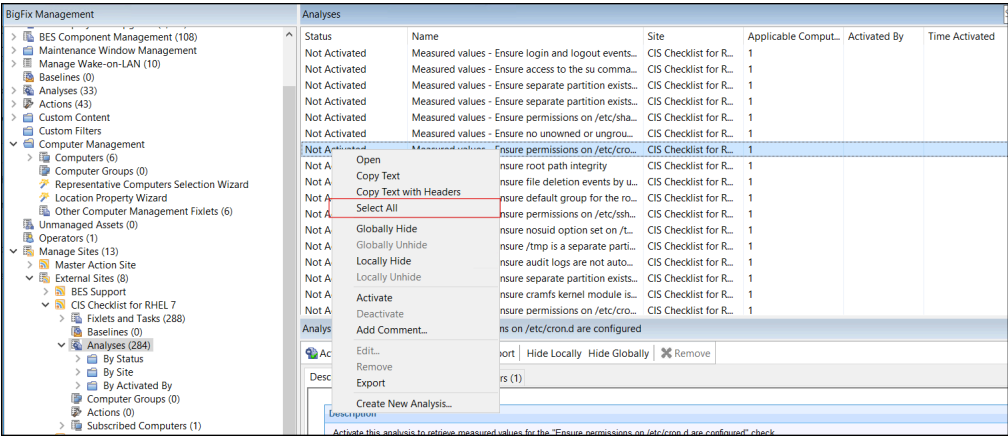
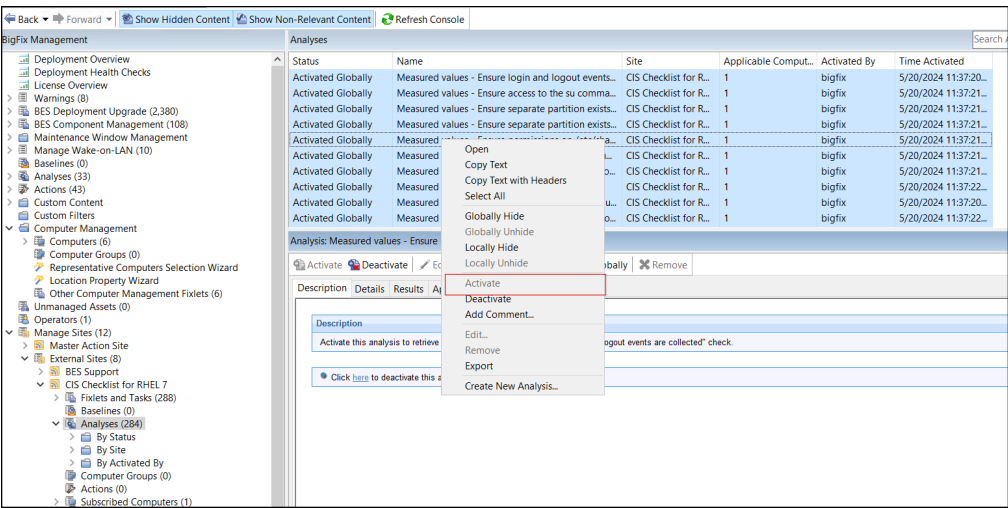


Figure 23. Analyses



Using checks and checklists

The check Fixlets in Configuration Management checklists evaluate an endpoint against a defined configuration standard. Many of these check Fixlets have a corresponding analysis, often referred to as "measured values", which reports the value of the element being assessed by the check Fixlet.

Viewing check Fixlets from the HCL BigFix console

A check Fixlet becomes relevant when a client computer is out of compliance with a configuration standard. By reviewing the **Configuration Management Fixlets**, Console Operators can identify non-compliant computers and the corresponding standards.

To access the check Fixlets, subscribe to the **Linux Checklist Fixlet sites**.

Steps to view the check Fixlets in the HCL BigFix Console:

1. From the **Security Configuration** domain, navigate to **All Security Configuration > Sites > External Sites**.
2. Expand the checklist you want to view.
3. Click **Fixlets and Tasks** to open the Fixlets and Tasks section.
4. Click on one of the Fixlets displayed in the list.

The Fixlet opens with the following tabs: **Description**, **Details**, **Applicable Computers**, and **Action History**.

5. Click the **Description** tab to view details about the Fixlet.

The Fixlet applies to a subset of endpoints on your network, and the size of that subset is shown in the **Applicable Computers** tab.

The description typically includes information about the check, the rationale, and guidelines for remediation actions. If the Fixlet is relevant, you need to take action listed in the **Remediation** section of the description to address non-compliance. You can also access the associated analysis from this tab.



Note: The **Check ID** refers to the **Source ID** of the Fixlet.

6. If the checklist includes **Deploy and Run**, execute the **Deploy and Run Task**.



Note: Run the **Deploy and Run Task** periodically to collect the latest results. For more information about this task, refer to **Configuring Endpoints**.

Chapter 5. Configuring Middleware Checklists

The Configuration Management checklists for Middleware systems are delivered as a set of Fixlet and tasks that can help you find the information you need to manage your deployment.

These checklists assist system administrators and IT professionals in managing and configuring Middleware systems efficiently within their environment.

The checklists usually include a series of actions or tasks that focus on important areas like system configuration, security, and compliance. The main goal is to ensure all systems are properly set up, secure, and meet organizational or industry standards.

Overview

Learn about concepts and the work process in Middleware checklists.

You can configure the Middleware checklists for the Databases and Webservers, including MSSQL, Oracle DB, IBM DB2, Apache HTTP Server, Apache Tomcat Server, MS IIS, and Oracle MySQL etc.

The Middleware checklists in BigFix effectively meet the requirements outlined in the CIS and DISA checklists, with a strong focus on compliance monitoring procedures.

Most Middleware checks come with built-in remediation. However, some allow you to audit non-default values. If a middleware check can be customized, you will see one or more input fields on the **Description tab** of the Fixlet®. To customize, simply change the field to match the value you want to audit and click the Apply button.

What's new in Middleware checklist

HCL BigFix Compliance Middleware checklist provides additional support and enhancement in the recent update.

Several checklists have been improved with new features, such as:

- Support for multiple instances, pools, and sites in all checklists.
- Ability to scan the endpoint as a user other than `NT Authority\SYSTEM` in the MSSQL checklist.
- Failover cluster support for MSSQL 2016, 2019, and 2022 checklists.
- Always On Availability Groups (AAG) support for MSSQL 2019 and 2022.
- Option to scan the endpoint using Oracle Wallet in Oracle checklists.
- Optimized code and improved performance for IBM DB2 checklists.
- Released new checklist for Oracle MySQL.

For a detailed list of releases, see the [Middleware Checklist Release Notes](#).

Available Middleware checklist

Middleware checklists are commonly used to ensure systems are secure, optimized, and compliant with best practices.

Below are the Middleware checklists available in the License dashboard:

Table 7. Middleware checklist

CIS Checklists	DISA STIG Checklists
Apache HTTP Server	Apache HTTP Server
Apache Tomcat Server	Apache Tomcat Server
MS IIS 10	MS IIS 10
IBM DB2 10	Oracle DB
Oracle DB	MS SQL Server
MS SQL Server	
Oracle MySQL	

To get more details of the Middleware checklist, refer to the [Middleware Checklist](#).

Setup and configuration

Create custom copies of the Middleware checklist content if you want to modify the checks based on a specific corporate policy. You can manually create a custom site to host the Middleware checklists or use the Create Custom Checklist wizard to create copies of the Middleware checklists and save them in a custom site.

You must subscribe to the SCM Reporting external site.

You can use custom checklists to fine-tune your ability to customize Configuration Management parameters, which gives you control over your security status. Custom checklists target specific sets of computers with tailored content using the subscription mechanism. This allows statistics to be gathered with finer granularity. For more information, see [Modifying check parameters \(on page 65\)](#).

Setting up your Configuration Management checklist for Middleware Checklist involves two basic steps:

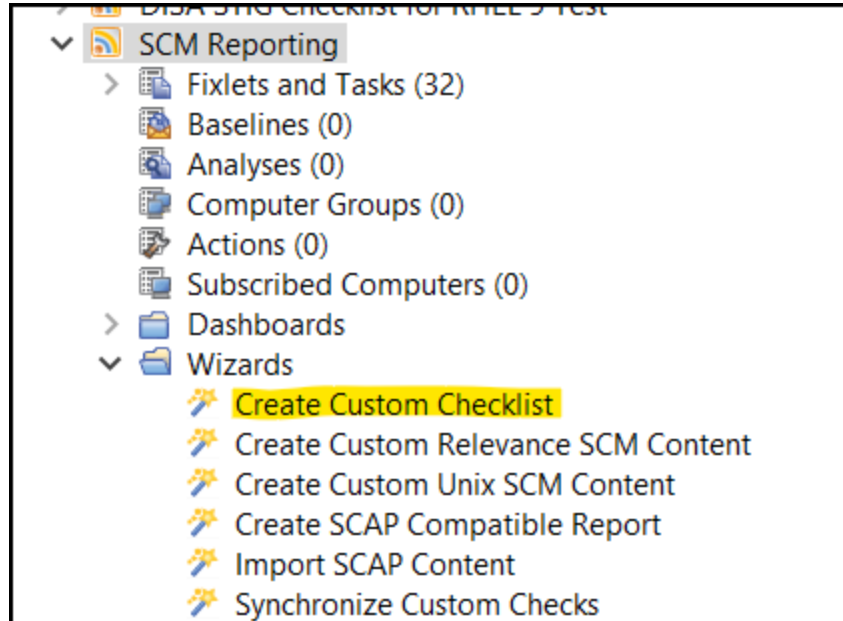
Create your checklist

- Creating custom checklist by using the **Create Custom Checklist** wizard:
 1. From the Security Configuration Domain, go to **Configuration Management > Checklist Tools > Create Custom Checklist**.
 2. Enter the name of the new checklist.
 3. Select the target platform.
 4. Click the drop-down menu to select which external checklist you copy the checks from. As you select the checks, they are shown in the staged list at the lower part of the window.
 5. Click the **Activate Measured Value analyses after copying** check box to activate all analyses that were copied.
 6. Click **Create Checklist**.

The console begins copying the checks in the selected lists into your new custom checklist. The process might take several minutes, depending on the number and size of the checklists selected.

Use the **Create Custom Checklist** wizard located in the **SCM Reporting** site under the wizard section.

Figure 24. Create custom checklist



- Creating custom checklists manually:

1. Select **Tools > Create Custom Site**.
2. You are prompted for a name for your custom site. Enter a name and click **OK**.
3. From the Domain panel, find your site under **Sites > Custom** and click it to describe your site.
From the **Details** tab, enter a description of your site. From the **Domain** pull-down menu, select a Domain to house your site.
4. From the **Computer Subscriptions** tab, indicate which subset of your BigFix client computers you want to subscribe to this site.
5. From the **Operator Permissions** tab, you can grant specific access permissions to specific operators.
6. Click the **Save Changes** button above the work area to complete the description of your site. You must enter your password to propagate your new custom site.

Subscribe computers to the custom checklist.



Note: Custom checklists do not support site relevance, so take extra precaution when you subscribe computers to custom checklists.



Figure 25. Create custom checklist

Create Custom Checklist

This wizard will assist you in creating a new custom checklist based on one or more of your currently subscribed external checklists.

New checklist name: 4 characters remaining (69 checks selected out of 69 displayed)

Select target platform:

- ☒ Apache Server 2.2 & 2.4 Linux
- ☐ MS SQL Server 2016
- ☐ Oracle 19c Linux
- ☐ Solaris 11.4
- ☐ All Others

External checklist to copy checks from: Search

Check Name	Source ID	Source Severity	Source Checklist
<input checked="" type="checkbox"/> Ensure the Log Config Module Is Enabled	cis-Apache2.4-2.2	Level 1	CIS Checklist for Apache Server 2_4 on Linux
<input checked="" type="checkbox"/> Ensure the WebDAV Modules Are Disabled	cis-Apache2.4-2.3	Level 1	CIS Checklist for Apache Server 2_4 on Linux
<input checked="" type="checkbox"/> Ensure the Status Module Is Disabled	cis-Apache2.4-2.4	Level 1	CIS Checklist for Apache Server 2_4 on Linux
<input checked="" type="checkbox"/> Ensure the Autoindex Module Is Disabled	cis-Apache2.4-2.5	Level 1	CIS Checklist for Apache Server 2_4 on Linux
<input checked="" type="checkbox"/> Ensure the Proxy Modules Are Disabled if not in use	cis-Apache2.4-2.6	Level 1	CIS Checklist for Apache Server 2_4 on Linux
<input checked="" type="checkbox"/> Ensure the User Directories Module Is Disabled	cis-Apache2.4-2.7	Level 1	CIS Checklist for Apache Server 2_4 on Linux
<input checked="" type="checkbox"/> Ensure the Info Module Is Disabled	cis-Apache2.4-2.8	Level 1	CIS Checklist for Apache Server 2_4 on Linux
<input checked="" type="checkbox"/> Ensure the Basic and Digest Authentication Modules Are Enabled	cis-Apache2.4-2.9	Level 1	CIS Checklist for Apache Server 2_4 on Linux
<input checked="" type="checkbox"/> Ensure the Apache Web Server Runs As a Non-Root User	cis-Apache2.4-3.1	Level 1	CIS Checklist for Apache Server 2_4 on Linux

Staged List: The following checks will be copied to your new checklist (including any necessary measured value analyses and/or applicability fidelets):

Check Name	Source ID	Source Severity	Source Checklist
<input checked="" type="checkbox"/> Ensure the Log Config Module Is Enabled	cis-Apache2.4-2.2	Level 1	CIS Checklist for Apache Server 2_4 on Linux
<input checked="" type="checkbox"/> Ensure the WebDAV Modules Are Disabled	cis-Apache2.4-2.3	Level 1	CIS Checklist for Apache Server 2_4 on Linux
<input checked="" type="checkbox"/> Ensure the Status Module Is Disabled	cis-Apache2.4-2.4	Level 1	CIS Checklist for Apache Server 2_4 on Linux
<input checked="" type="checkbox"/> Ensure the Autoindex Module Is Disabled	cis-Apache2.4-2.5	Level 1	CIS Checklist for Apache Server 2_4 on Linux
<input checked="" type="checkbox"/> Ensure the Proxy Modules Are Disabled if not in use	cis-Apache2.4-2.6	Level 1	CIS Checklist for Apache Server 2_4 on Linux
<input checked="" type="checkbox"/> Ensure the User Directories Module Is Disabled	cis-Apache2.4-2.7	Level 1	CIS Checklist for Apache Server 2_4 on Linux
<input checked="" type="checkbox"/> Ensure the Info Module Is Disabled	cis-Apache2.4-2.8	Level 1	CIS Checklist for Apache Server 2_4 on Linux
<input checked="" type="checkbox"/> Ensure the Basic and Digest Authentication Modules Are Enabled	cis-Apache2.4-2.9	Level 1	CIS Checklist for Apache Server 2_4 on Linux
<input checked="" type="checkbox"/> Ensure the Apache Web Server Runs As a Non-Root User	cis-Apache2.4-3.1	Level 1	CIS Checklist for Apache Server 2_4 on Linux

69 total checks will be copied to the new checklist

Activate Measured Value analyses after copying ☐ Create Checklist

- Run or Schedule your checklist:

1. Schedule or run the **Environment Setup Task**. Select the **Environment Setup Task** and click the **Take Action** button.
2. Enter the credentials or required details in the pop-up, if prompted.
3. Choose the target computer or group of computers from the target section.
4. Set up the execution criteria based on your environment and click **OK** to schedule or set up the **Environment Setup Task**.



Note: To get more details about the **Environment Setup Task**, see [Environment Setup Task \(on page 54\)](#) section.

Middleware checklist components

The Middleware checklist components ensure that the system is systematically reviewed and remains operational, secure, and compliant.

Environment Setup Task

The Environment Setup Task is a crucial component of middleware checklists. It plays a key role in determining the compliance status of each check in the checklist.

Under normal conditions, once an endpoint subscribes to the site, the **Environment Setup Task** becomes relevant, enabling you to click **Take Action**. When executed, this task downloads the `sqlite_detect.db` file from an external site, which contains all the available detection scripts. Using relevance, the task identifies and extracts the scripts corresponding to the checks available in the current site. These scripts are then copied to the SCM folder and executed sequentially.

During execution, individual logs are generated in the **Logs** directory, while the results are saved in the **Results** folder. Additionally, a comprehensive log file, **Environment_Setup_Task.log**, is created to record all execution details.

Figure 26. Environment Setup Task

Fixlets and Tasks

Source ID	Name
	Applicability Fixlet - CIS Apache HTTP Server 2.4 - All levels
	Applicability Fixlet - CIS Apache HTTP Server 2.4 - Level 1
	Environment Setup Task
cis-10.1	Ensure the LimitRequestLine directive is Set to 8190 or less

<

Task: Environment Setup Task

Take Action | Edit | Copy | Export | Hide Locally | Hide Globally | Remove

Description | Details | Applicable Computers (0) | Action History (0)

Description

This task downloads the `sqlite_detect.db` file from the external site, which contains all the available detect scripts. Relevance is then used to identify checks available in the current site. These scripts are subsequently copied to the SCM folder and executed sequentially.

This task will dynamically scan all Apache HTTPD instances on the endpoint, ensuring comprehensive monitoring and management.

It will populate the necessary properties on the endpoint which will be read by the fixlets of this site for relevance evaluation.

☐ Exclude **Level 2** benchmarks.

Actions

Click [here](#) to deploy this action.

The check Fixlets from the site will display the latest results only after the **Environment Setup Task** is completed.

To ensure regular compliance validation, schedule periodic executions of the Environment Setup Task.

Schedule periodic executions of the Environment Setup task

This means automating the task at regular intervals to continuously validate and update the compliance status of endpoints. This ensures that compliance checks are consistently performed, logs and results remain up to date, and any deviations or non-compliance issues are promptly identified and addressed.

1. From the Security Configuration Domain, go to **All Security Configuration > Sites > External sites**.

Figure 27. Environment Setup Task in CIS Checklist for Apache Server 2_4 on Linux

Fixlets and Tasks	
Source ID ^	Name
	Applicability Fixlet - CIS Apache HTTP Server 2.4 - All levels
	Applicability Fixlet - CIS Apache HTTP Server 2.4 - Level 1
	Environment Setup Task
cis-10.1	Ensure the LimitRequestLine directive is Set to 8190 or less
<	
Task: Environment Setup Task	
Take Action Edit Copy Export Hide Locally Hide Globally Remove	
Description	Details Applicable Computers (0) Action History (0)
<p>Description</p> <p>This task downloads the sqlite_detect.db file from the external site, which contains all the available detect scripts. Relevance is then used to identify checks available in the current site. These scripts are subsequently copied to the SCM folder and executed sequentially.</p> <p>This task will dynamically scan all Apache HTTPD instances on the endpoint, ensuring comprehensive monitoring and management.</p> <p>It will populate the necessary properties on the endpoint which will be read by the fixlets of this site for relevance evaluation.</p> <p><input type="checkbox"/> Exclude Level 2 benchmarks.</p>	
<p>Actions</p> <p> Click here to deploy this action.</p>	

2. Select a checklist and click **Fixlets and Tasks**.
3. In the **List** panel, find and select the **Environment Setup Task**.
4. Click **Take Action** on the **Environment Setup Task**.
5. Choose the appropriate endpoints in your environment.
6. Click the **Execution** tab.

Figure 28. Take Action - Execution tab

Take Action

Name: Create in domain:

Preset: ☐ Show only personal presets

Target Execution Users Messages Offer Post-Action Applicability Success Criteria Action Script

Constraints

☐ Starts on at

☒ Ends on at

☐ Run between and

☐ Run only on

☐ Run only when

Behavior

☐ On failure, retry times

☒ Wait between attempts

☐ Wait until computer has rebooted

☐ Reapply this action

☒ whenever it becomes relevant again

☐ while relevant, waiting between reapplications

☒ Limit to reapplications

☐ Start client downloads before constraints are satisfied

☐ Stagger action start times over minutes to reduce network load

7. Configure the **Environment Setup Task** to run as needed, and click **OK**.

Understanding the output of Environment Setup task

With Middleware content, endpoint scans are accomplished using a series of shell or Powershell scripts, that provide greater accessibility to system administrators.

In most BigFix content, Fixlets continuously evaluate conditions on each endpoint. The console shows the results when the relevance clause of the Fixlet evaluates to **true** or **false**. However, for Middleware content, an **Environment Setup Task** triggers a scan of the endpoints. This task can be executed on-demand whenever a scan is needed or scheduled as a recurring policy from the console.

The endpoint scan is performed using a series of Shell/Powershell scripts available within individual checks or Fixlets. These scripts write collected data to **individual Result files**, which are then accessed by the corresponding Fixlet checks for evaluation. Once the results files are written to disk, the Fixlets read each results file and show the results in the console.

After running the **Environment Setup Task** from the Security Checklist, the scripts execute and generate multiple files for each check, including a script file, a log file, and a result file:

Table 8. File paths for Logs and results

File Name	Path in Windows	Path in Linux	Content
Environment_Setup_-Task.log	C:\Program Files (x86)\Big-Fix Enterprise\BES Client\SCM\<ProjectID>\<CIS/DISA>\	/var/opt/BESClient/SCM/<ProjectID>/<CIS/DISA>/	Execution details of Task and individual checks.
<sourceID.log>	C:\Program Files (x86)\Big-Fix Enterprise\BES Client\SCM\<ProjectID>\<CIS/DISA>\Logs	/var/opt/BESClient/SCM/<ProjectID>/<CIS/DISA>/Logs	Logs for execution of particular fixlet/Check
<sourceID.Result>	C:\Program Files (x86)\Big-Fix Enterprise\BES Client\SCM\<ProjectID>\<CIS/DISA>\Results	/var/opt/BESClient/SCM/<ProjectID>/<CIS/DISA>/Results	Compliance status of particular fixlet/Check
<sourceID.sh/ps1>	C:\Program Files (x86)\Big-Fix Enterprise\BES Client\SCM\<ProjectID>\<CIS/DISA>\Scripts	/var/opt/BESClient/SCM/<ProjectID>/<CIS/DISA>/Scripts	Individual scripts for all the checks in the site



Note: Depending on your checklist, separate folders are available for each instance under Logs and Results.



Note: If an individual Fixlet contains a parameter, then it will be added in a file named `Parameter.txt`, which is then stored in the `custom site folder`.

Environment Setup task options depend on checklist

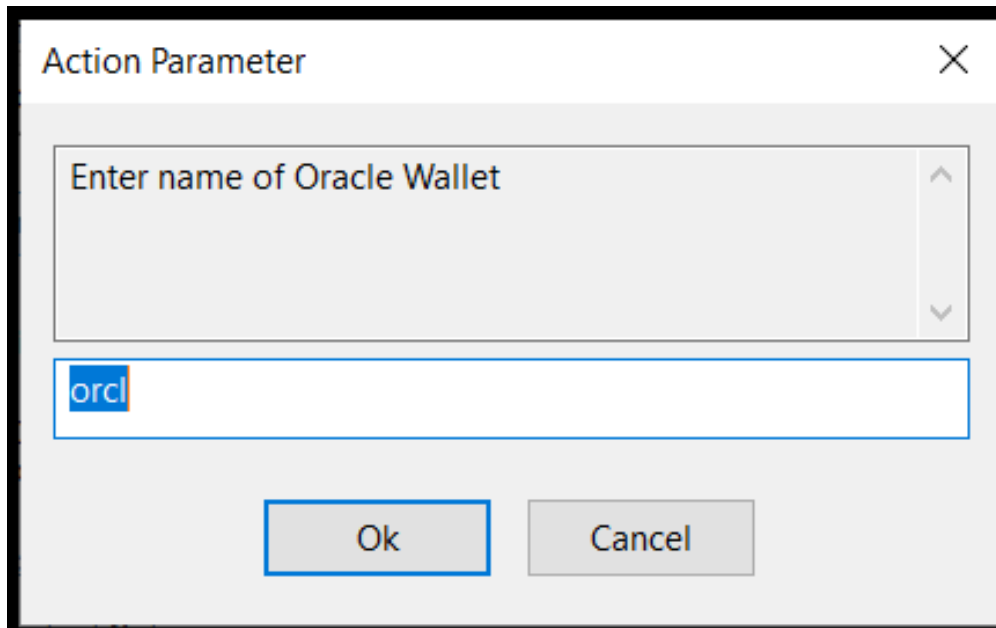
This means that the available configurations and execution parameters of the **Environment Setup Task** vary based on the specific compliance checklist being used.

Oracle Checklist

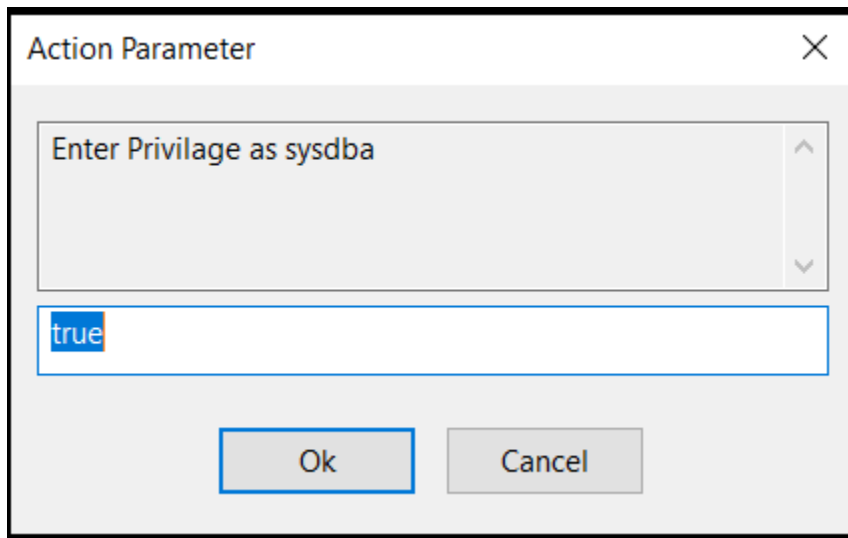
This Oracle checklist includes two different Environment Setup Tasks.

1. Environment Setup Task(OracleWallet)
 - Run Environment Setup Task using oracle wallet
 - Pop up will be coming to enter wallet name and privilege
 - scan all available databases which is having same wallet name

Figure 29. Action Parameter



The dialog box is titled "Action Parameter" and has a close button (X) in the top right corner. It contains a large text area with the prompt "Enter name of Oracle Wallet". Below this is a text input field containing the text "orcl". At the bottom of the dialog are two buttons: "Ok" and "Cancel".



The dialog box is titled "Action Parameter" and has a close button (X) in the top right corner. It contains a large text area with the prompt "Enter Privilage as sysdba". Below this is a text input field containing the text "true". At the bottom of the dialog are two buttons: "Ok" and "Cancel".

2. Environment Setup Task (Username/Password)

- You have to enter credentials before taking the action
- You can add multiple databases and credentials

Figure 30. Credential page in Oracle traditional Environmental Setup task

Environment Setup Task(Username/Password)

Task: Environment Setup Task(Username/Password)

Take Action Edit Copy Export Hide Locally Hide Globally Remove

Description Details Applicable Computers (0) Action History (0)

Environment Setup Task(Username/Password)

Application version Supported: Oracle Database version 19c
Operating System Platform: Red Hat Enterprise Linux 7 | 8, SUSE Linux Enterprise Server 12 | 15, and Oracle Linux 7 | 8

Important Notes:

- You must fill all the input fields in order to take an action.
- Because of the way secure parameters work, you cannot use this task in a baseline, target an action dynamically by property (e.g., automatic groups), or add additional actions.
- Run this task periodically to get the latest compliance reports.

Database Instance Name:

Database User:

Database Password:

ORACLE_HOME path:

FIPS_HOME path:

☐ Run AS SYSDBA

Add New Database Instance

MSSQL Checklist

In the MSSQL Checklist, there is a single Environment Setup Task with multiple execution options:

Option 1: Run as NT Authority\System

Executes the Environment Setup Task using the default BigFix user, ensuring it has the minimum required permissions specified in the checklist for successful execution.

Option 2: Run as Windows Use

Runs the Environment Setup Task as a custom Windows user with the necessary permissions for both Windows OS and SQL, as outlined in the checklist.

Figure 31. Environment Setup task in MSSQL

Environment Setup Task

V-213900 SQL Server databases must integrate with an organization-level authentication/access mechanism providing account r

V-213902 SQL Server must protect against a user falsely repudiating by ensuring only clearly unique Active Directory user account

Task: Environment Setup Task

Take Action Edit Copy Export Hide Locally Hide Globally Remove

Click here to deploy this action as NT Authority/System.

Click here to deploy this action as Windows user.

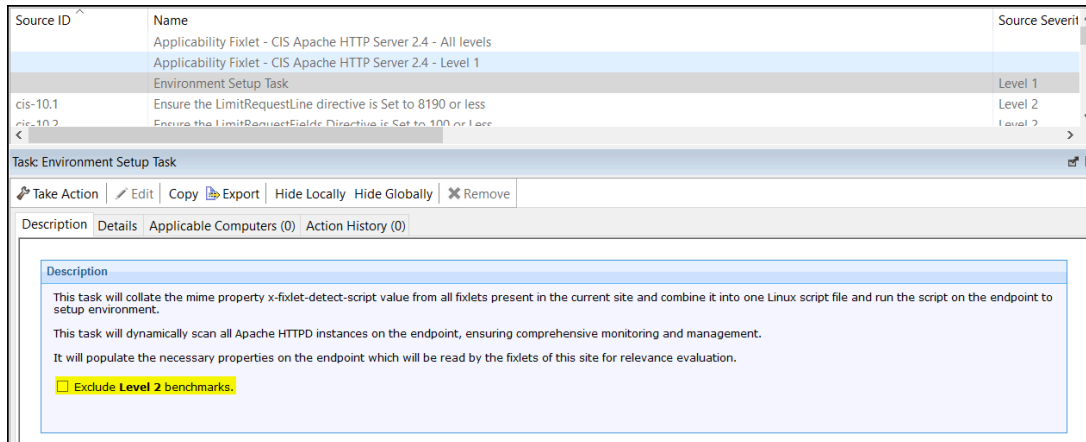
Description

It will populate the necessary properties on the endpoint which will be read by the fixlets of this site for relevance evaluation.

Apache Checklist

In the CIS Apache checklists, a checkbox is available to exclude Level 2 checks. If selected, the Environment Setup Task will execute only Level 1 checks.

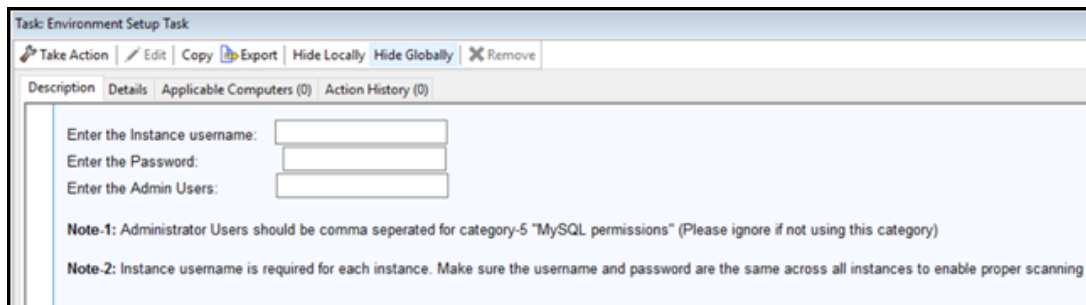
Figure 32. Environment Setup task in CIS Apache Checklist



Oracle MySQL Checklist

For this environment setup task, provide a single username and password for all MySQL instances. The system will use this same set of credentials to scan each instance in the series. In a separate field, enter a list of administrator usernames, separated by commas. This list is only for the Category 5 series.

Figure 33. Environment Setup task in Oracle MySQL Checklist



Applicability Fixlets

Learn about concepts and the work process in Configuration Management.

Each Middleware checklist includes Applicability Fixlets based on the checklist requirements. For example, in the **CIS Checklist for Apache Server 2.4 on Linux**, the following Applicability Fixlets are available:

1. Applicability Fixlet - CIS Apache HTTP Server 2.4 - All Levels
2. Applicability Fixlet - CIS Apache HTTP Server 2.4 - Level 1

These Fixlets work with HCL BigFix Compliance to determine whether endpoints subscribed to the checklist meet the required conditions. A Fixlet is relevant only for applicable endpoints and remains irrelevant otherwise. To optimize performance, site subscriptions should be limited to applicable endpoints.



Note: The number of Applicability Fixlets may vary depending on checklist requirements.

Fixlets with remediation action on applicability Fixlets

The Omit List in applicability Fixlets is a predefined list of checks that are excluded from the evaluation process.

In the **Applicability Fixlet - CIS Apache HTTP Server 2.4 - All Levels**, we specify the Fixlets that include remediation actions.

Figure 34. List of Checks containing an action for remediation

Description	
Applicability Fixlet - CIS Apache HTTP Server 2.4 Linux	
<p>This fixlet is used in connection with HCL BigFix Compliance to determine whether endpoints subscribed to the current checklist meet the following condition:</p> <ul style="list-style-type: none"> ● Operating System Platform: Red Hat Enterprise Linux 6 7 8 9 and CentOS 6 7 8 ● Applicability Profile: Apache HTTP Server 2.4 ● Benchmark severity: Level 1 ● Environment Setup Task has been run periodically. (at least 90 days) <p>Effort should be made to limit site subscription to applicable endpoints. There may be nearly identical applicability fixlets included within a checklist in cases where the conditions for applicability are related but different.</p>	
Fixlets with Remediation Actions	
Source ID	Fixlet Name
cis-3.2	Ensure the Apache User Account Has an Invalid Shell
cis-3.3	Ensure the Apache User Account Is Locked
cis-3.4	Ensure Apache Directories and Files Are Owned By Root
cis-3.5	Ensure the Group Is Set Correctly on Apache Directories and Files
cis-3.6	Ensure Other Write Access on Apache Directories and Files Is Restricted
cis-3.7	Ensure the Core Dump Directory Is Secured
cis-3.11	Ensure Group Write Access for the Apache Directories and Files Is Properly Restricted
cis-3.12	Ensure Group Write Access for the Document Root Directories and Files Is Properly Restricted
cis-5.6	Ensure the Default CGI Content test-cgi Script Is Removed
cis-11.3	Ensure the httpd.t Type Is Not in Permissive Mode

Omit List in applicability Fixlets

The Omit List in applicability Fixlets is a predefined list of checks that are excluded from the evaluation process.

In the **Applicability Fixlet - CIS Apache HTTP Server 2.4 - All Levels**, we include the Omit List, which specifies checks that are not supported from the benchmark. These omitted checks typically require human interaction or have technical limitations that prevent automated evaluation.

Figure 35. Omit list from the CIS Checklist for Apache Server 2_4 on Linux

Take Action
Edit
Copy
Export
Hide Locally
Hide Globally
Remove

Description
Details
Applicable Computers (1)
Action History (0)

Description

Applicability Fixlet - CIS Apache HTTP Server 2.4 Linux

This fixlet is used in connection with HCL BigFix Compliance to determine whether endpoints subscribed to the current checklist meet the following condition:

- **Operating System Platform:** Red Hat Enterprise Linux 6 | 7 | 8 | 9 and CentOS 6 | 7 | 8
- **Applicability Profile:** Apache HTTP Server 2.4
- **Benchmark severity:** Level 1
- **Environment Setup Task has been run periodically. (at least 90 days)**

Effort should be made to limit site subscription to applicable endpoints.
There may be nearly identical applicability fixlets included within a checklist in cases where the conditions for applicability are related but different.

Fixlets with Remediation Actions

Source ID	Fixlet Name
cis-3.2	Ensure the Apache User Account Has an Invalid Shell
cis-3.3	Ensure the Apache User Account Is Locked
cis-3.4	Ensure Apache Directories and Files Are Owned By Root
cis-3.5	Ensure the Group Is Set Correctly on Apache Directories and Files
cis-3.6	Ensure Other Write Access on Apache Directories and Files Is Restricted
cis-3.7	Ensure the Core Dump Directory Is Secured
cis-3.11	Ensure Group Write Access for the Apache Directories and Files Is Properly Restricted
cis-3.12	Ensure Group Write Access for the Document Root Directories and Files Is Properly Restricted
cis-5.6	Ensure the Default CGI Content test-cgi Script Is Removed
cis-11.3	Ensure the httpd_t Type is Not in Permissive Mode

Checks not supported from CIS Checklist Apache2.4 on Linux in this site.

List of checks not supported from CIS Checklist for Apache2.4 on Linux due to the requirement of human interaction / technical limitations.

Total number of checks: 87
Checks supported: 69
Checks not supported: 18

Benchmark file check No.	Reason
1.1	Manual Intervention required
1.2	Manual Intervention required
1.3	Manual Intervention required

Activate Windows
Go to Settings to activate Windows.

Remediation

Most Middleware checks include built-in remediation capabilities. However, a smaller subset of Middleware audit checks allows customization to audit a non-default value.

If a Middleware audit check supports customization, the **Description tab** of the Fixlet will contain **one or more input fields** for user-defined values.

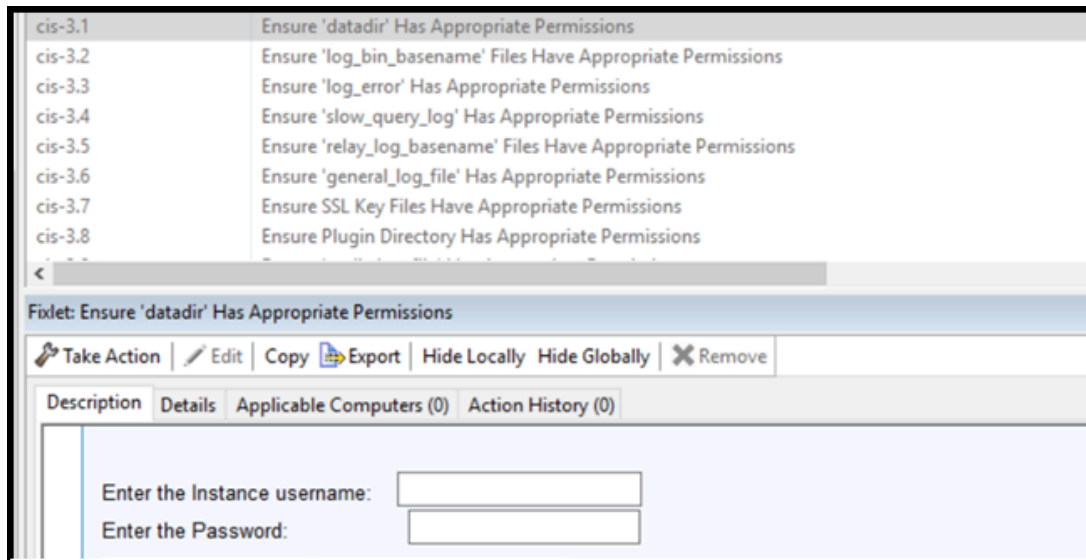
Remediating configuration settings

Middleware checklists support remediation, allowing console operators to resolve vulnerabilities with a single action. A remediation action can only be executed on an endpoint where the Fixlet is relevant.

You can audit, assess, and remediate configuration settings using **Security and Compliance Analytics (SCA)**, now known as **BigFix Compliance Analytics**. For Fixlet checks that support automatic remediation, an **action button** appears within the relevant Fixlet. Remediation actions can only be applied to relevant and selected endpoints.

Oracle MySQL Checklist - Provide a single username and password that will be used for every instance to remediate

Figure 36. Oracle MySQL Checklist for remediation



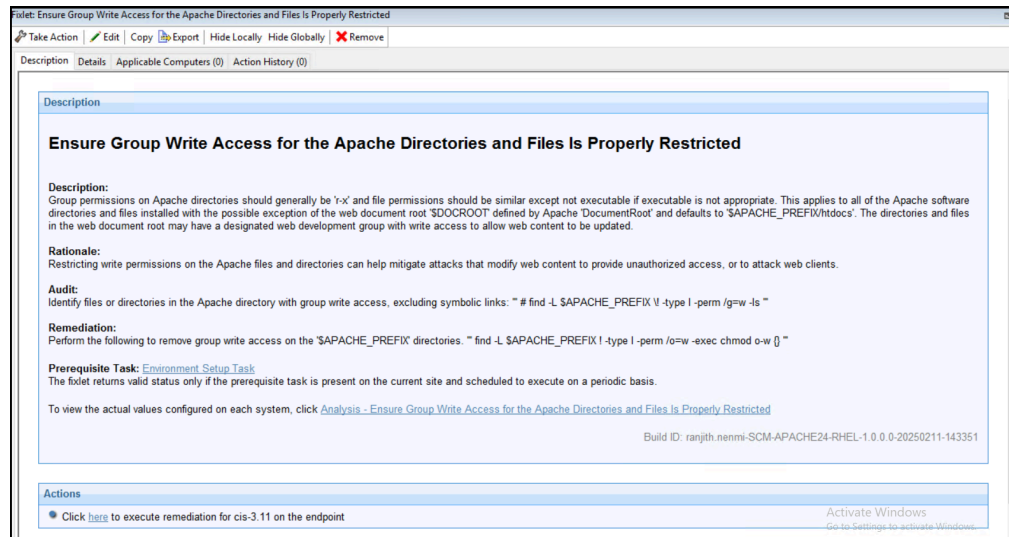
Note: Not all Fixlets include a remediation action.



Note: If an external global policy is enabled, any local endpoint changes will be overwritten. In such cases, remediation must be performed using the external global policy solution.

1. Navigate to the **Security Configuration Domain > All Security Configuration > Fixlets and Tasks**.
2. Expand the sub-folders to locate the desired Fixlet.
3. Open the Fixlet, click the **Description** tab, and scroll down to the **Actions** box.
4. Click the link in the **Actions** box to remediate the specified policy issue.

Figure 37. Check containing an action for remediation




5. Set your parameters in the **Take Action** dialog and click **OK**.


Modifying check parameters


In addition to monitoring compliance status and remediating non-compliant settings, you can modify configuration settings to align with your organization's policies.

To adjust the desired value of a check parameter in the Fixlet check description, you must first create a custom site. For details on custom sites, refer to [Creating Custom Checklists](#). Since parameters are stored as site settings, the same check can be parameterized differently across sites containing a copy of the check.

 **Note:** Not all checks in custom sites can be parameterized.

Certain Fixlet checks allow you to specify a more restrictive value than the default specified by the Middleware checklist, providing greater flexibility to customize security policies to meet the specific requirements.

 **Important:** Custom parameterization may take a few minutes to process. Allow sufficient time between updating a parameter and executing the **Environment Setup Task** for optimal results.

 **Note:** Parameter changes will only take effect after running the **Environment Setup Task**. For more details, see [Configuring Endpoints](#).

1. Open the Fixlet check and navigate to the **Description** tab.
2. Scroll down to the **Parameters** section and enter the desired value.

Figure 38. Setting up Parameterization for Fixlets



3. Click **Apply**.
4. Execute the **Environment Setup Task**.

Measured Value Analysis

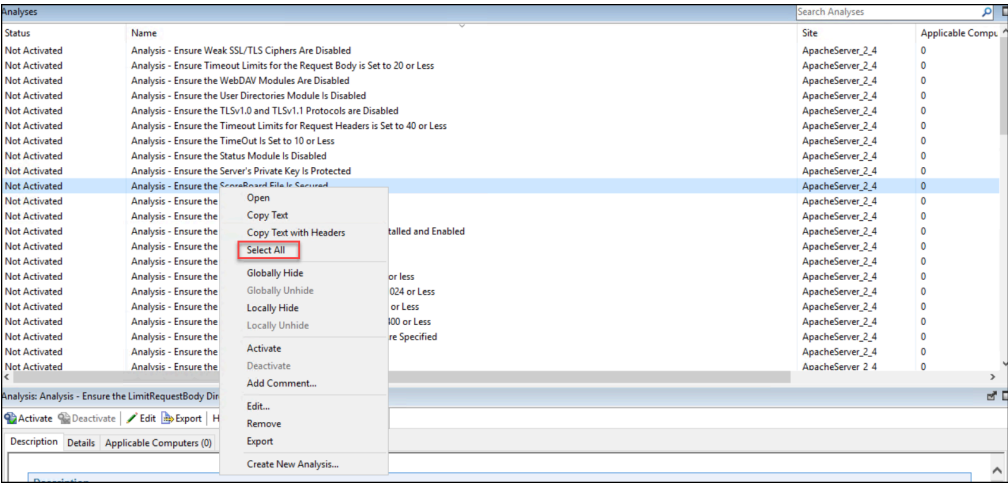
Many check Fixlets have a corresponding analysis, often referred to as "measured values", which report the value of the element being evaluated by the check Fixlet.

Each computer reports its properties and analysis values, including active check measured values in your deployment. These results are aggregated by the BigFix Compliance Analytics server and enhanced with computer properties and analysis values, providing both compliance overviews and detailed result lists.

Steps to activate measured values:

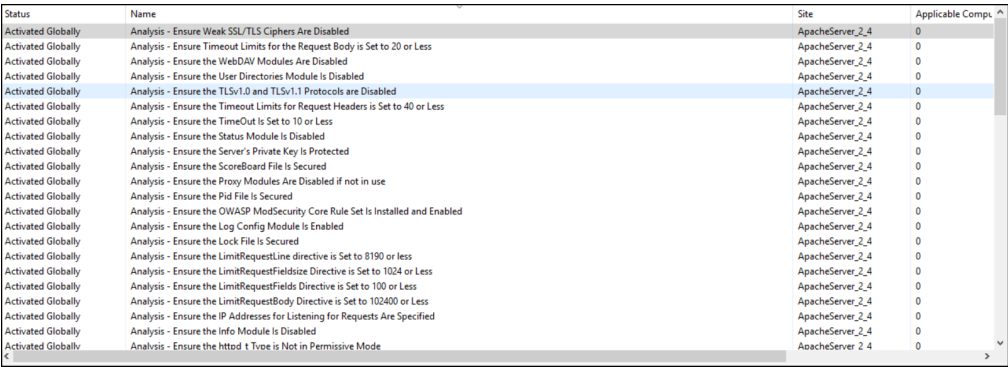
- Expand the checklist.
- Navigate to the **Analysis** section.
- In the right-hand panel, select all the analyses.
- Right-click and select **Activate Analysis**.

Figure 39. Non-Activated Measured Value Analyses



Status	Name	Site	Applicable Comp.
Not Activated	Analysis - Ensure Weak SSL/TLS Ciphers Are Disabled	ApacheServer_2_4	0
Not Activated	Analysis - Ensure Timeout Limits for the Request Body is Set to 20 or Less	ApacheServer_2_4	0
Not Activated	Analysis - Ensure the WebDAV Modules Are Disabled	ApacheServer_2_4	0
Not Activated	Analysis - Ensure the User Directories Module Is Disabled	ApacheServer_2_4	0
Not Activated	Analysis - Ensure the TLSv1.0 and TLSv1.1 Protocols are Disabled	ApacheServer_2_4	0
Not Activated	Analysis - Ensure the Timeout Limits for Request Headers is Set to 40 or Less	ApacheServer_2_4	0
Not Activated	Analysis - Ensure the TimeOut Is Set to 10 or Less	ApacheServer_2_4	0
Not Activated	Analysis - Ensure the Status Module Is Disabled	ApacheServer_2_4	0
Not Activated	Analysis - Ensure the Server's Private Key is Protected	ApacheServer_2_4	0
Not Activated	Analysis - Ensure the ScoreBoard File is Secured	ApacheServer_2_4	0
Not Activated	Analysis - Ensure the Proxy Modules Are Disabled if not in use	ApacheServer_2_4	0
Not Activated	Analysis - Ensure the Pid File is Secured	ApacheServer_2_4	0
Not Activated	Analysis - Ensure the OWASP ModSecurity Core Rule Set is Installed and Enabled	ApacheServer_2_4	0
Not Activated	Analysis - Ensure the Log Config Module is Enabled	ApacheServer_2_4	0
Not Activated	Analysis - Ensure the Lock File is Secured	ApacheServer_2_4	0
Not Activated	Analysis - Ensure the LimitRequestLine directive is Set to 8190 or less	ApacheServer_2_4	0
Not Activated	Analysis - Ensure the LimitRequestFields directive is Set to 1024 or Less	ApacheServer_2_4	0
Not Activated	Analysis - Ensure the LimitRequestFields directive is Set to 100 or Less	ApacheServer_2_4	0
Not Activated	Analysis - Ensure the LimitRequestBody Directive is Set to 102400 or Less	ApacheServer_2_4	0
Not Activated	Analysis - Ensure the IP Addresses for Listening for Requests Are Specified	ApacheServer_2_4	0
Not Activated	Analysis - Ensure the Info Module Is Disabled	ApacheServer_2_4	0
Not Activated	Analysis - Ensure the httpd t Type is Not in Permissive Mode	ApacheServer_2_4	0

Figure 40. Activated Measured Value Analyse



Status	Name	Site	Applicable Comp.
Activated Globally	Analysis - Ensure Weak SSL/TLS Ciphers Are Disabled	ApacheServer_2_4	0
Activated Globally	Analysis - Ensure Timeout Limits for the Request Body is Set to 20 or Less	ApacheServer_2_4	0
Activated Globally	Analysis - Ensure the WebDAV Modules Are Disabled	ApacheServer_2_4	0
Activated Globally	Analysis - Ensure the User Directories Module Is Disabled	ApacheServer_2_4	0
Activated Globally	Analysis - Ensure the TLSv1.0 and TLSv1.1 Protocols are Disabled	ApacheServer_2_4	0
Activated Globally	Analysis - Ensure the Timeout Limits for Request Headers is Set to 40 or Less	ApacheServer_2_4	0
Activated Globally	Analysis - Ensure the TimeOut Is Set to 10 or Less	ApacheServer_2_4	0
Activated Globally	Analysis - Ensure the Status Module Is Disabled	ApacheServer_2_4	0
Activated Globally	Analysis - Ensure the Server's Private Key is Protected	ApacheServer_2_4	0
Activated Globally	Analysis - Ensure the ScoreBoard File is Secured	ApacheServer_2_4	0
Activated Globally	Analysis - Ensure the Proxy Modules Are Disabled if not in use	ApacheServer_2_4	0
Activated Globally	Analysis - Ensure the Pid File is Secured	ApacheServer_2_4	0
Activated Globally	Analysis - Ensure the OWASP ModSecurity Core Rule Set is Installed and Enabled	ApacheServer_2_4	0
Activated Globally	Analysis - Ensure the Log Config Module is Enabled	ApacheServer_2_4	0
Activated Globally	Analysis - Ensure the Lock File is Secured	ApacheServer_2_4	0
Activated Globally	Analysis - Ensure the LimitRequestLine directive is Set to 8190 or less	ApacheServer_2_4	0
Activated Globally	Analysis - Ensure the LimitRequestFields directive is Set to 1024 or Less	ApacheServer_2_4	0
Activated Globally	Analysis - Ensure the LimitRequestFields directive is Set to 100 or Less	ApacheServer_2_4	0
Activated Globally	Analysis - Ensure the LimitRequestBody Directive is Set to 102400 or Less	ApacheServer_2_4	0
Activated Globally	Analysis - Ensure the IP Addresses for Listening for Requests Are Specified	ApacheServer_2_4	0
Activated Globally	Analysis - Ensure the Info Module Is Disabled	ApacheServer_2_4	0
Activated Globally	Analysis - Ensure the httpd t Type is Not in Permissive Mode	ApacheServer_2_4	0

Using checks and checklists

The check Fixlets in Configuration Management checklists evaluate an endpoint against a defined configuration standard. Many of these check Fixlets have a corresponding analysis, often referred to as "measured values", which reports the value of the element being assessed by the check Fixlet.

Viewing check Fixlets from the HCL BigFix console

A check Fixlet becomes relevant when a client computer is out of compliance with a configuration standard. By reviewing the **Configuration Management Fixlets**, Console Operators can identify non-compliant computers and the corresponding standards.

To access the check Fixlets, subscribe to the **Middleware Checklist Fixlet sites**.

Steps to view the check Fixlets in the HCL BigFix Console:

1. From the **Security Configuration** domain, navigate to **All Security Configuration > Sites > External Sites**.
2. Expand the checklist you want to view.

3. Click **Fixlets and Tasks** to open the Fixlets and Tasks section.
4. Click on one of the Fixlets displayed in the list.

The Fixlet opens with the following tabs: **Description**, **Details**, **Applicable Computers**, and **Action History**.

5. Click the **Description** tab to view details about the Fixlet.

The Fixlet applies to a subset of endpoints on your network, and the size of that subset is shown in the **Applicable Computers** tab.

The description typically includes information about the check, the rationale, and guidelines for remediation actions. If the Fixlet is relevant, you need to take action listed in the **Remediation** section of the description to address non-compliance. You can also access the associated analysis from this tab.

Chapter 6. Configuring Unix checklists

The Configuration Management checklists for UNIX™ systems are delivered as a set of Fixlets and tasks that can help you find the information you need to manage your deployment.

These checklists help system administrators and IT professionals to efficiently manage and configure UNIX™ systems in their environment.

These checklists typically include a series of actions or tasks that cover critical areas of system configuration, security, and compliance. The goal is to ensure that all systems are correctly set up, secure, and aligned with organizational or industry standards.

Overview

You can configure the UNIX™ checklists for the AIX®, MAC, and Solaris.

The UNIX™ checklist in BigFix efficiently addresses the requirements outlined in the CIS and DISA checklists placing significant focus on compliance monitoring procedures.

The majority of UNIX™ audit checks comes with built-in remediation. However, a smaller portion of UNIX™ audit checks offer the flexibility to audit non-default values. If customization is available for a UNIX™ audit check, you will find one or more input fields on the **Description tab** of the Fixlet®. You can simply modify the field corresponding to the desired audit value and click the **Apply** button.

What's new in Unix checklist

HCL BigFix Compliance UNIX™ checklist provides additional support and enhancement in the recent update.

Several checklists have been improved with new features, such as:

- Replaced **Deploy and Run** with an **Environment Setup Task**.
- Improved code performance to facilitate comprehensive file system scanning in AIX and Solaris checklists.
- Optimized code across all checklists for improved performance.
- Introduced continuous compliance for 40% checks using BigFix relevance in CIS Checklist for AIX 7.x.
- Implemented new applicability Fixlets to clearly separate and manage applicability across relevance-based checks in CIS Checklist for AIX 7.x.

For a detailed list of releases, see the [Unix Checklist Release Notes](#).

Available Unix checklist

UNIX™ checklists are commonly used to ensure systems are secure, optimized, and compliant with best practices.

Below are the UNIX™ checklists available in the License dashboard:

Table 9. Unix checklist

CIS/DISA STIG Checklists
AIX
MacOS
Solaris

To get more details of the UNIX™ checklist, refer to the [Unix Checklist](#).

Setup and configuration

Create custom copies of the UNIX™ checklist content if you want to modify the checks based on a specific corporate policy. You can manually create a custom site to host the UNIX™ checklists or use the Create Custom Checklist wizard to create copies of the UNIX™ checklists and save them in a custom site.

You must subscribe to the SCM Reporting external site.

You can use custom checklists to fine-tune your ability to customize Configuration Management parameters, which gives you control over your security status. Custom checklists target specific sets of computers with tailored content using the subscription mechanism. This allows statistics to be gathered with finer granularity. For more information, see [Modifying check parameters \(on page 79\)](#).

Setting up your Configuration Management checklist for UNIX™ Checklist involves two basic steps:

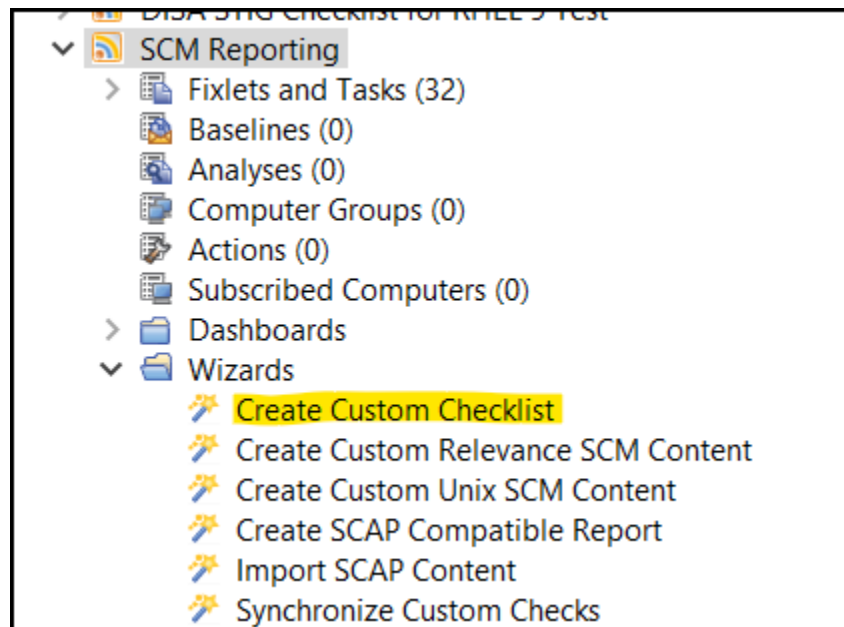
Create your checklist

- Creating custom checklist by using the **Create Custom Checklist** wizard:
 1. From the Security Configuration Domain, go to **Configuration Management > Checklist Tools > Create Custom Checklist**.
 2. Enter the name of the new checklist.
 3. Select the target platform.
 4. Click the drop-down menu to select which external checklist you copy the checks from. As you select the checks, they are shown in the staged list at the lower part of the window.
 5. Click the **Activate Measured Value analyses after copying** check box to activate all analyses that were copied.
 6. Click **Create Checklist**.

The console begins copying the checks in the selected lists into your new custom checklist. The process might take several minutes, depending on the number and size of the checklists selected.

Use the **Create Custom Checklist** wizard located in the **SCM Reporting** site under the wizard section.

Figure 41. Create custom checklist



- Creating custom checklists manually:

1. Select **Tools > Create Custom Site**.
2. You are prompted for a name for your custom site. Enter a name and click **OK**.
3. From the Domain panel, find your site under **Sites > Custom** and click it to describe your site.
From the **Details** tab, enter a description of your site. From the **Domain** pull-down menu, select a Domain to house your site.
4. From the **Computer Subscriptions** tab, indicate which subset of your BigFix client computers you want to subscribe to this site.
5. From the **Operator Permissions** tab, you can grant specific access permissions to specific operators.
6. Click the **Save Changes** button above the work area to complete the description of your site. You must enter your password to propagate your new custom site.

Subscribe computers to the custom checklist.



Note: Custom checklists do not support site relevance, so take extra precaution when you subscribe computers to custom checklists.



Figure 42. Create custom checklist

Create Custom Checklist

This wizard will assist you in creating a new custom checklist based on one or more of your currently subscribed external checklists.

New checklist name: 9 characters remaining (98 checks selected out of 98 displayed)

Select target platform:

- ☐ MacOS 13
- ☒ MacOS 15
- ☐ Oracle 19c Windows

External checklist to copy checks from: Search

Check Name	Source ID	Source Severity	Source Checklist
<input checked="" type="checkbox"/> Ensure iCloud Drive Document and Desktop...	cis-2.1.1.3	Level 2	CIS Checklist for MacOS 15
<input checked="" type="checkbox"/> Ensure File Sharing Is Disabled	cis-2.3.3.3	Level 1	CIS Checklist for MacOS 15
<input checked="" type="checkbox"/> Ensure Time Machine Volumes Are Encrypt...	cis-2.3.4.2	Level 1	CIS Checklist for MacOS 15
<input checked="" type="checkbox"/> Ensure 'Show Location Icon in Control Cen...	cis-2.6.1.2	Level 2	CIS Checklist for MacOS 15
<input checked="" type="checkbox"/> Ensure the OS Is Not Active When Resumi...	cis-2.9.1.1	Level 2	CIS Checklist for MacOS 15
<input checked="" type="checkbox"/> Ensure Automatic Login Is Disabled	cis-2.12.3	Level 1	CIS Checklist for MacOS 15
<input checked="" type="checkbox"/> Ensure the Sudo Timeout Period Is Set to ...	cis-5.4	Level 1	CIS Checklist for MacOS 15
<input checked="" type="checkbox"/> Ensure Apple Mobile File Integrity (AMFI) I...	cis-5.1.3	Level 1	CIS Checklist for MacOS 15
<input checked="" type="checkbox"/> Ensure Complex Password Must Contain Up...	cis-5.2.6	Level 2	CIS Checklist for MacOS 15
<input checked="" type="checkbox"/> Ensure HTTP Server Is Disabled	cis-4.2	Level 1	CIS Checklist for MacOS 15

Staged List: The following checks will be copied to your new checklist (including any necessary measured value analyses and/or applicability filelets):

Check Name	Source ID	Source Severity	Source Checklist
<input checked="" type="checkbox"/> Ensure iCloud Drive Document and Desktop Sync Is D...	cis-2.1.1.3	Level 2	CIS Checklist for MacOS 15
<input checked="" type="checkbox"/> Ensure File Sharing Is Disabled	cis-2.3.3.3	Level 1	CIS Checklist for MacOS 15
<input checked="" type="checkbox"/> Ensure Time Machine Volumes Are Encrypted If Time ...	cis-2.3.4.2	Level 1	CIS Checklist for MacOS 15
<input checked="" type="checkbox"/> Ensure 'Show Location Icon in Control Center when S...	cis-2.6.1.2	Level 2	CIS Checklist for MacOS 15
<input checked="" type="checkbox"/> Ensure the OS Is Not Active When Resuming from ST...	cis-2.9.1.1	Level 2	CIS Checklist for MacOS 15
<input checked="" type="checkbox"/> Ensure Automatic Login Is Disabled	cis-2.12.3	Level 1	CIS Checklist for MacOS 15
<input checked="" type="checkbox"/> Ensure the Sudo Timeout Period Is Set to Zero	cis-5.4	Level 1	CIS Checklist for MacOS 15
<input checked="" type="checkbox"/> Ensure Apple Mobile File Integrity (AMFI) Is Enabled	cis-5.1.3	Level 1	CIS Checklist for MacOS 15
<input checked="" type="checkbox"/> Ensure Complex Password Must Contain Uppercase a...	cis-5.2.6	Level 2	CIS Checklist for MacOS 15
<input checked="" type="checkbox"/> Ensure HTTP Server Is Disabled	cis-4.2	Level 1	CIS Checklist for MacOS 15

98 total checks will be copied to the new checklist

Activate Measured Value analyses after copying ☒ Create Checklist

- Run or Schedule your checklist:

1. Schedule or run the **Environment Setup Task**. Select the **Environment Setup Task** and click the **Take Action** button.
2. Enter the credentials or required details in the pop-up, if prompted.
3. Choose the target computer or group of computers from the target section.
4. Set up the execution criteria based on your environment and click **OK** to schedule or set up the **Environment Setup Task**.



Note: To get more details about the **Environment Setup Task**, see [Environment Setup Task \(on page 72\)](#) section.

Unix checklist components

The Unix checklist components ensure that the system is systematically reviewed and remains operational, secure, and compliant.

Environment Setup Task

The Environment Setup Task is a crucial component of UNIX™ checklists. It plays a key role in determining the compliance status of each check in the checklist.

Under normal conditions, once an endpoint subscribes to the site, the **Environment Setup Task** becomes relevant, enabling you to click **Take Action**. When executed, this task downloads the `sqlite_detect.db` file from an external site, which contains all the available detection scripts. Using relevance, the task identifies and extracts the scripts corresponding to the checks available in the current site. These scripts are then copied to the SCM folder and executed sequentially.

During execution, individual logs are generated in the **Logs** directory, while the results are saved in the **Results** folder. Additionally, a comprehensive log file, **Environment_Setup_Task.log**, is created to record all execution details.

Figure 43. Environment Setup Task

The screenshot displays the 'Fixlets and Tasks' window. At the top, a table lists tasks with columns 'Source ID' and 'Name'. The 'Environment Setup Task' is highlighted. Below the table, a toolbar contains icons for 'Take Action', 'Edit', 'Copy', 'Export', 'Hide Locally', 'Hide Globally', and 'Remove'. Below the toolbar, there are tabs for 'Description', 'Details', 'Applicable Computers (0)', and 'Action History (0)'. The 'Description' tab is active, showing a text box with the following content:

Description

This task downloads the `sqlite_detect.db` file from the external site, which contains all the available detect scripts. Relevance is then used to check checks available in the current site. These scripts are subsequently copied to the SCM folder and executed sequentially. It will populate the necessary properties on the endpoint which will be read by the fixlets of this site for relevance evaluation.

Actions

Click [here](#) to deploy this action.

The check Fixlets from the site will display the latest results only after the **Environment Setup Task** is completed.

To ensure regular compliance validation, schedule periodic executions of the Environment Setup Task.

Schedule periodic executions of the Environment Setup task

This means automating the task at regular intervals to continuously validate and update the compliance status of endpoints. This ensures that compliance checks are consistently performed, logs and results remain up to date, and any deviations or non-compliance issues are promptly identified and addressed.

1. From the Security Configuration Domain, go to **All Security Configuration > Sites > External sites**.
2. Select a checklist and click **Fixlets and Tasks**.
3. In the **List** panel, find and select the **Environment Setup Task**.

Figure 44. Environment Setup Task in CIS Checklist for MacOS 12

Fixlets and Tasks	
Source ID ^	Name
	Applicability Fixlet - MacOS 12
	Environment Setup Task
cis-1.1	Ensure All Apple-provided Software Is Current
cis-1.2	Ensure Auto Update Is Enabled
cis-1.3	Ensure Download New Updates When Available Is Enabled
cis-1.4	Ensure Installation of App Update Is Enabled
cis-1.5	Ensure System Data Files and Security Updates Are Downloaded Automatically Is Enabled
cis-1.6	Ensure Install of macOS Updates Is Enabled
cis-1.7	Ensure Software Update Deferment Is Less Than or Equal to 30 Days

Task: Environment Setup Task

Take Action
 Edit
 Copy
 Export
 Hide Locally
 Hide Globally
 Remove

Description
 Details
 Applicable Computers (0)
 Action History (0)

Description

This task downloads the sqlite_detect.db file from the external site, which contains all the available detect scripts. Relevance is then used to check checks available in the current site. These scripts are subsequently copied to the SCM folder and executed sequentially.

It will populate the necessary properties on the endpoint which will be read by the fixlets of this site for relevance evaluation.

Actions

Click [here](#) to deploy this action.

4. Click **Take Action** on the **Environment Setup Task**.
5. Choose the appropriate endpoints in your environment.
6. Click the **Execution** tab.

Figure 45. Take Action - Execution tab

Take Action

Name: Create in domain:

Preset: ☐ Show only personal presets

Target Execution Users Messages Offer Post-Action Applicability Success Criteria Action Script

Constraints

☐ Starts on at

☒ Ends on at

☐ Run between and

☐ Run only on

☐ Run only when

Behavior

☐ On failure, retry times

☒ Wait between attempts

☐ Wait until computer has rebooted

☐ Reapply this action

☒ whenever it becomes relevant again

☐ while relevant, waiting between reapplications

☒ Limit to reapplications

☐ Start client downloads before constraints are satisfied

☐ Stagger action start times over minutes to reduce network load

7. Configure the **Environment Setup Task** to run as needed, and click **OK**.

The **Environment Setup Task** updates reports in the **Security and Compliance Analytics (SCA)** console, now called **BigFix Compliance Analytics**, with the latest results. To ensure up-to-date content, execute this task on the endpoint before performing an import. If automatic daily import is enabled in BigFix Compliance Analytics, additional runs of the Environment Setup Task are unnecessary.



Note: Parameter changes will take effect only after the next execution of the Environment Setup Task.

Understanding the output of Environment Setup task

With UNIX™ content, endpoint scans are accomplished using a series of shell or Powershell scripts, that provide greater accessibility to system administrators.

In most BigFix content, Fixlets continuously evaluate conditions on each endpoint. The console shows the results when the relevance clause of the Fixlet evaluates to **true** or **false**. However, for UNIX™ content, an **Environment Setup**

Task triggers a scan of the endpoints. This task can be executed on-demand whenever a scan is needed or scheduled as a recurring policy from the console.

The endpoint scan is performed using a series of Shell/Powershell scripts available within individual checks or Fixlets. These scripts write collected data to **individual Result files**, which are then accessed by the corresponding Fixlet checks for evaluation. Once the results files are written to disk, the Fixlets read each results file and show the results in the console.

After running the **Environment Setup Task** from the Security Checklist, the scripts execute and generate multiple files for each check, including a script file, a log file, and a result file:

Table 10. File paths for Logs and results

File Name	Path in MacOS	Path in AIX and Solaris	Content
Environment_Setup_-Task.log	/Library/Application Support/BigFix/BES Agent/SCM/<ProjectID>/<CIS/DISA>/	/var/opt/BESClient/SCM/<ProjectID>/<CIS/DISA>/	Execution details of Task and individual checks.
<sourceID.log>	/Library/Application Support/BigFix/BES Agent/SCM/SCM/<ProjectID>/<CIS/DISA>/Logs	/var/opt/BESClient/SCM/<ProjectID>/<CIS/DISA>/Logs	Logs for execution of particular fixlet/Check
<sourceID.Result>	/Library/Application Support/BigFix/BES Agent/SCM/SCM/<ProjectID>/<CIS/DISA>/Results	/var/opt/BESClient/SCM/<ProjectID>/<CIS/DISA>/Results	Compliance status of particular fixlet/Check
<sourceID.sh>	/Library/Application Support/BigFix/BES	/var/opt/BESClient/SCM/<ProjectID>/<CIS/D	Individual scripts for all the checks in the site
	Agent/SCM/SCM/<ProjectID>/<CIS/DISA>/Scripts	ISA>/Scripts	



Note: If an individual Fixlet contains a parameter, then it will be added in a file named **Parameter.txt**, which is then stored in the **custom site folder**.

Applicability Fixlets

Learn about concepts and the work process in Configuration Management.

Each UNIX™ checklist includes Applicability Fixlets based on the checklist requirements. For example, in the **CIS Checklist for MacOS 13**, the following Applicability Fixlets are available:

1. Applicability Fixlet - MacOS 13

These Fixlets work with HCL BigFix Compliance to determine whether endpoints subscribed to the checklist meet the required conditions. A Fixlet is relevant only for applicable endpoints and remains irrelevant otherwise. To optimize performance, site subscriptions should be limited to applicable endpoints.



Note: The number of Applicability Fixlets may vary depending on checklist requirements.

Fixlets with remediation action on applicability Fixlets

The Omit List in applicability Fixlets is a predefined list of checks that are excluded from the evaluation process.

In the **Applicability Fixlet - MacOS 13**, we specify the Fixlets that include remediation actions.

Figure 46. List of Checks containing an action for remediation

Description	
Applicability Fixlet - MacOS 13	
This fixlet is used in connection with HCL Endpoint Manager Analytics to determine whether endpoints subscribed to the current checklist meet the following condition:	
<ul style="list-style-type: none"> • Operating System Platform: MacOS 13.0 Ventura • Applicability Profile: MAC 13 	
Effort should be made to limit site subscription to applicable endpoints.	
There may be nearly identical applicability fixlets included within a checklist in cases where the conditions for applicability are related but different.	
Fixlets with Remediation Actions	
Source ID	Fixlet Name
cis-1.2	Ensure Auto Update Is Enabled
cis-1.3	Ensure Download New Updates When Available Is Enabled
cis-1.4	Ensure Install of macOS Updates Is Enabled
cis-1.5	Ensure Install Application Updates from the App Store Is Enabled
cis-1.6	Ensure Install Security Responses and System Files Is Enabled
cis-3.1	Ensure Security Auditing Is Enabled
cis-3.3	Ensure install.log Is Retained for 365 or More Days and No Maximum Size
cis-3.4	Ensure Security Auditing Retention Is Enabled
cis-3.5	Ensure Access to Audit Records Is Controlled
cis-3.6	Ensure Firewall Logging Is Enabled and Configured
cis-4.1	Ensure Bonjour Advertising Services Is Disabled

Omit List in applicability Fixlets

The Omit List in applicability Fixlets is a predefined list of checks that are excluded from the evaluation process.

In the **Applicability Fixlet - MacOS 13**, we include the Omit List, which specifies checks that are not supported from the benchmark. These omitted checks typically require human interaction or have technical limitations that prevent automated evaluation.

Figure 47. Omit list from the CIS Checklist for MacOS 13

Checks not supported from CIS Checklist for MacOS 13	
List of checks not supported from CIS Checklist for MacOS 13 due to the requirement of human interaction / technical limitations.	
Total number of checks: 119 Checks supported: 96 Checks not supported: 23	
Benchmark file check No.	Reason
2.1.1.2	Manual Intervention required
2.1.1.4	Manual Intervention required
2.1.1.6	Manual Intervention required
2.1.2	Manual Intervention required
2.3.3.12	Manual Intervention required
2.6.1.3	Manual Intervention required
2.6.2.1	Manual Intervention required
2.6.7	Manual Intervention required
2.11.2	Manual Intervention required
2.13.1	Manual Intervention required
2.14.1	Manual Intervention required
2.15.1	Manual Intervention required

Remediation

Most UNIX™ checks include built-in remediation capabilities. However, a smaller subset of UNIX™ audit checks allows customization to audit a non-default value.

If a UNIX™ audit check supports customization, the **Description tab** of the Fixlet will contain **one or more input fields** for user-defined values.

Remediating configuration settings

UNIX™ checklists support remediation, allowing console operators to resolve vulnerabilities with a single action. A remediation action can only be executed on an endpoint where the Fixlet is relevant.

You can audit, assess, and remediate configuration settings using **Security and Compliance Analytics (SCA)**, now known as **BigFix Compliance Analytics**. For Fixlet checks that support automatic remediation, an **action button** appears within the relevant Fixlet. Remediation actions can only be applied to relevant and selected endpoints.



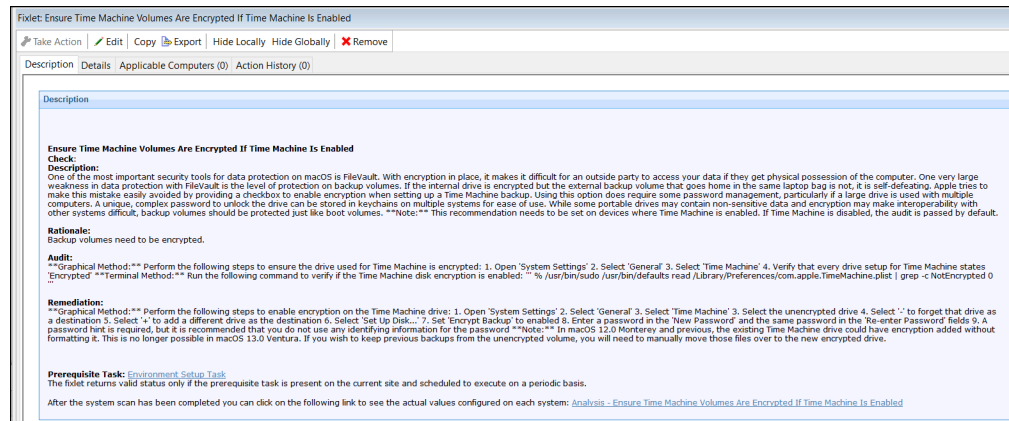
Note: Not all Fixlets include a remediation action.



Note: If an external global policy is enabled, any local endpoint changes will be overwritten. In such cases, remediation must be performed using the external global policy solution.

1. Navigate to the **Security Configuration Domain > All Security Configuration > Fixlets and Tasks**.
2. Expand the sub-folders to locate the desired Fixlet.
3. Open the Fixlet, click the **Description** tab, and scroll down to the **Actions** box.
4. Click the link in the **Actions** box to remediate the specified policy issue.

Figure 48. Check containing an action for remediation



5. Set your parameters in the **Take Action** dialog and click **OK**.

Modifying check parameters

In addition to monitoring compliance status and remediating non-compliant settings, you can modify configuration settings to align with your organization's policies.

To adjust the desired value of a check parameter in the Fixlet check description, you must first create a custom site. For details on custom sites, refer to [Creating Custom Checklists](#). Since parameters are stored as site settings, the same check can be parameterized differently across sites containing a copy of the check.



Note: Not all checks in custom sites can be parameterized.

Certain Fixlet checks allow you to specify a more restrictive value than the default specified by the UNIX™ checklist, providing greater flexibility to customize security policies to meet the specific requirements.



Important: Custom parameterization may take a few minutes to process. Allow sufficient time between updating a parameter and executing the **Environment Setup Task** for optimal results.



Note: Parameter changes will only take effect after running the **Environment Setup Task**. For more details, see [Configuring Endpoints](#).

1. Open the Fixlet check and navigate to the **Description** tab.
2. Scroll down to the **Parameters** section and enter the desired value.

Figure 49. Setting up Parameterization for Fixlets

Fixlet: Ensure Home Folders Are Secure

Take Action | Edit | Copy | Export | Hide Locally | Hide Globally | Remove

Description | Details | Applicable Computers (0) | Action History (0)

Description

Ensure Home Folders Are Secure

Check:

Description:
By default, macOS allows all valid users into the top level of every other user's home folder and restricts access to the Apple default folders within. Another user on the same system can see you have a "Documents" folder but cannot see inside it. This configuration does work for personal file sharing but can expose user files to standard accounts on the system. The best parallel for Enterprise environments is that everyone who has a Dropbox account can see everything that is at the top level but can't see your pictures. Similarly with macOS, users can see into every new Directory that is created because of the default permissions. Home folders should be restricted to access only by the user. Sharing should be used on dedicated servers or cloud instances that are managing access controls. Some environments may encounter problems if execute rights are removed as well as read and write. Either no access or execute only for group or others is acceptable.

Rationale:
Allowing all users to view the top level of all networked users' home folder may not be desirable since it may lead to the revelation of sensitive information.

Audit:
Terminal Method: Run the following command to ensure that all home folders are secure: "" % /usr/bin/sudo /usr/bin/find /System/Volumes/Data/Users -mindepth 1 -maxdepth 1 -type d -not -perm 700 | /usr/bin/grep -v "Shared" | /usr/bin/grep -v "Guest" "" The output will show what user folders are not secure. _example_: "" % /usr/bin/sudo /usr/bin/find /System/Volumes/Data/Users -mindepth 1 -maxdepth 1 -type d -not -perm 700 | /usr/bin/grep -v "Shared" | /usr/bin/grep -v "Guest" /System/Volumes/Data/Users/firstuser /System/Volumes/Data/Users/thirduser

Remediation:
Terminal Method: For each user, run the following command to secure all home folders: "" % /usr/bin/sudo /bin/chmod -R og-rwx /Users/ "" Alternately, run the following command if there needs to be executable access for a home folder: "" % /usr/bin/sudo /bin/chmod -R og-rw /Users/ "" _example_: "" % /usr/bin/sudo /bin/chmod -R og-rw /Users/firstuser/ % /usr/bin/sudo /bin/chmod -R og-rwx /Users/thirduser/ ""

Parameters

EXCLUDE_PATHS_1: Space separated list of directories in /Users to exclude

Default Value:

Current Value:

PERMS_1: Octal value of permissions

Default Value:

Current Value:

Note: Parameters can only be set on a custom copy of this check

Prerequisite Task: [Environment Setup Task](#)
The fixlet returns valid status only if the prerequisite task is present on the current site and scheduled to execute on a periodic basis.

After the system scan has been completed you can click on the following link to see the actual values configured on each system: [Analysis - Ensure Home Folders Are Secure](#)

3. Click **Apply**.
4. Execute the **Environment Setup Task**.

Measured Value Analysis

Many check Fixlets have a corresponding analysis, often referred to as "measured values", which report the value of the element being evaluated by the check Fixlet.

Each computer reports its properties and analysis values, including active check measured values in your deployment. These results are aggregated by the BigFix Compliance Analytics server and enhanced with computer properties and analysis values, providing both compliance overviews and detailed result lists.

Steps to activate measured values:

- Expand the checklist.
- Navigate to the **Analysis** section.
- In the right-hand panel, select all the analyses.
- Right-click and select **Activate Analysis**.

Figure 50. Non-Activated Measured Value Analyses

Analyses						
Status	Name	Site	Applicable Comput...	Activated By	Time Activated	
Not Activated	Analysis - Ensure All Apple...	CIS Checklist for M...	0			
Not Activated	Analysis - Ensure Auto Up...	CIS Checklist for M...	0			
Not Activated	Analysis - Ensure Downloa...	CIS Checklist for M...	0			
Not Activated	Analysis - Ensure Install of ...	CIS Checklist for M...	0			
Not Activated	Analysis - Ensure Install Ap...	CIS Checklist for M...	0			
Not Activated	Analysis - Ensure Install Se...	CIS Checklist for M...	0			
Not Activated	Analysis - Ensure Software ...	CIS Checklist for M...	0			
Not Activated	Analysis - Ensure the Syste...	CIS Checklist for M...	0			
Not Activated	Analysis - Ensure Security...	CIS Checklist for M...	0			
Not Activated	Analysis - Ensure Security...	CIS Checklist for M...	0			
Not Activated	Analysis - Ensure install.J...	CIS Checklist for M...	0			
Not Activated	Analysis - Ensure Security...	CIS Checklist for M...	0			
Not Activated	Analysis - Ensure Access...	CIS Checklist for M...	0			
Not Activated	Analysis - Ensure Firewall...	CIS Checklist for M...	0			
Not Activated	Analysis - Ensure Bonjour...	CIS Checklist for M...	0			
Not Activated	Analysis - Ensure HTTP S...	CIS Checklist for M...	0			
Not Activated	Analysis - Ensure NFS Ser...	CIS Checklist for M...	0			
Not Activated	Analysis - Ensure the Sudo...	CIS Checklist for M...	0			
Not Activated	Analysis - Ensure a Separ...	CIS Checklist for M...	0			
Not Activated	Analysis - Ensure the "root...	CIS Checklist for M...	0			
Not Activated	Analysis - Ensure an Adm...	CIS Checklist for M...	0			
Not Activated	Analysis - Ensure a Login...	CIS Checklist for M...	0			
Not Activated	Analysis - Ensure Legacy...	CIS Checklist for M...	0			
Not Activated	Analysis - Ensure the Gue...	CIS Checklist for M...	0			
Not Activated	Analysis - Ensure XProtect...	CIS Checklist for M...	0			
Not Activated	Analysis - Ensure Firewall...	CIS Checklist for M...	0			
Analysis: Analysis - Ensure the System is Managed by a Mobile Device Management (MDM) Software						

Figure 51. Activated Measured Value Analyse

Analyses						
Status	Name	Site	Applicable Comput...	Activated By	Time Activated	
Activated Globally	Analysis - Ensure All Apple...	mac13_prod	1	bigfix	3/3/2025 7:38:03 PM	
Activated Globally	Analysis - Ensure Auto Up...	mac13_prod	1	bigfix	3/3/2025 7:38:04 PM	
Activated Globally	Analysis - Ensure Downloa...	mac13_prod	1	bigfix	3/3/2025 7:38:04 PM	
Activated Globally	Analysis - Ensure Install of ...	mac13_prod	1	bigfix	3/3/2025 7:38:05 PM	
Activated Globally	Analysis - Ensure Install Ap...	mac13_prod	1	bigfix	3/3/2025 7:38:05 PM	
Activated Globally	Analysis - Ensure Software ...	mac13_prod	1	bigfix	3/3/2025 7:38:06 PM	
Activated Globally	Analysis - Ensure Software ...	mac13_prod	1	bigfix	3/3/2025 7:38:06 PM	
Activated Globally	Analysis - Ensure the Syste...	mac13_prod	1	bigfix	3/3/2025 7:38:07 PM	
Activated Globally	Analysis - Ensure Security ...	mac13_prod	1	bigfix	3/3/2025 7:38:07 PM	
Activated Globally	Analysis - Ensure Security ...	mac13_prod	1	bigfix	3/3/2025 7:38:08 PM	
Activated Globally	Analysis - Ensure install.J...	mac13_prod	1	bigfix	3/3/2025 7:38:08 PM	
Activated Globally	Analysis - Ensure Security ...	mac13_prod	1	bigfix	3/3/2025 7:38:09 PM	
Activated Globally	Analysis - Ensure Access to...	mac13_prod	1	bigfix	3/3/2025 7:38:09 PM	
Activated Globally	Analysis - Ensure Firewall L...	mac13_prod	1	bigfix	3/3/2025 7:38:09 PM	
Activated Globally	Analysis - Ensure Bonjour ...	mac13_prod	1	bigfix	3/3/2025 7:38:10 PM	
Activated Globally	Analysis - Ensure HTTP Ser...	mac13_prod	1	bigfix	3/3/2025 7:38:10 PM	
Activated Globally	Analysis - Ensure NFS Serv...	mac13_prod	1	bigfix	3/3/2025 7:38:11 PM	
Activated Globally	Analysis - Ensure the Sudo ...	mac13_prod	1	bigfix	3/3/2025 7:38:11 PM	
Activated Globally	Analysis - Ensure a Separat...	mac13_prod	1	bigfix	3/3/2025 7:38:11 PM	
Activated Globally	Analysis - Ensure the "root...	mac13_prod	1	bigfix	3/3/2025 7:38:12 PM	
Activated Globally	Analysis - Ensure an Admi...	mac13_prod	1	bigfix	3/3/2025 7:38:12 PM	
Activated Globally	Analysis - Ensure a Login ...	mac13_prod	1	bigfix	3/3/2025 7:38:13 PM	
Activated Globally	Analysis - Ensure Legacy E...	mac13_prod	1	bigfix	3/3/2025 7:38:13 PM	
Activated Globally	Analysis - Ensure the Gue...	mac13_prod	1	bigfix	3/3/2025 7:38:14 PM	
Activated Globally	Analysis - Ensure XProtect...	mac13_prod	1	bigfix	3/3/2025 7:38:15 PM	
Activated Globally	Analysis - Ensure Firewall...	mac13_prod	1	bigfix	3/3/2025 7:38:15 PM	

Using checks and checklists

The check Fixlets in Configuration Management checklists evaluate an endpoint against a defined configuration standard. Many of these check Fixlets have a corresponding analysis, often referred to as "measured values", which reports the value of the element being assessed by the check Fixlet.

Viewing check Fixlets from the HCL BigFix console

A check Fixlet becomes relevant when a client computer is out of compliance with a configuration standard. By reviewing the **Configuration Management Fixlets**, Console Operators can identify non-compliant computers and the corresponding standards.

To access the check Fixlets, subscribe to the **UNIX Checklist Fixlet sites**.

Steps to view the check Fixlets in the HCL BigFix Console:

1. From the **Security Configuration** domain, navigate to **All Security Configuration > Sites > External Sites**.
2. Expand the checklist you want to view.
3. Click **Fixlets and Tasks** to open the Fixlets and Tasks section.
4. Click on one of the Fixlets displayed in the list.

The Fixlet opens with the following tabs: **Description**, **Details**, **Applicable Computers**, and **Action History**.

5. Click the **Description** tab to view details about the Fixlet.

The Fixlet applies to a subset of endpoints on your network, and the size of that subset is shown in the **Applicable Computers** tab.

The description typically includes information about the check, the rationale, and guidelines for remediation actions. If the Fixlet is relevant, you need to take action listed in the **Remediation** section of the description to address non-compliance. You can also access the associated analysis from this tab.

Chapter 7. Importing SCAP content

BigFix uses an Security Content Automation Protocol (SCAP) Import Wizard to convert SCAP XML input files, typically XCCDF files, into BigFix content such as Fixlets. This process enables the integration of standardized security content into the BigFix platform.



Important: Importing a SCAP datastream will create a new site in BigFix, which may contain hundreds of Fixlets and analyses. This may cause the BigFix console to temporary slowdown after the import is complete. It is recommended to proceed thoughtfully and monitor performance after the import.

Learning about SCAP

The Security Content Automation Protocol (SCAP) is a suite of open standards designed to automate vulnerability management, measurement, and policy compliance evaluation of computer systems. SCAP consists of multiple standards like CVE (vulnerability enumeration), CPE (platform enumeration), XCCDF (checklist format), and OVAL (vulnerability checks). It facilitates automated reporting, scoring, and remediation workflows to reduce manual security management efforts.

You can find NIST's official documentation about SCAP at the following link: [CSRC-SCAP](#).

Information Security Automation Program (ISAP)

The Information Security Automation Program (ISAP) automates and standardizes technical security operations. Primarily focused on government, ISAP offers security checking, remediation, and automation of technical compliance activities to such regulations as FISMA and the FDCC.

ISAP objectives include enabling standards-based communication of vulnerability data, customizing and managing configuration baselines for various IT products, assessing information systems and reporting compliance status, using standard metrics to weight and aggregate potential vulnerability impact, and remediating identified vulnerabilities.

SCAP standards

Common Vulnerabilities and Exposures (CVE)

The SCAP CVE standard is a dictionary of publicly known information security vulnerabilities that enable data exchanges between security products and provide a baseline index point for evaluating coverage of tools and services.

HCL BigFix has actively supported CVE for several versions of the product and maintains a mature product integration with CVE content. Any security patch or vulnerability that has an associated CVE ID and is available as either a SCAP data stream or available through other HCL BigFix developed processes will display the relevant CVE ID within the HCL BigFix console.

You can find this ID associated with a given security patch or vulnerability by opening the HCL BigFix console and navigating to a patch or vulnerability Fixlet site, double-clicking a relevant Fixlet, selecting the Details tab and viewing the CVE ID. The CVE ID is also accessible from other views and can be used as part of the reporting criteria for detailed and summary reports on individual end-point systems or for a large group of systems reported on in the aggregate.

Common Configuration Enumeration (CCE)

The SCAP CCE standard provides unique identifiers to system configuration issues to facilitate fast and accurate correlation of configuration data across multiple information sources and tools. For example, CCE Identifiers can associate checks in configuration assessment tools with statements in configuration best practice documents. The HCL BigFix platform includes the ability to assess workstations, laptops, servers, and mobile computing devices against common configuration settings to identify misconfiguration states in a diverse computing environment. HCL BigFix fully supports CCE and displays the CCE ID for each misconfiguration for which there is a CCE ID within the HCL BigFix console. In the case where a misconfiguration is associated with multiple CCE IDs, all IDs are cross-referenced and displayed.

To find the CCE ID associated with a configuration setting, open the HCL BigFix console and navigate to a configuration setting used by a SCAP data stream. Click on a Fixlet that represents a configuration setting and view the Source ID column. The Source ID displays the CCE ID. The CCE ID is also accessible from other views and can be used as part of the reporting criteria for detailed reports and summary reports on individual end-point systems or for a large group of systems reported on in the aggregate.

Common Platform Enumeration (CPE)

The SCAP CPE standard is a structured naming scheme for information technology systems, platforms, and packages. Based on the generic syntax for Uniform Resource Identifiers (URI), CPE includes a formal name format, a language for describing complex platforms, a method for checking names against a system, and a description format for binding text and tests to a name. HCL BigFix uses CPE to ensure that configuration settings are assessed on the correct system. Regardless of the operating system, the CPE ID can identify a platform and ensure that an assessment is performed.

You can assess and remediate system configurations by targeting systems by platform in addition to other targeting mechanisms. By targeting a particular platform, you can ensure that system scans are done properly and are weighed against applicable configuration checks. Checks are assessed in real-time based on the platform and policies can be enforced, giving administrators current visibility and control over platforms in a distributed or non-distributed computing environment.

Common Vulnerability Scoring System (CVSS)

The SCAP CVSS standard provides an open framework for communicating the characteristics of IT vulnerabilities. Its quantitative model ensures repeatable, accurate measurement while displaying vulnerability characteristics used to generate the scores. Thus, CVSS is well suited as a standard measurement system for industries, organizations, and agencies that need accurate and consistent vulnerability impact scores.

HCL BigFix assesses and reports on vulnerabilities and quantifies the impact for multiple computing platforms. HCL BigFix fully supports the CVSS standard and displays both the CVSS base score for each applicable vulnerability and the CVSS Base Score Vector used to produce the score.

HCL BigFix administrators can access the CVSS score and the associated vector string from within the HCL BigFix console. For additional details, administrators can navigate to the a vulnerability definition from within the Fixlets. HCL BigFix provides a link for administrators to connect to the CVSS definition located on the NVD website. HCL BigFix enhances the value of CVSS by displaying this common metric for detailed reports on individual end-point systems and for large groups of systems reported on in the aggregate.

Extensible Configuration Checklist Description Format (XCCDF)

The SCAP XCCDF standard is a specification language for writing security checklists, benchmarks, and related documents. An XCCDF document represents a structured collection of security configuration rules for some sets of target systems and is the core element of the SCAP data stream. The specification also defines a data model and format for storing results of checklist compliance testing.

SCAP data streams use the XCCDF format to translate underlying configuration checks that are defined in HCL BigFix Fixlets. When created, these SCAP-based configuration Fixlets allow administrators to assess their computing assets against the SCAP-defined configuration rules in real-time and on a global scale.

When the SCAP configuration rules are imported into HCL BigFix, any system can immediately assess against the defined configuration rules. The results of those configuration checks are relayed to the HCL BigFix console, where administrators can view results and generate detailed reports on an individual system or on large groups of systems.

HCL BigFix also exports the results of the configuration checks into the defined XCCDF report format so that the organization can store, send, or import those reports into another tool.

Open Vulnerability and Assessment Language (OVAL)

The SCAP OVAL standard is an international, information security community standard that promotes security content and standardizes the transfer of this information across an entire spectrum of security tools and services. The OVAL language is a collection of XML schema for representing system information, expressing specific machine states, and reporting the results of an assessment.

Through a repository of vulnerability assessment policies, HCL BigFix assesses managed computers against OVAL vulnerability definitions using real-time data tracking based on the data elements of each definition. These policies are automatically retrieved by the HCL BigFix product within an organization's network. When validated for authenticity, the policies are made available to the HCL BigFix client installed on each managed computer and added to their local library of configuration policies. The agent continuously evaluates the state of the machine against each policy so that any instance of non-compliance can be reported to the HCL BigFix Server for administrator review. If pre-authorized

by an administrator, the appropriate corrective action is applied to the computer immediately upon misconfiguration detection, even to remote or mobile users not connected to the organization's network.

Asset Reporting Format (ARF)

The Asset Reporting Format (ARF) is a standardized data model that is able to capture report requests, reports, assets and their relationships. HCL BigFix can generate standard ARF reports which can be used to further analyze or import into other third party applications.

SCAP Checklists

SCAP checklist helps you automatically check your system's security by comparing it to set rules. This makes it easier to find weaknesses and make sure your system follows security policies.

HCL BigFix uses the SCAP checklist XML to create BigFix content and makes it available through subscription. Users can load the external site mastheads for each of the available SCAP checklist in the BigFix console. The BigFix server then downloads the content and makes it available to the BigFix administrator for system evaluations.

BigFix currently provides out-of-the-box content for the Federal Desktop Core Configuration (FDCC) SCAP checklists. As new checklists are made available by NIST, HCL BigFix might include those sites as part of the subscription service.

In addition to the Fixlet sites, BigFix includes a reporting dashboard that provides visibility into the results of the system evaluations and a reporting dashboard for generating BigFix content from an SCAP checklist. These dashboards are found in the **SCM Reporting** site.

To know the supported SCAP checklists, see the [SCM Checklist](#).

Using the Import SCAP Content wizard

The Import SCAP Content wizard is a tool that allows users to load SCAP-compliant content, such as security baselines and checklists, into a system for automated compliance scanning.

Configure your anti-virus and firewall to avoid blocking executable files which facilitate processes that are initiated when importing checklists or generating reports. The details of the processes are as follows:

- **File:** SHA256 checksum

ruby.exe

62a02cd27eccc8f16e9396459ecb3bdec6dff9ee4bad20fa6b251c908dc74840

scap2.exe

cf4f3ae7e675be16b93494ccaf1b1730d90fccb02bba57f66f312242a2dc1187

scap2results.exe

dcba8436dad1b2fb9dc67c3872df5150c68d9f152f0897c44a177140e505b4d5

scap_results.exe

4f47d9943422371c7b4b16d4e853ad7f03810f9bf274836f8735222fbde2fe4c



Note: These values are examples of the file checksum function for the SCAP Tools. The value varies with each published release version of the SCAP Tools. For values that are applicable to new SCAP releases, see [SCAP Release Notes](#).

- **File path:** [Path_to_Console]/Sites/SCM Reporting

The Import SCAP Content wizard generates HCL BigFix content from a set of SCAP XML input files into a custom site. The content that is generated includes a Fixlet for each check found in the SCAP checklist.

To find SCAP checklists, see the [National Checklist Program Repository](#). The SCAP Import wizard has been validated for checklists at Tier IV in this repository. The wizard supports checklists designed for the Windows platform.

1. From the **Security Configuration Domain**, go to **All Security Configuration > Import SCAP Content**.
2. Click **Select** and choose the XCDDF file that will be imported.

Import Windows SCAP Content

Use this wizard to import a Windows SCAP checklist into a custom site. This will make it possible to assess the compliance of the endpoints in a deployment against technical security standards provided by USGCB, DISA, FDCC and others. Importing UNIX SCAP content is not currently supported.

C:\tmp\scap_reports_actions\scap_gov.nist_USGCB-Windows-7.xml

Select a datastream from the following choices:

scap_gov.nist_datastream_USGCB-Windows-7-1.2.3.1.zip ▼

Source id: scap_gov.nist_datastream_USGCB-Windows-7-1.2.3.1.zip

Select a benchmark from the following choices:

USGCB: Guidance for Securing Microsoft Windows 7 Systems ▼

Name: USGCB: Guidance for Securing Microsoft Windows 7 Systems

Source id: xccdf_gov.nist_benchmark_USGCB-Windows-7

Description: This guide has been created to assist IT professionals in effectively securing systems running Microsoft 7

Select a profile from the following choices:

United States Government Configuration Baseline 1.2.3.1 ▼

Name: United States Government Configuration Baseline 1.2.3.1

Source id: xccdf_gov.nist_profile_united_states_government_configuration_baseline_version_1.2.3.1

Description: This profile represents guidance outlined in United States Government Configuration Baseline for desktop systems with Microsoft Windows 7 installed.

How strictly should issues and errors in the source XML be handled?

☐ Strict

☒ Lenient (ignore minor issues)

☐ Lax (make a best effort to import the content)

☐ Include OVAL checklists?

☐ Skip OVAL validation?

☐ Skip XML validation?

☐ Allow unescaped HTML in check descriptions? (may contain script tags - use with caution)

3. When the source content has more than one data stream, you can choose the data stream options from the dropdown menu. Select the data stream to import.
4. When the source content has more than one benchmark, you can choose the benchmark options from the dropdown menu. Select the benchmark to import.
5. Select a profile to import from the dropdown menu.
6. Identify how the issues and errors should be handled. Click to select from the following choices:

- Strict
 - Lenient (ignore minor issues)
 - Lax (make a best effort to import the content)
7. Optional: You can choose to apply the following conditions to the Windows checklist that will be imported.
 - Include OVAL checklists - Select this box to process XCCDF rules that reference an entire OVAL file.
 - Skip OVAL validation
 - Skip XML validation
 - Allow unescaped HTML in check description - Use with caution. This option may contain script tags.
 8. Click **Import**.
 9. Select the custom site from the menu.
 10. Click **OK**.

Using the Import SCAP 1.3 Content wizard

The Import SCAP Content wizard is a tool that allows users to load SCAP compliant content, such as security baselines and checklists, into a system for automated compliance scanning.

Overview and Function

The SCAP 1.3 Wizard is an import utility within the BigFix console that enables administrators to import SCAP (Security Content Automation Protocol) benchmark content and automatically generate Fixlets and Analyses for compliance assessment.

This wizard supports both DISA STIG and CIS Benchmarks, allowing you to evaluate endpoints against industry-standard configuration baselines such as USGCB, DISA STIG, CIS, and FDCC.

The wizard parses **XCCDF**, **OVAL**, and **CPE** components defined in SCAP datastreams and generates corresponding BigFix content for assessment and remediation.

Accessing the SCAP Wizard

1. Launch the BigFix console.
2. Navigate to **All Content > Wizards > BES Support > SCM Reporting > Import SCAP 1.3 Content**.
3. Double-click **Import SCAP 1.3 Content** to open the wizard interface.



Note: You must have appropriate operator permissions to import content into a site.

Figure 52. Initial Wizard Screen File Selection - DISA

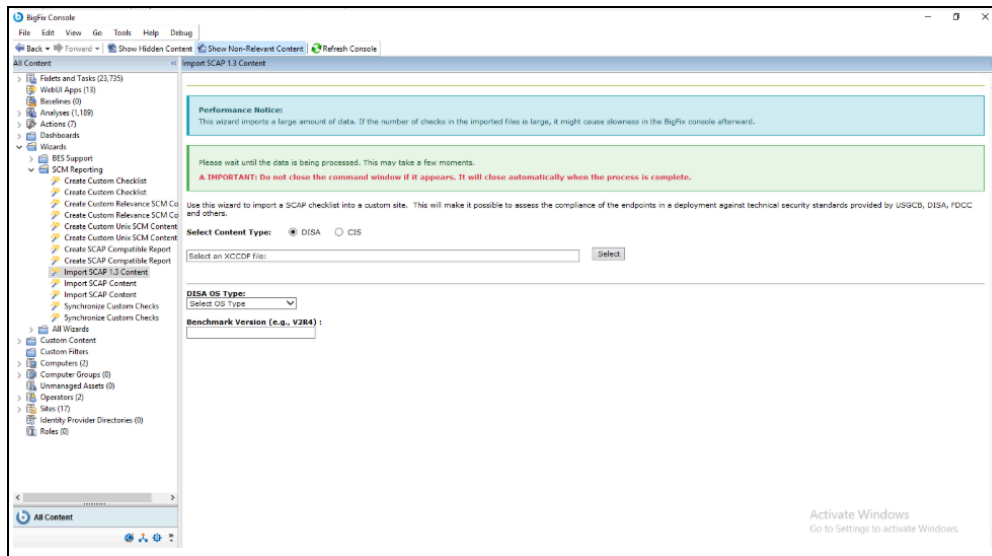
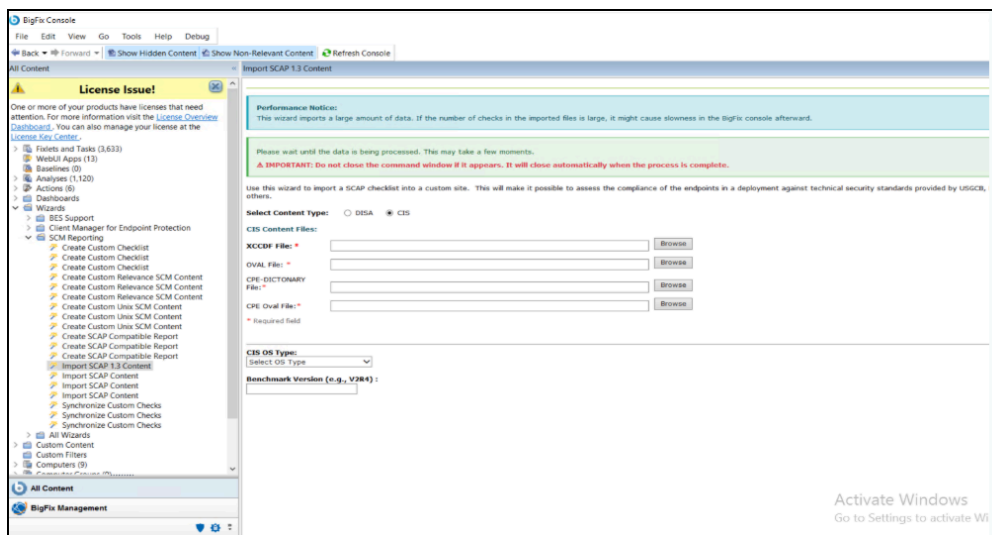


Figure 53. Initial Wizard Screen File Selection - CIS



Wizard Interface Overview

The SCAP 1.3 wizard interface is divided into several sections:

- Content Type Selection (DISA / CIS)
- File Selection Panel
- Datastream / Benchmark / Profile Auto-population
- Target Platform Selection
- OS Type and Benchmark Version Fields
- Import Action & Console Feedback

Using the SCAP 1.3 Wizard

1. Select Content Type

Choose the benchmark type:

- **DISA** - for DISA STIG SCAP benchmarks
- **CIS** - for CIS SCAP benchmarks

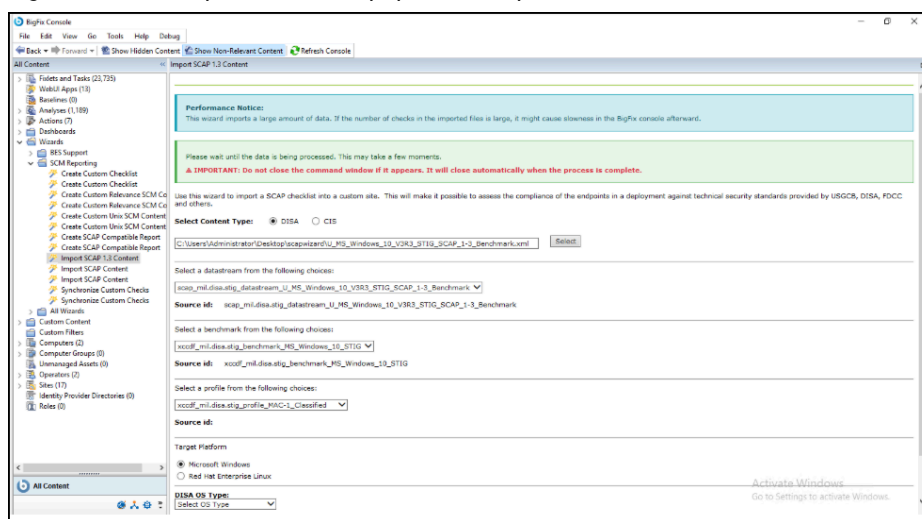
This selection determines which fields and file upload options appear below.

2. Browse and Load Files

Depending on your selection:

- **If "DISA" is selected:**
 - Upload a single XCCDF file (e.g., U_MS_Windows_10_V3R3_STIG_SCAP_1-3_Benchmark.xml).
 - Click **Select**, browse to the file location, and choose the file.
 - Once loaded, the wizard will automatically read the datastream, benchmark, and profile identifiers.

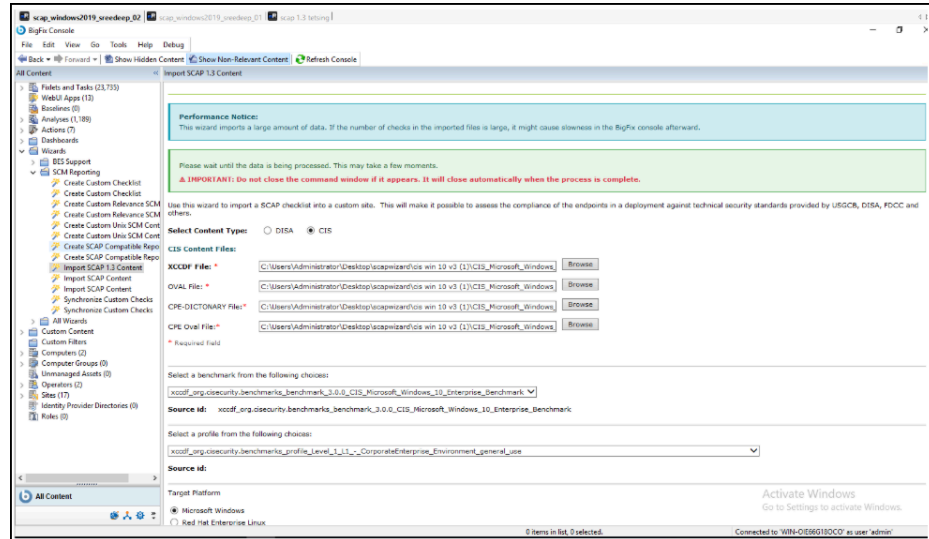
Figure 54. DISA Import View Auto-populated dropdowns



- **If "CIS" is selected:**
 - Upload four files in the correct order:
 - XCCDF File
 - OVAL File
 - CPE Dictionary File
 - CPE OVAL File

- Ensure the file names match the CIS benchmark structure. For example, `CIS_Microsoft_Windows_10_Enterprise_Benchmark_v3.0.0`.
- The wizard will use these files to populate benchmark and profile choices.

Figure 55. CIS Import View Auto-populated dropdowns



3. Wait for Dropdown Auto-population

After selecting the files, wait for the wizard to populate the dropdowns:

- Datastream
- Benchmark
- Profile



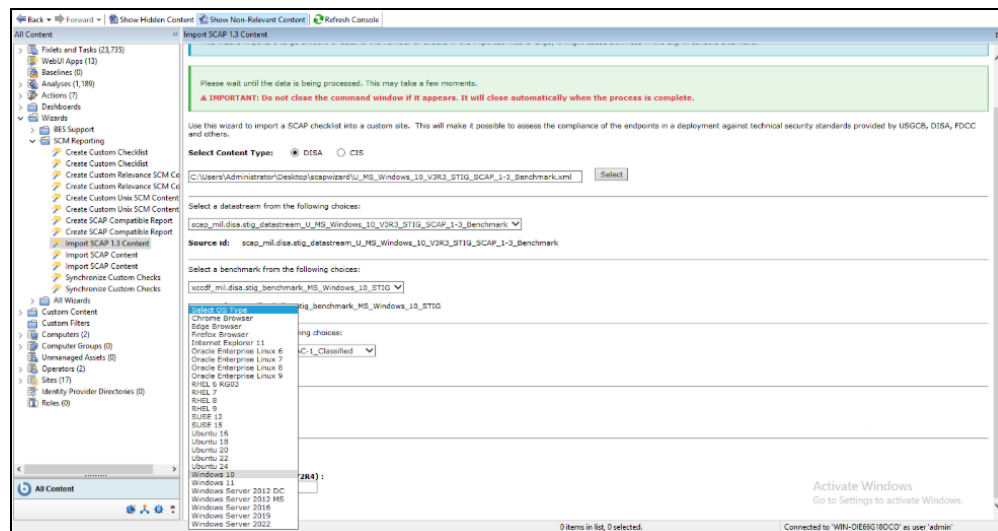
Note: The wizard may temporarily appear unresponsive while parsing XML files. Do not close or switch windows during this time.

4. Select Target Platform and OS Type

Choose the Target Platform (e.g., *Microsoft Windows* or *Red Hat Enterprise Linux*).

Then select the OS Type from the dropdown. *Example: Windows 10, Windows Server 2019 DC, RHEL 8, Edge Browser, etc.*

Figure 56. OS Type Selection Multiple supported platforms



5. Enter Benchmark Version

Provide the Benchmark Version as indicated in the SCAP benchmark file name.

- For DISA, use the following format: v3r3, v2r4, etc.
- For CIS, use the following format: v3.0.0.

This version uniquely tags the generated site content.

6. Import the Content

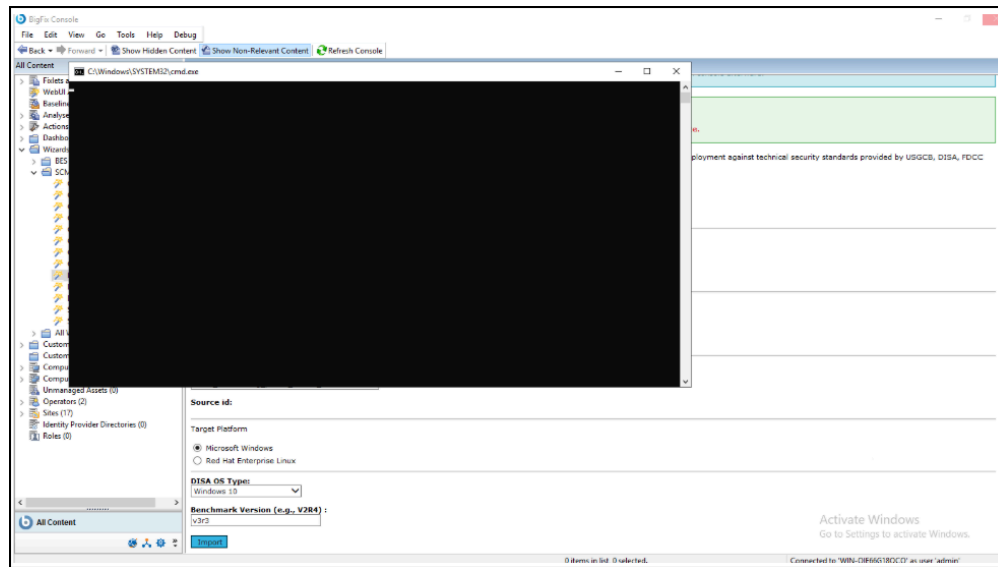
After verifying all fields:

- Click **Import**.
- A **Command Prompt window** opens and executes internal SCAP import logic.
- The console will display a progress message.



Note: Do not close the command prompt window manually. It will close automatically when the import completes successfully.

Figure 57. Processing Stage Command window in execution



7. Review and Create Site

Once the import is successful:

- A **Fixlet Review dialog** appears showing all generated Fixlets and Analyses (e.g., password policy checks, audit rules).
- Review the objects if needed.
- Choose the destination site (recommended: a custom site created for this benchmark).
- Click **OK** to finalize the import.

The new Fixlets and Analyses appear under the selected site in the BigFix Console.

Example Workflow

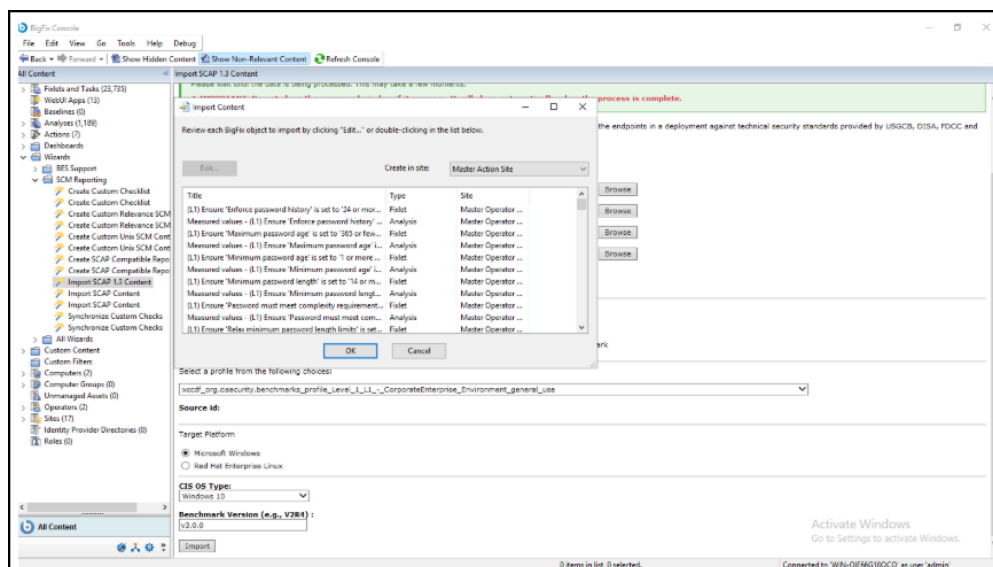
Example: DISA Import

1. Select DISA.
2. Browse and upload: U_MS_Windows_10_V3R3_STIG_SCAP_1-3_Benchmark.xml
3. Wait for auto-populated fields:
 - Datastream: scap_mil.disa.stig_datastream_U_MS_Windows_10_V3R3_STIG_SCAP_1-3_Benchmark
 - Benchmark: xccdf_mil.disa.stig_benchmark_MS_Windows_10_STIG
 - Profile: xccdf_mil.disa.stig_profile_MAC-1_Classified
4. Set **OS Type**: Windows 10.
5. Set **Benchmark Version**: v3r3.
6. Click **Import** and wait for the process to complete.

Example: CIS Import

1. Select CIS.
2. Upload the following:
 - XCCDF: CIS_Microsoft_Windows_10_Enterprise_Benchmark.xml
 - OVAL: CIS_Microsoft_Windows_10_Enterprise_OVAL.xml
 - CPE Dictionary: CIS_Microsoft_Windows_10_Enterprise_CPE_DICTIONARY.xml
 - CPE OVAL: CIS_Microsoft_Windows_10_Enterprise_CPE_OVAL.xml
3. Wait for benchmark and profile dropdowns to populate.
4. Set **OS Type**: Windows 10.
5. Set **Benchmark Version**: v3.0.0.
6. Click **Import** and wait for the import dialog.
7. Select the target site and click OK.

Figure 58. Fixlet Review Popup Import confirmation screen



Important Notes and Warnings

- **Performance Notice:**

The wizard imports a large amount of data. If the benchmark contains hundreds of checks, it may slow down the BigFix Console after import.

- **Do Not Interrupt:**

When the Command Prompt window opens, do not close it manually. It will automatically close once the process completes.

- **Console Responsiveness:**

The BigFix Console may appear unresponsive during processing; this is expected behavior.

- **Site Load Time:**

Import time depends on the number of checks and system resources. You may experience slowness while the Fixlets are created and indexed.

Troubleshooting

Issue	Possible Cause	Resolution
Dropdowns not populated	Large file or slow XML parsing	Wait 2-3 minutes; ensure files are SCAP 1.3-compliant
Command prompt closes instantly	File path or syntax issue	Ensure all file paths are valid and accessible
Console hangs	Large dataset (e.g., >1000 Fixlets)	Wait until processing completes; do not force close
Missing Fixlets post-import	Incomplete upload or invalid XML	Verify benchmark integrity and re-import

References

- NIST SCAP 1.3 Specification: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-126r3.pdf>.
- DISA STIG Benchmarks: <https://csrc.nist.gov/projects/security-content-automation-protocol/scap-releases/scap-1-3>
- CIS Benchmarks: <https://www.cisecurity.org/cis-benchmarks>

Using the Create SCAP Compatible Report wizard

The SCAP Compatible Report wizard helps users create reports that follow SCAP standards. It guides the process of compiling compliance and vulnerability scan results in a standard format, making it easier to share, analyze, and meet regulatory requirements.

The Create SCAP Compatible Report wizard generates SCAP 1.0 and 1.1 XCCDF result files or SCAP 1.2 ARF files. The report replaces the Create SCAP Report wizard.

To generate an SCAP 1.2 ARF file, see the instructions on how to use the SCAP command line tools located here: [SCAP 1.2](#).

1. From the **Security Configuration** domain, go to **All Security Configuration > Wizards > Create SCAP Compatible Report**.
2. Select a report type to generate. You can choose from the following report types:
 - XCCDF Test Result format (Compatible with SCAP 1.0/1.1)
 - ARF Result XML format (Compatible with SCAP 1.2)
3. Depending on the report type, follow these steps.

- XCCDF Test Result format
 - a. Click **Select** to specify an output folder to save the reports into.
 - b. Select additional computer properties by checking the applicable boxes and view each selection in the corresponding Included in Report box on the right.
 - c. Select the target computers. You can target computers by property or computer group. You can also manually enter a list of computers in the designated field. Click **View Computers** to check your selection.

Create SCAP Report

Select a report type: **XCCDF TestResult XML format (Compatible with SCAP 1.0/1.1)** ▼

Select a folder for the files that will be generated: **Select**

Select additional computer properties to include:

<p>Computer properties containing <input type="text"/> Add all</p> <div style="border: 1px solid #ccc; padding: 5px;"> <input type="checkbox"/> Active Directory Path <input type="checkbox"/> Agent Type <input type="checkbox"/> Agent Version <input type="checkbox"/> BES Relay Selection Method <input type="checkbox"/> BES Relay Service Installed <input type="checkbox"/> BES Root Server <input type="checkbox"/> BIOS <input type="checkbox"/> CPU </div>	<p>Included in report Remove all</p> <div style="border: 1px solid #ccc; padding: 5px;"> <input checked="" type="checkbox"/> Computer Name </div>
---	---

Select a checklist: **SCAP10_USGCB_WIN7** ▼

Select one or more computers:

☐ All computers with the values selected below
☐ All computers within the selected computer group
☒ The computers specified in the list of names below (separated by spaces or newlines)

- ARF Result XML format
 - a. Re-enter the console operator's password. The console operator will be re-authenticated with the HCL BigFix server.
 - b. Click **Select** to choose the SCAP 1.2 checklist source file that matches the target checklist against which the report will be generated.
 - c. If there are multiple data streams in the source file, select the data stream that matches the target checklist against which the report will be generated.
 - d. Click **Select** to choose the file location where you are saving the report.

- e. Select a custom site checklist from the dropdown menu that corresponds to the SCAP 1.2 checklist that was selected in step b.
- f. Select the target computers. You can target computers by property or computer group. You can also manually enter a list of computers in the designated field. Click **View Computers** to check your selection.

Create SCAP Report

Select a report type: **ARF Result XML format (Compatible with SCAP 1.2)** ▼

Reauthentication required. Enter password:

Select SCAP 1.2 checklist or legacy OVAL definitions file: **Select**

Select a data stream: **<Default>** ▼

Save report as: **Select**

Select a checklist: **SCAP_USGCB_WIN7** ▼

Select one or more computers:

☐ All computers with the values selected below
☐ All computers within the selected computer group
☒ The computers specified in the list of names below (separated by spaces or newlines)

View computers

Create

4. Click **Create**.

Allocate adequate time for the creation of these reports. The amount of time to generate a report depends on the size of your deployment. For example, creating a report for a deployment of 5,000 computers can take 15 minutes on a properly-sized console computer.



Note: A warning might display stating that the data stream failed to be retrieved. You can safely ignore the warning which shows when the source content does not contain a data stream.

Using the Create SCAP 1.3 Compatible Report wizard

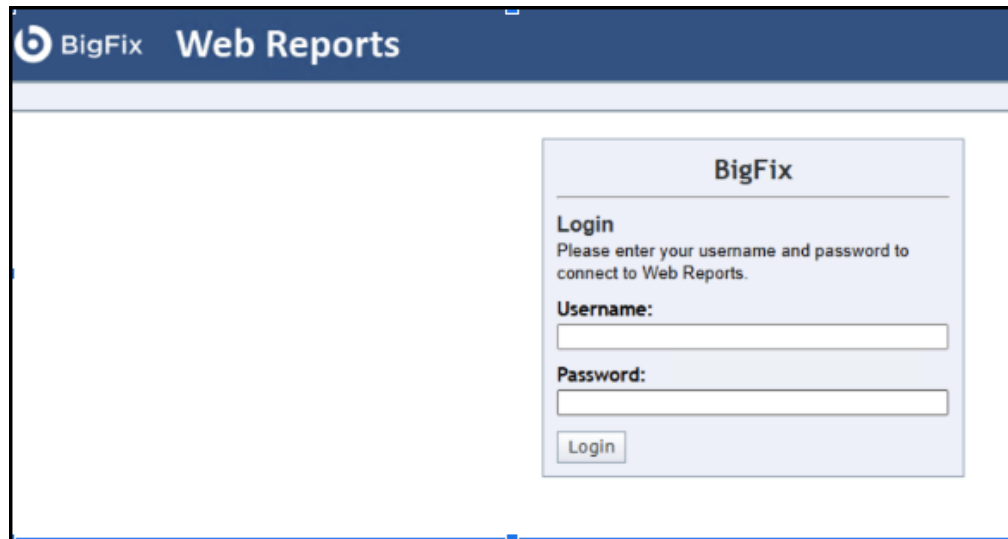
The SCAP Compatible Report wizard helps users make reports that follow SCAP standards. It guides the process of compiling compliance and vulnerability scan results in a standard format, making it easier to share, analyze, and meet regulatory requirements. This guide explains how to use the Web Reports interface to create a compliance report in the Asset Reporting Format (ARF).

For optimal performance and compatibility, use Microsoft Edge or Google Chrome as your browser when running ARF reports.

To generate an SCAP 1.3 ARF file, see the instructions on how to use the SCAP command line tools located here: [SCAP 1.3](#).

How to Launch Web Reports from BigFix console:

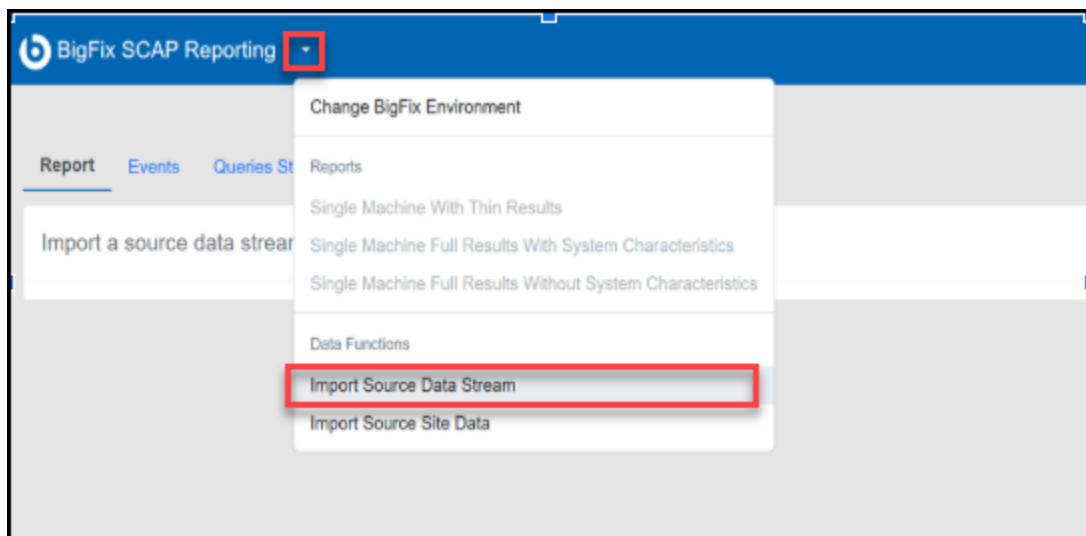
- Open the **BigFix Console**.
- Navigate to **Tools** → **Launch Web Reports**.
- Enter your **web report credentials** when prompted.



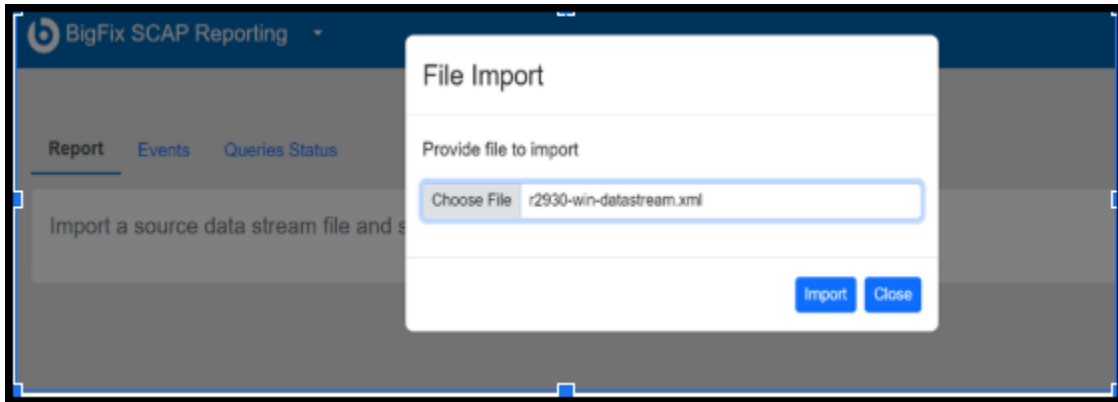
- Click on **Report List**.
- Select **ARF Report Generator 1.0.71b** from the list.

Follow the steps below to generate the ARF report:

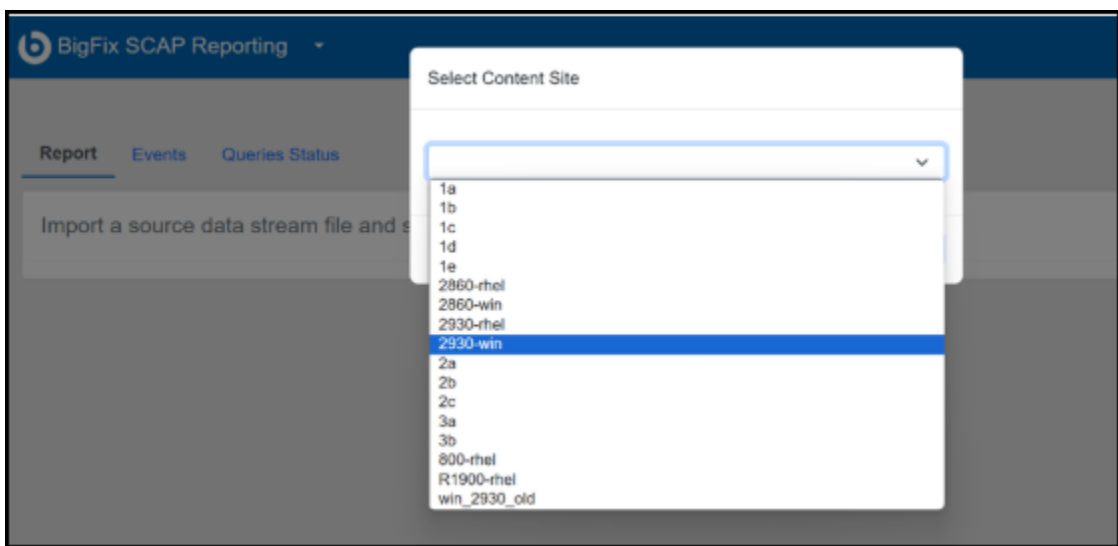
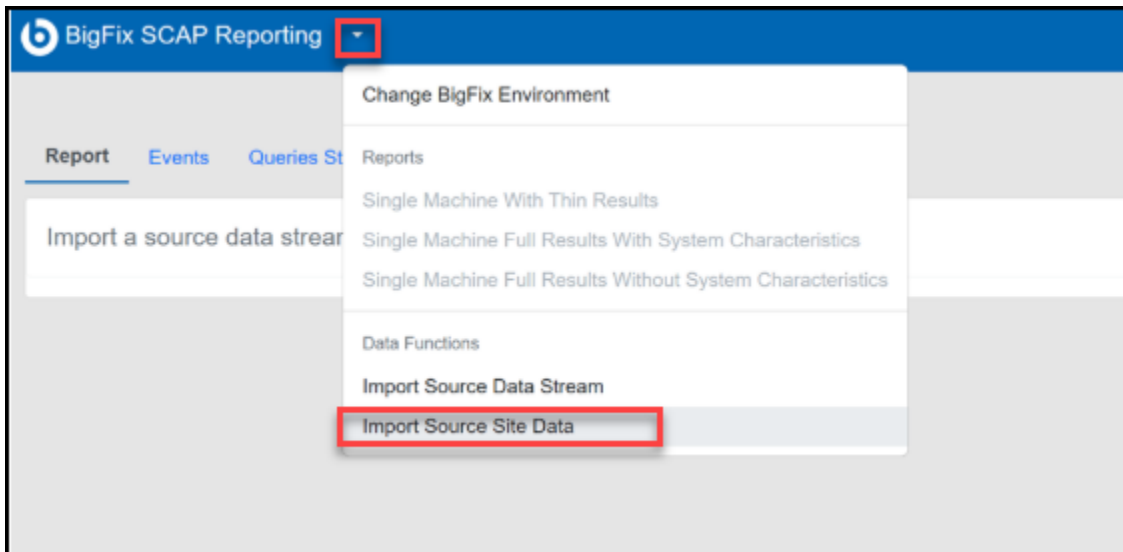
1. Click the dropdown arrow beside **BigFix SCAP Reporting** to expand the menu.



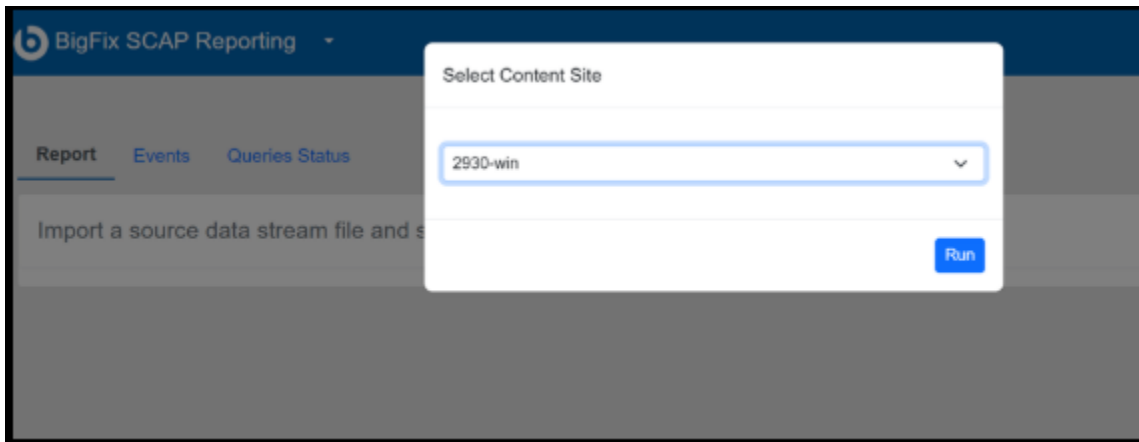
2. Click the **Import Source Data Stream** and choose a datastream file to import.



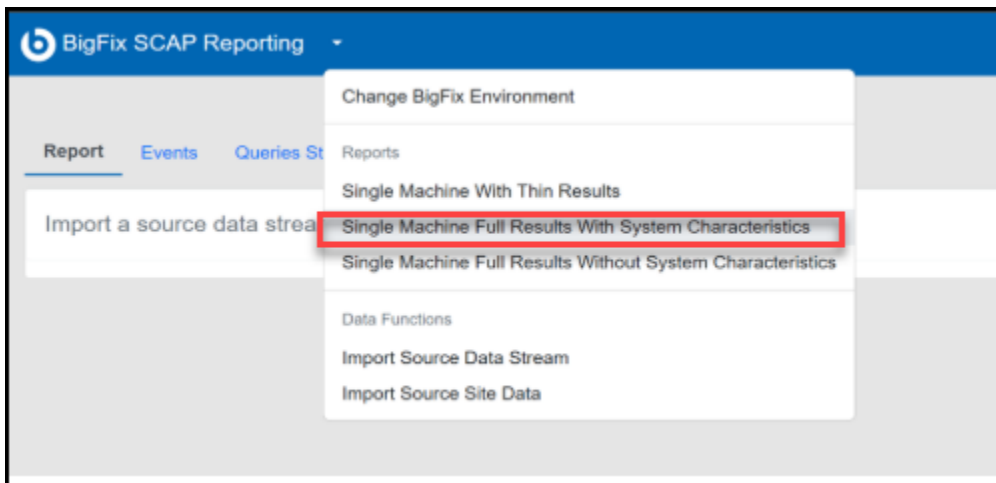
3. Click on **Import Source Site Data** and select the **Custom Site** from the dropdown menu.



4. Click the **Run** button.



5. Once the run is complete, select the report view titled **Single Machine Full Results with System Characteristics** to generate the ARF report.



BigFix SCAP Reporting - ARF Report Types Summary



Note: Single Machine With This Results

- Key Data Included: Evaluation Results (TestResult) ONLY.
- System Characteristics: No (Minimal Data).
- Best Use Case: Quick verification, debugging, minimal metadata needs.



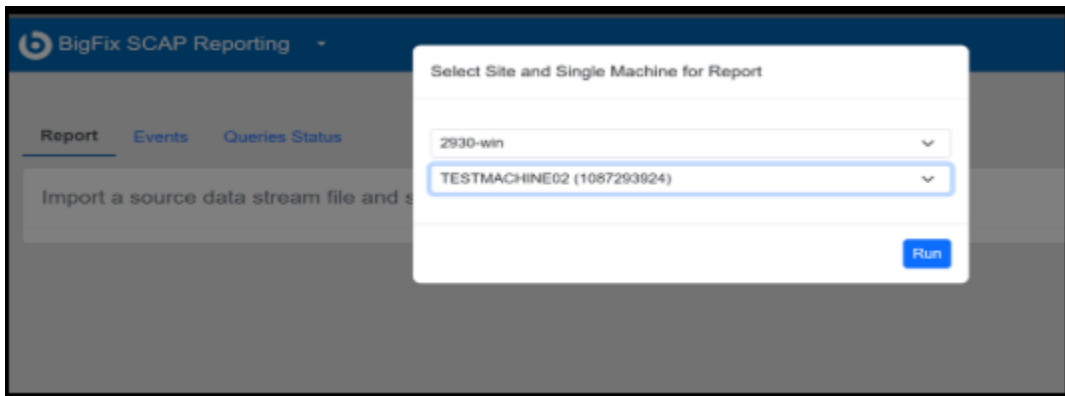
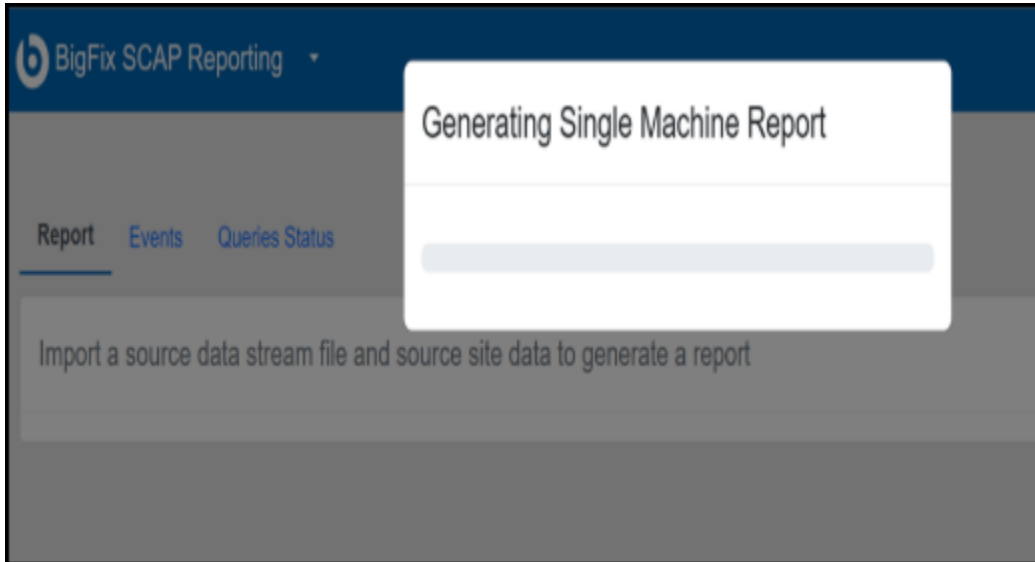
Note: Single Machine Full Results With System Characteristics

- Key Data Included: Evaluation Results (TestResult) + System Characteristics (oval-system-characteristics).
- System Characteristics: Yes (Full Data).
- Best Use Case: Official NIST SCAP 1.3 certification, compliance submissions, full audit.

**Note: Single Machine Full Results Without System Characteristics**

- Key Data Included: Evaluation Results (TestResult) ONLY.
- System Characteristics: No (Anonymized Data).
- Best Use Case: Privacy-conscious export, combining reports (aggregation), data redaction.

6. Select the specific endpoint (machine) for which you wish to generate the compliance report.



7. On the generated report view, click the **Download Report** button. The ARF result file will be downloaded with the generic name: `xmlresult.xml`.

Rule ID	Definition ID	Severity	Result
xccdf_gov.nist_rule_r2930_SV-48018r1_rule	oval:gov.nist.validation.r2930-win:def:4212	low	pass
xccdf_gov.nist_rule_r2930_SV-48024r1_rule	oval:gov.nist.validation.r2930-win:def:4149	low	pass
xccdf_gov.nist_rule_r2930_SV-48034r1_rule	oval:gov.nist.validation.r2930-win:def:4142	medium	pass
xccdf_gov.nist_rule_r2930_SV-48042r1_rule	oval:gov.nist.validation.r2930-win:def:4173	low	pass
xccdf_gov.nist_rule_r2930_SV-48052r1_rule	oval:gov.nist.validation.r2930-win:def:4211	low	pass
xccdf_gov.nist_rule_r2930_SV-48053r1_rule	oval:gov.nist.validation.r2930-win:def:4210	high	pass
xccdf_gov.nist_rule_r2930_SV-48055r1_rule	oval:gov.nist.validation.r2930-win:def:4152	medium	pass
xccdf_gov.nist_rule_r2930_SV-48057r1_rule	oval:gov.nist.validation.r2930-win:def:4154	low	pass
xccdf_gov.nist_rule_r2930_SV-48062r1_rule	oval:gov.nist.validation.r2930-win:def:4215	low	pass
xccdf_gov.nist_rule_r2930_SV-48063r1_rule	oval:gov.nist.validation.r2930-win:def:4170	low	pass
xccdf_gov.nist_rule_r2930_SV-48064r1_rule	oval:gov.nist.validation.r2930-win:def:3939	high	pass
xccdf_gov.nist_rule_r2930_SV-48070r1_rule	oval:gov.nist.validation.r2930-win:def:4195	high	pass

- It is essential to rename the generated `xmlresult.xml` to a more meaningful name based on the datastream used. For example: If the datastream is `r.400.1.1`, rename the file to `r.400.1.1.xml`.

You now have a properly generated and named ARF report ready for use or submission.

Using OVALDI

Security Configuration Management uses Oval Interpreter (OVALDI), an open-source reference implementation that uses OVAL to scan computer vulnerabilities and generate OVAL full results.

The Oval Interpreter (OVALDI) is a freely available reference implementation that demonstrates the evaluation of OVAL definitions. Using command line interface, OVALDI collects and evaluates system information to generate an OVAL Results file based on a set of Definitions. OVALDI is under BSD license. For more information about OVALDI, see Fixlet 9 in the SCM Reporting site.

Chapter 8. Configuration Management Reporting

In previous releases, the primary reporting tools for the Configuration Management solution included the Configuration Management dashboard, Exception Management dashboard, and Web Reports. These tools, while still accessible for customers with previously-saved reports and exceptions, have now been superseded by Security and Compliance Analytics, which is included in all Configuration Management subscription packages.

For more information about BigFix Compliance Analytics, see the [Security and Compliance Analysis User Guide](#).

Chapter 9. Frequently asked questions

Can I parameterize all checks?

Not all checks can be parameterized using the Fixlet user interface we provide. In cases where a check can be parameterized, the method depends on the type of content. See the Configuration Management Checklists Guide for more information.

Are remediation actions available for all checks?

Remediation actions are available for a subset of checks.

Where can I find a sample file containing UNIX parameters?

See the Configuration Management Checklists Guide.

Are there compliance evaluation reports/mechanisms that compare a laptop or server against FISMA/NIST/DISA standards?

Configuration Management checks assess servers, laptops, and desktops against a predefined set of configuration guidance such as DISA STIG and FDCC.

HCL BigFix also supports configuration standards from NIST, NSA, and other standards organizations. Regulatory compliance regulations such as FISMA, PCI, and others can easily be supported by customizing the checklists provided by HCL.

What happens if I subscribe sites incorrectly to a system?

Each Configuration Management site applies to a specific operating system or product. It is important that each computer subscribed to each site matches the correct operating system configuration. This ensures the accuracy of the compliance results for each Configuration Management site, and prevents potential performance issues. External sites contain site relevance to ensure that only applicable computers are subscribed. However, custom sites do not support site relevance, so you are responsible for maintaining accurate subscriptions.

When I run a remediation action on a UNIX endpoint, how do I ensure that a system is not remediated more than once?

When a remediation action is run, the remediation action reruns the detection script. When the detection script is run, it provides the validation of whether or not the remediation was successful. If successful, the Fixlet becomes non-relevant. If unsuccessful, the Fixlet remains relevant.

What does the letter designation mean on the end of some of the scripts within the UNIX content?

We used the DISA STIG unique identifiers as part of the naming convention for each DISA STIG control that was built. In the case where we had to separate a single control into multiple scripts, the scripts include a letter designator on the end that provides a unique ID for each control.

What is the security associated with the base parameter file that defines the parameters for the UNIX content?

The standard permissions for this file are 700 (RWE for the owner of the file). In this case, the owner must be root or whichever user is the owner of the BES Client.

When using the Create SCAP Compatible Report wizard, a warning displays stating that the data stream failed to be retrieved. What should I do?

You can safely ignore the warning which shows when the source content does not contain a data stream.

Chapter 10. 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](#)

Chapter 11. 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.