

**BigFix Compliance
Security Configuration Management
(SCM) App in WebUI User Guide**



Special notice

Before using this information and the product it supports, read the information in [Notices \(on page 51\)](#).

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. Welcome to the SCM App in WebUI.....	5
Chapter 2. What's new in SCM App in WebUI.....	6
Chapter 3. System requirements.....	8
Chapter 4. Supported benchmarks.....	9
Chapter 5. SCM App in WebUI: Overview.....	11
Custom checklist.....	13
Viewing a custom checklist.....	13
Creating a custom checklist.....	17
Deploying a custom checklist.....	21
Synchronizing a custom checklists.....	25
Modifying check parameters.....	28
Custom check.....	29
Creating a custom check using relevance.....	30
Creating a custom check using Unix content.....	33
Editing a custom check.....	36
Deleting a custom check or checks.....	37
External checklist.....	40
Viewing an external checklist.....	40
Deploying an external checklist.....	42
Exporting report.....	46
Inline reports.....	47
Chapter 6. Support.....	50
Chapter 7. Notices.....	51

Chapter 1. Welcome to the SCM App in WebUI

Security Configuration Management (SCM) is a collection of checks and checklists that organizations can use to configure devices and ensure that the devices meet compliance standards.

SCM App in WebUI utilizes the new WebUI design to provide a streamlined workflow for better user experience in managing devices in a BigFix network. With the SCM App, operators can manage the security configuration of the devices with the help of benchmarks such as CIS, DISA STIG, FDCC, PCI DSS, USGCB, and custom checklists.

With SCM App checks and checklists, security teams can define the security parameters and configurations that corporate policies require. It also helps the operators assess and manage device configurations through checks, checklists, synchronization and provides remediation action if devices do not meet compliance standards. Operators focus on the detailed day-to-day configuration management of all devices.

Chapter 2. What's new in SCM App in WebUI

This topic provides information about the new features and updates in SCM App in WebUI.

What's new in v1.1.0

The SCM App in WebUI includes the following features:

- **Landing page:** Implementation of data grid for custom and external checklists in the SCM App landing page allows you to view, search, and sort checklists based on various properties such as No. of checks, created, updated, subscribed device count, platform, and status.
- **Create:** You can create both custom checklist and check using the **Create** drop-down in the landing page.
- **Compliance check creation wizard:** This wizard allows you to create checks using **SCM relevance** and **Unix content** method.
- **Inline reports:** SCM App leverages the **Inline reports** feature available in BigFix WebUI and generates a donut chart and bar graphs for the selected custom or external checklist. These chart and graph provide an overall status of the checklist by assessing the available checks in both custom or external checklist. For more information, see [Viewing a custom checklist \(on page 13\)](#) and [Viewing an external checklist \(on page 40\)](#).
- **Checklist details page:** Added four new columns in the contents tab of custom checklist details page and external checklist details page. The new columns are **deployment percentage**, **undeployed device count**, **compliance percentage**, and **non-compliant devices count** which also contributes to inline reporting. Additionally, **Content ID** column is added in the external checklist details page. For more information on Inline reporting, see [Inline reports \(on page 47\)](#).
- **Export:** This feature allows you to customize and download the custom or external checklist reports in **.csv**, **.xlsx**, and **.pdf** formats. For more information, see [Exporting report \(on page 46\)](#).
- **Show/Hide summary:** This feature allows you to display and hide the inline reports for both custom and external checklist.
- **Modifying checks:** You can edit or delete a custom copy of a check or the checks which are created and added to the custom checklist. Also, you can add multiple relevance and remediation script when you edit the check. For more information, see [Editing a custom check \(on page 36\)](#).

Features added in previous version

The following updates were released with SCM App in WebUI v1.0.0:

- **Landing page:** Shows all the available custom and external checklist with details such as number of checks, updated information, number of subscribed devices, status of checklist (out of sync or new or refreshed) and site information in a tile or list view.
- **Data Grid:** By implementing a data grid in SCM App, you can quickly view the checks in a tabular format and use the features such as filter, search, and sort to find checks quickly. For more information on the data grid, see [Grid View](#).

- **Create Custom Checklists:** Create checklist by using **multiple external checklists** that result in managing a large category of devices.
- **Custom Checklist Affected:** Lists all the custom checklist that are affected by the external checklist.
- **New and Refreshed External checklists:** Representation of newly published or refreshed external checklists with icons.
- **Deployment Summary:** Quick access to other WebUI apps such as Devices and Deployments from SCM App.

Chapter 3. System requirements

SCM App in WebUI requires certain system requirements to work in your environment, this topic provides the necessary information to use SCM App.

You must meet the following requirements to use SCM App:

- Ensure that you have any one of the BigFix Compliance licenses:
 - Security and Compliance
 - Security and Compliance POC
 - Starter Kit for Security and Compliance
 - Starter Kit for Security and Compliance POC
- Enable the required SCM (external) sites from the **License Overview** dashboard in BigFix Console. For more information on how to enable SCM sites, see [Subscribing with the Licensing Dashboard](#).
- Subscribe to SCM reporting in BigFix Console. For more information on how to subscribe to SCM reporting, see [Subscribing to the SCM reporting site](#).
- Devices 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 BigFix console version that you installed. For more information, see the [BigFix Configuration Guide](#).
- Enable JavaScript in the browser. For instruction on how to enable JavaScript visit <https://support.google.com/admanager/answer/12654?hl=en>.
- You must have a Master Operator (MO) access to create custom checklists in SCM App.

The following tables lists the supported browser, BigFix components and operating systems:



Note: Currently, SCM App do not support synchronization feature in Linux-based operating systems.

Table 1. Supported browser and components

Components	Requirements
Supported browsers	<ul style="list-style-type: none">• Google Chrome v93.0 or later• Microsoft Edge v93.0 or later• Mozilla Firefox v92.0 or later• Safari v13.x or later
BigFix component versions	<ul style="list-style-type: none">• Agent v9.5 or later• Console v9.5 or later• Platform v9.5 or later• Server v9.5 or later• WebUI v9.5 or later

Chapter 4. Supported benchmarks

BigFix Compliance SCM provides checklists that are created based on the following security configuration benchmarks:

Center for Internet Security (CIS)

The CIS guidelines recommend technical control rules and values that apply to network devices, operating systems, software applications, and middleware applications. The 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 files 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/cis-benchmarks/>.

Defense Information System Agency (DISA) Security Technical Implementation Guidelines (STIG)

The DISA STIG provides recommendations for secure installation, configuration, and maintenance of software, hardware, and information systems. The DISA STIG is one of the bases of configuration standards that the US government uses.

For more information about the DISA STIG, see <https://public.cyber.mil/stigs/>.

Payment Card Industry Data Security Standard (PCI DSS)

The 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 devices and servers in your organization, and it can help your organization protect devices to meet security compliance for PCI DSS.

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

For more information about PCI DSS, see the PCI Security Standards Council resources:

- www.pcisecuritystandards.org/security_standards/
- [Payment Card Industry Data Security Standard \(PCI DSS\) User's Guide](#)

Federal Desktop Core Configuration (FDCC)

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

United States Government Configuration Baseline (USGCB)

The USGCB provides guidance for the security configuration of Information Technology products that US government federal agencies deploy. USGCB addresses the following platforms Microsoft 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.

USGBC replaced the Federal Desktop Core Configuration (FDCC).

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

Chapter 5. SCM App in WebUI: Overview

The SCM App landing page lists all the custom and external checklists that are used to manage devices.

To navigate to the SCM App, log in to the **WebUI** and select **SCM** from the **Apps** menu.

Figure 1. SCM App in WebUI: Overview

Checklist Name	No. of checks	Created	Updated	Subscribed ...	Platform	Status
DISA Windows 2016-complianceReport	220	DISA Windows 201...	DISA Windows 201...	3	All Other	<none>
CIS MSSQL Server 2019	44	CIS MSSQL Server ...	CIS MSSQL Server ...	3	MS SQL Server 2019	Out of Sync
MSSQL2019_Console	39	MSSQL2019_Cons...	MSSQL2019_Cons...	3	MS SQL Server 2019	<none>
DISA STIG Checklist Windows 2016	211	DISA STIG Checkli...	DISA STIG Checkli...	0	All Other	<none>
CIS Windows 10	425	CIS Windows 10	CIS Windows 10	0	All Other	<none>
DISA Windows 10	229	DISA Windows 10	DISA Windows 10	3	All Other	<none>
CIS Checklist for Windows 2016	339	CIS Checklist for ...	CIS Checklist for ...	3	All Other	Out of Sync
CIS MS SQL Server 2016	43	CIS MS SQL Server ...	CIS MS SQL Server ...	3	MS SQL Server 2016	Out of Sync

The SCM App landing page contains the following elements:

- **Custom checklists:** This tab lists all the available custom checklists which are created by Master Operators (MO). The number in the parentheses indicates the number of available custom checklists. On top of the data grid you have number of available custom content and pagination feature to navigate.

Each column in the custom checklists tab contains the following information:

- **Checklist Name:** Shows the name of the custom checklist, a **out of sync** icon appears when the custom checklist has to be synced with its source (external checklist).
- **No. of checks:** Shows the total number of checks in the custom checklist.
- **Created:** Shows the date of checklist creation.
- **Updated:** Shows the date of the last update of the custom checklist.
- **Subscribed Device:** Shows the number of devices that are subscribed to the custom checklist.
- **Search or Filter and Sort:** Every column gives an option to search or filter, you can view the newest updated checklist first or the oldest updated checklist first using the sort icon the column header.



Note: It is recommended to create a custom checklist based on an external checklist and deploy a custom checklist to applicable devices. For more information on creating and deploying custom checklist, see [Creating a custom checklist \(on page 17\)](#) and [Deploying a custom checklist \(on page 21\)](#).

- **External checklists:** This tab lists all external checklists that are implemented by the BigFix Compliance team based on benchmarks such as CIS, DISA STIG, FDCC, PCI DSS, and USGCB. Use these checklists to create custom checklists. The number in the parentheses indicates the number of available external checklists. On top of the data grid you have number of available custom content and pagination feature to navigate.

Figure 2. External checklist

Checklist Name	No. of checks	Created	Updated	Benchmark version	Platform	Benchmark	Status
DISA STIG Checklist for Windows 2008 R2 MS	262	04/26/2019	10/25/2019	<none>	All Other	DISA	<none>
DISA STIG Checklist for Windows 2012 MS	284	03/05/2021	06/30/2021	<none>	All Other	DISA	<none>
CIS Checklist for Windows 10	425	07/12/2021	12/24/2021	<none>	All Other	CIS	<none>
DISA Checklist for Windows 10	229	04/08/2022	07/22/2022	<none>	All Other	DISA	<none>
CIS Checklist for CentOS Linux 6	196	01/30/2017	06/22/2020	<none>	All Other	CIS	<none>
CIS Checklist for Mac OS X 10.12	80	11/04/2016	04/24/2019	<none>	OSX 10.12	CIS	<none>
CIS Checklist for Windows 2016 DC	351	07/12/2021	08/12/2022	<none>	All Other	CIS	<none>
CIS Checklist for Windows 2016 MS	254	07/12/2021	08/12/2022	<none>	All Other	CIS	<none>

Each column in the custom checklists tab contains the following information:

- **Checklist Name:** Shows the name of an external checklist.

Different icons display the status of the checklist:

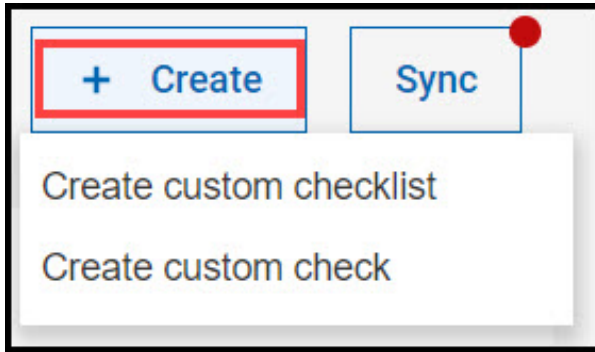
New

Appears when an external checklist is newly published in last 7 days.

Refreshed

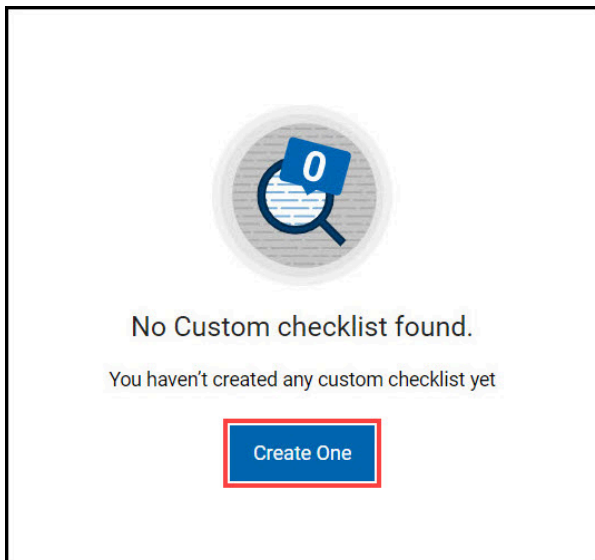
Appears when an external checklist is updated (refreshed) in last 7 days.

- **No. of checks:** Shows the total number of checks in an external checklist.
- **Created:** Shows the date of checklist creation.
- **Updated:** Shows the date of the last update of the custom checklist.
- **Benchmark:** Shows the version details of the benchmark.
- **Search or Filter and Sort:** Every column gives an option to search or filter, you can view the newest updated checklist first or the oldest updated checklist first using the sort icon the column header.
- **Create:** Operator uses **Create** function to create Custom checklists and Custom checks. For more information, see [Creating custom checklist \(on page 17\)](#), [Creating a custom check using relevance \(on page 30\)](#), and [Creating a custom check using Unix content \(on page 33\)](#).



Note: **Create** function will be disabled for Non-Master Operators (NMOs) if access to custom content is set as "No" in BigFix console.

When you log in to SCM App for the first time or you do not have any custom checklist created, you are prompted with the following screen:



You can create a custom checklist by clicking **Create One** or **Create**.

- **Sync:** Sync function allows operators to synchronize checklists. For more information, see [Synchronizing custom checklist \(on page 25\)](#).

Custom checklist

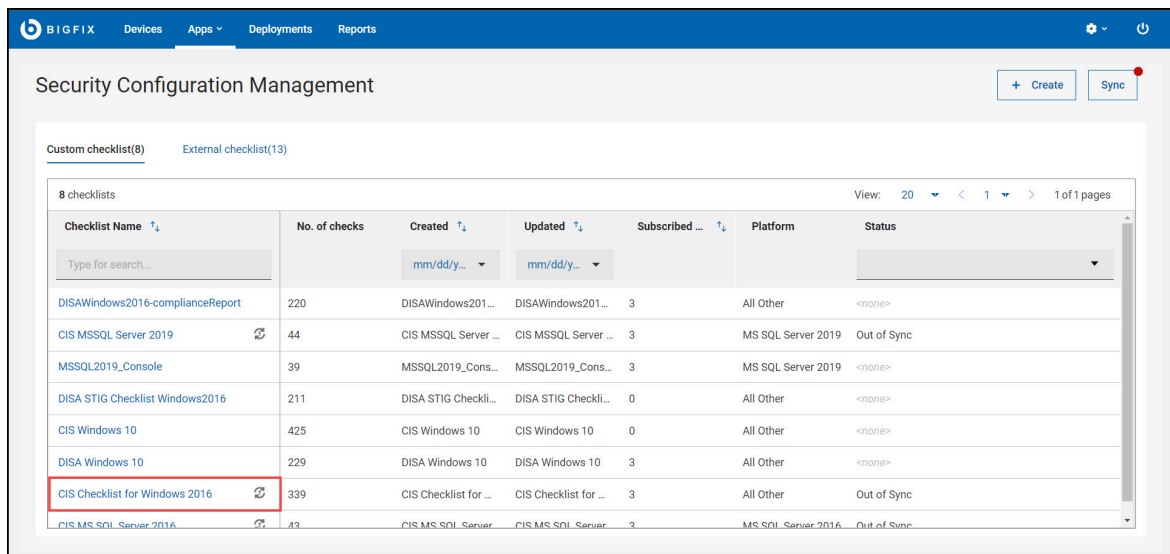
A custom checklist is a modified version or a copy of an external checklist. These checklists are created by using one or more external checklists. With custom checklists, Master Operators (MO) can exclude certain checks from an external checklist and deploy those checklists to any device.

Viewing a custom checklist

Understand how to view a custom checklist and its overview.

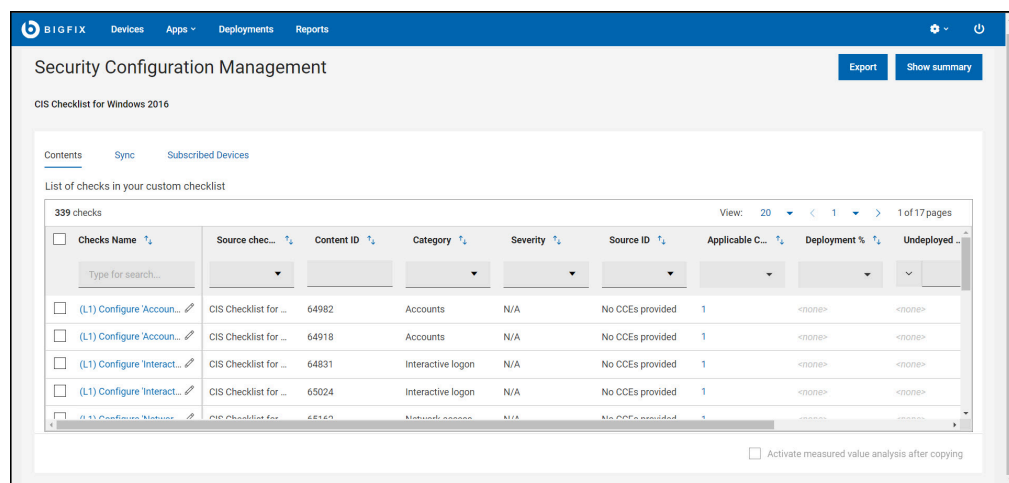
Perform the following steps to view a custom checklist:

1. Navigate to the SCM App landing page and click **Custom checklist**.



You are directed to the custom checklist details page which contains the **Contents**, **Sync**, and **Subscribed devices** tabs that provides information about the selected custom checklist.

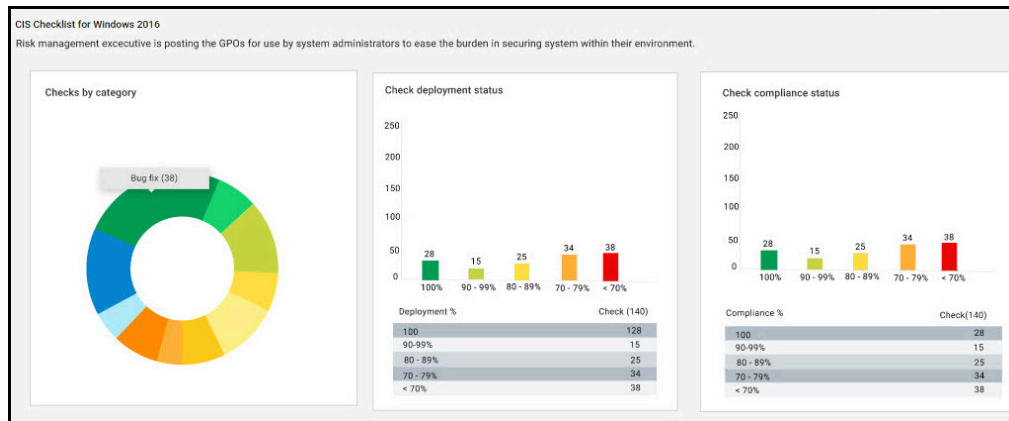
Figure 3. Custom checklist details page



The custom checklist page contains the following elements:

- **Export:** Use this feature to download reports of an individual custom checklist. For more information, see [Exporting report \(on page 46\)](#).
- **Show/Hide summary:** Use this feature to display or hide the inline reports.

• Inline reports:



Donut chart and bar graphs, such as **checks by category**, **check deployment status**, and **check compliance status** shows the status of the selected custom checklist. These chart and graphs are updated dynamically when you apply filters in contents tab. You can also click on any of the chart or graphs to see information related to specific set of checks.

Inline reports chart and graphs:

- **Checks by category:** The checks are grouped together based on the custom site they belong to. For example, account management, password policies, auditing and network security are the few category of checks.
- **Check deployment status:** This graph is generated based on the deployment percentage checks.
- **Check compliance status:** This graph is generated based on the compliance percentage of the checks.

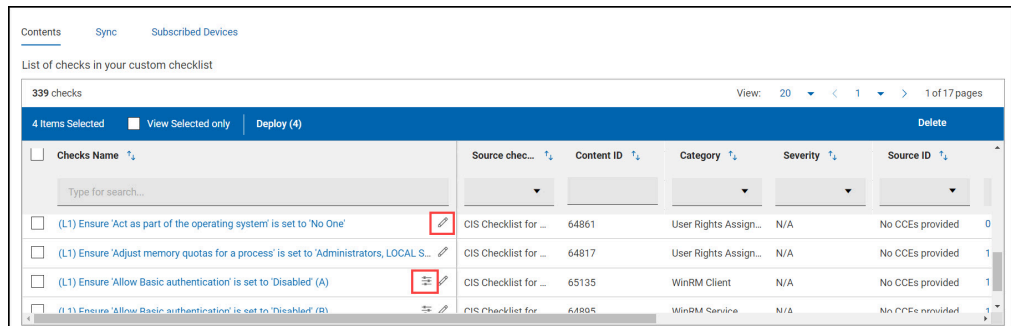
For more information, see [Inline reports \(on page 47\)](#).

- **Custom checklist tabs:** The checks in the **Contents** and **Sync** tabs are represented in a data grid format. Each column has a search or filter option, which you can use to find checks by entering text or a keyword. The pagination allows you to navigate between pages. Use the checkbox in each row to select the required checks or select all the checks using the checkbox available in header section of **Checks Name** column. To view only the checks that you have selected, use **View Selected only**. To know more about data grid, see [Grid view](#).






Note: On the lower-right corner, the checkbox represents if **Activate measured value analysis after copying** option is checked or unchecked for the custom checklist. For more information on activate measured value analysis after copying, see [Measured value analysis \(on page 20\)](#).

- **Contents:** This tab contains all the available checks in a custom checklist. You can select one or more checks and deploy them to the target devices by clicking **deploy**. For more information on deploying custom content, see [Deploying a custom checklist \(on page 21\)](#).

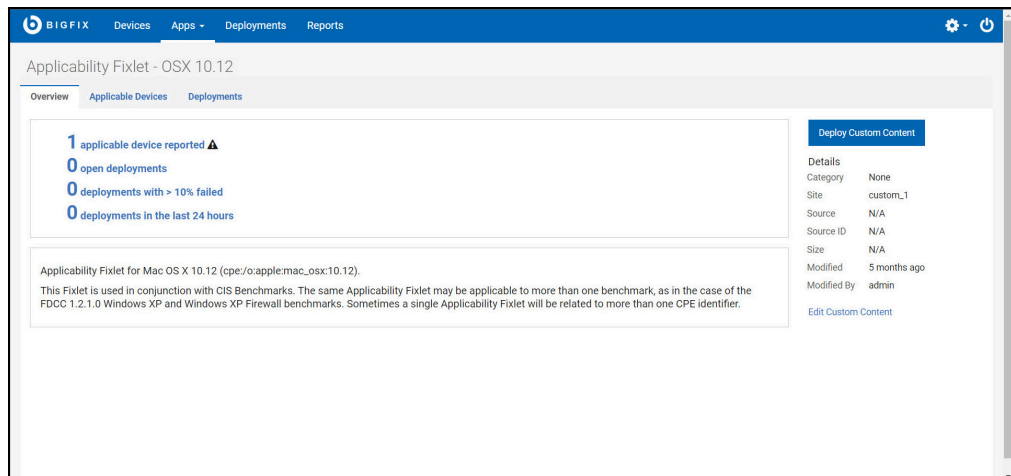


You can modify the parameters used in determining the compliance of checks. Use **Edit**

parameter  icon to customize the checks. Similarly, use **Edit check**  edit the contents of the check. For more information, see [Modifying check parameters \(on page 28\)](#) and [Editing a custom check \(on page 36\)](#).

When a new check is created and added to a custom checklist, it is indicated by a  icon and it is categorized as **Custom** under source checklist column.

You can view the details of the check by clicking any of the available checks. The details page contains Overview, Applicable Devices and Deployment sections.



- **Sync:** This tab contains the list of checks to be synced with the source checklist (external checklist). You can select one or more checks (Out of Sync checks) and sync them with the source checklist by clicking **Sync Selected**. For more information on synchronization, see [Synchronizing custom checklist \(on page 25\)](#).

Contents Sync **Subscribed Devices**

Select any check and sync with your checklists.

352 checks View: 20 1 1 of 18 pages

4 Items Selected View Selected only Sync Selected (4)

<input type="checkbox"/>	Checks Name ↑	Source chec... ↑	Source ID ↑	Category ↑	Severity ↑	Status ↑
<input type="text" value="Type for search..."/>						
<input checked="" type="checkbox"/>	(L1) Configure 'Accounts: ...	CIS Checklist for ...	No CCEs provided	Accounts	N/A	Out Of Sync
<input checked="" type="checkbox"/>	(L1) Configure 'Accounts: ...	CIS Checklist for ...	No CCEs provided	Accounts	N/A	Out Of Sync
<input checked="" type="checkbox"/>	(L1) Configure 'Interactive...	CIS Checklist for ...	No CCEs provided	Interactive logon	N/A	Out Of Sync
<input checked="" type="checkbox"/>	(L1) Configure 'Interactive...	CIS Checklist for ...	No CCEs provided	Interactive logon	N/A	Out Of Sync

- **Subscribed Devices:** This tab contains all the available devices that a custom checklist can be applied to. You have **Groups**, **All devices**, and **None** options to apply the checklist.

Contents Sync **Subscribed Devices**

Manage subscription to this checklist

☒ Groups ☐ All devices ☐ None Update

4 groups View: 20 1 1 of 1 pages

<input type="checkbox"/>	Group Name ↑	Member count ↑
<input type="text" value="Type for search..."/>		
<input type="checkbox"/>	SCM_Computer_Group	1
<input type="checkbox"/>	SCM_GROUP_2	0
<input type="checkbox"/>	SCM_Automatic_Computer_Group	1
<input type="checkbox"/>	SCM_Manual_Computer_Group	1

- **Groups:** This list contains available device groups in SCM. You can apply the checklist to one or more groups.
- **All devices:** Checklist is applied to all the devices in SCM.
- **None:** Checklist is applied to any device.

A success message is displayed after applying the checklist to any selected groups or all devices.

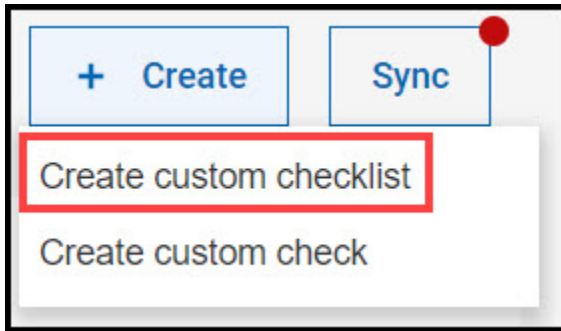
Creating a custom checklist

This task helps you in creating a custom checklist from one or more external checklist.

1. You must be subscribed to SCM Reporting.
2. You must have Master Operator (MO) access to create custom checklist.

Perform the following steps to create a custom checklist:

1. Navigate to the SCM App landing page and click **Create > Create custom checklist**.



2. Enter the **Name** and **Description** of the new checklist and click **Next**.

A screenshot of the 'Create custom checklist' form in the BIGFIX Security Configuration Management app. The form is titled 'Create custom checklist' and has a progress bar with four steps: 1. General, 2. Target platform and source checklists, 3. Check Selection, and 4. Review. The 'General' step is active. It contains two text input fields: 'Name' and 'Description'. The 'Name' field has a red arrow pointing to it and contains the text 'Win_10_Custom_Checklist'. The 'Description' field has a red arrow pointing to it and contains the placeholder text 'Enter text'. A 'Next' button is located at the bottom right of the form, highlighted with a red box. The top of the page shows the BIGFIX logo and navigation tabs for 'Devices', 'Apps', and 'Deployments'. An 'Exit' button is in the top right corner.

! **Important:** The **Name** field has text validation enabled. It notifies you when an existing checklist name is used. In the Description field, you can add information related to the custom checklist. You cannot use characters such as double quotation, tabs, and new lines or carriage returns in either fields.

3. Select the **Target Platform, Benchmark** from the drop-down, select the **Checklist**, and click **Next**.

The screenshot shows the 'Create custom checklist' wizard in the BIGFIX Security Configuration Management app. The wizard has four steps: 1. General, 2. Target platform and source checklists (current), 3. Check Selection, and 4. Review. In Step 2, the 'Target Platform*' is set to 'All Others'. Under 'Source Checklist* (2)', there are two benchmarks selected: 'CIS Checklist for RHEL 7 (228)' and 'CIS Checklist for Windows 10 (430)'. A search bar is available to find benchmarks. On the right, a list of created checklists is shown with their creation dates. At the bottom right, there are 'Previous' and 'Next' buttons, with 'Next' highlighted in red.



Note: The benchmarks in the **Source Checklist** entries vary with the **Target Platform** selection. Each target platform has different benchmarks linked to them. You can also use **Search** to find the benchmarks.

4. Select the **Checks** to include in the new custom checklist and click **Review**.


The screenshot shows the 'Create custom checklist' wizard in the BIGFIX Security Configuration Management app, Step 3: Check Selection. The wizard has four steps: 1. General, 2. Target platform and source checklists, 3. Check Selection (current), and 4. Review. In Step 3, there are 229 checks available. A table displays the selected checks. The table has columns: Checks Name, Source checklist, Source ID, Category, Severity, and Applicable Compu... (Applicable Computers). Four items are selected, indicated by green checkmarks in the first column. At the bottom right, there are 'Previous' and 'Review' buttons, with 'Review' highlighted in red.

Checks Name	Source checklist	Source ID	Category	Severity	Applicable Compu...
<input checked="" type="checkbox"/> Account Lockout Duration	USGCB Checklist for Wind...	CCE-2363-0, CCE-980	Account Lockout Policy Se...	N/A	0
<input checked="" type="checkbox"/> Account Lockout Threshold	USGCB Checklist for Wind...	CCE-3177-3, CCE-658	Account Lockout Policy Se...	N/A	0
<input checked="" type="checkbox"/> Accounts: Administrator account status	USGCB Checklist for Wind...	CCE-3032-0, CCE-499	Security Options Settings (...)	N/A	0
<input checked="" type="checkbox"/> Accounts: Guest account status	USGCB Checklist for Wind...	CCE-3248-2, CCE-332	Security Options Settings (...)	N/A	0
<input type="checkbox"/> Accounts: Limit local account use to ...	USGCB Checklist for Wind...	CCE-2398-6, CCE-533	Security Options Settings (...)	N/A	0



Note:



- If required, you can modify the parameters using **Edit parameter**  icon. For more information on modifying parameters, see [Modifying check parameters \(on page 28\)](#).
- Not all checks in custom checklist can be parameterized. For example, **Ensure Latest SQL Server Service Packs and Hotfixes are Installed** check will only confirm if the devices meet the described criteria. So this check cannot be parameterized

5. Review the selected parameters and click **Create Checklist**.



Note: If required, select **Activate measured value analysis after copying** before you create the checklist.

Checklists include analyses that provide the actual values of the items being checked. Measured values are retrieved using analysis properties. By default, measured value analysis will be added to the custom checklist while creating a custom checklist. When **Activate measured value analysis after copying** is enabled it makes the measured value analyses to be activated globally.

By default, measured value analysis is added to the custom checklist while you create a custom checklist. When **Activate measured value analysis after copying** is enabled, it activates the measured value analyses globally.

You are directed to the custom checklist details page when the custom checklist is created, which contains **Contents**, **Sync** and **Subscribed Devices** tabs. For more information on custom checklist details page, see [Viewing a custom checklist \(on page 13\)](#).

The screenshot shows the 'Security Configuration Management' app interface. The top navigation bar includes 'BIGFIX', 'Devices', 'Apps', 'Deployments', and 'Reports'. The main header is 'Security Configuration Management' with 'Export' and 'Show summary' buttons. Below the header, there's a section for 'CIS Checklist for Windows 2016' with tabs for 'Contents', 'Sync', and 'Subscribed Devices'. The main content area displays a table of checks with columns: Checks Name, Source chec..., Content ID, Category, Severity, Source ID, Applicable C..., Deployment %, and Undeployed ... The table shows 339 checks in total, with a view of 20 items per page. The first few rows show checks related to 'Accounts' and 'Interactive logon'.

Checks Name	Source chec...	Content ID	Category	Severity	Source ID	Applicable C...	Deployment %	Undeployed ...
(L1) Configure 'Accoun...	CIS Checklist for ...	64982	Accounts	N/A	No CCEs provided	1	<none>	<none>
(L1) Configure 'Accoun...	CIS Checklist for ...	64918	Accounts	N/A	No CCEs provided	1	<none>	<none>
(L1) Configure 'Interact...	CIS Checklist for ...	64831	Interactive logon	N/A	No CCEs provided	1	<none>	<none>
(L1) Configure 'Interact...	CIS Checklist for ...	65024	Interactive logon	N/A	No CCEs provided	1	<none>	<none>

Deploying a custom checklist

Use this task to deploy a custom checklist to one or more targets.

Perform the following steps to deploy a custom checklist:


1. Navigate to the SCM App landing page and click the **Custom checklist** to deploy.

The screenshot shows the 'Security Configuration Management' app interface. The top navigation bar includes 'BIGFIX', 'Devices', 'Apps', 'Deployments', and 'Reports'. The main header is 'Security Configuration Management' with '+ Create' and 'Sync' buttons. Below the header, there's a section for 'Custom checklist(8)' and 'External checklist(13)'. The main content area displays a table of checklists with columns: Checklist Name, No. of checks, Created, Updated, Subscribed ..., Platform, and Status. The table shows 8 checklists in total, with a view of 20 items per page. The 'CIS Checklist for Windows 2016' is highlighted with a red box.

Checklist Name	No. of checks	Created	Updated	Subscribed ...	Platform	Status
CIS MSSQL Server 2019	44	CIS MSSQL Server ...	CIS MSSQL Server ...	3	MS SQL Server 2019	Out of Sync
MSSQL2019_Console	39	MSSQL2019_Cons...	MSSQL2019_Cons...	3	MS SQL Server 2019	<none>
DISA STIG Checklist Windows2016	211	DISA STIG Checkli...	DISA STIG Checkli...	0	All Other	<none>
CIS Windows 10	425	CIS Windows 10	CIS Windows 10	0	All Other	<none>
DISA Windows 10	229	DISA Windows 10	DISA Windows 10	3	All Other	<none>
CIS Checklist for Windows 2016	339	CIS Checklist for ...	CIS Checklist for ...	3	All Other	Out of Sync
CIS MS SQL Server 2016	43	CIS MS SQL Server...	CIS MS SQL Server...	3	MS SQL Server 2016	Out of Sync




2. Select the **Checks** and click **deploy**.

**Note:**

- If required, you can modify the parameters using **Edit parameter**  icon. For more information on modifying parameters, see [Modifying check parameters \(on page 28\)](#).
- Not all checks in custom checklist can be parameterized. For example, **Ensure Latest SQL Server Service Packs and Hotfixes are Installed** check will only confirm if the devices meet the described criteria. So this check cannot be parameterized.

3. Review the available tasks and click **Next**.

Different icons display the state of the tasks:

-  : The task is not associated with the action. Click the **delete** icon to remove the task.
-  : Check the parameter of the task. You can click the  icon and edit the parameter of the task.

Deploy Custom Content

☒ Select custom content
 ☒ **Select action**
☐ Select targets
 ☐ Configure

9 Tasks Clear All (9)

- Check System Wide Applications f... Action1 Click here to remediate this issue.
- Configure account lockout thresho... Action1 Click here to remediate this issue.
- Configure Security Auditing Flags -... Action1 Click here to remediate this issue.
- Deploy and Run Security Checklist ... Action1 Click here to deploy and scan.
- Disable "Allow guests to connect t... Action1 Click here to remediate this issue.
- Disable "Show password hints" - D... Action1 Click here to remediate this issue.
- Disable "Wake for network access" ... Action1 Click here to remediate this issue.

Deployment Summary

Deployment Name
Multiple Action Group

9 Tasks

Back Next →



Note: You can also rename the **Deployment Name** in **Deployment Summary** panel.

4. Select the **Target** and click **Next**.

Deploy Custom Content

☒ Select custom content
 ☒ Select action
 ☒ **Select targets**
☐ Configure

Target by device Target by group Target by properties Target by client relevance

2 devices View: 20 1 of 1 pages

1 Item Selected View Selected only

Computer Name	Critical Patches	Applicable P...	Deployments	Device Type	OS	Groups
localhost.localdomain	No	0	0	Server	SLE 15	<none>
<input checked="" type="checkbox"/> DESKTOP-1N003P0	No	0	69	Server	Windows 10	<none>

Deployment Summary

Deployment Name *
Multiple Action Group

3 Tasks

1 Target
DESKTOP-1N003P0

Back Next →



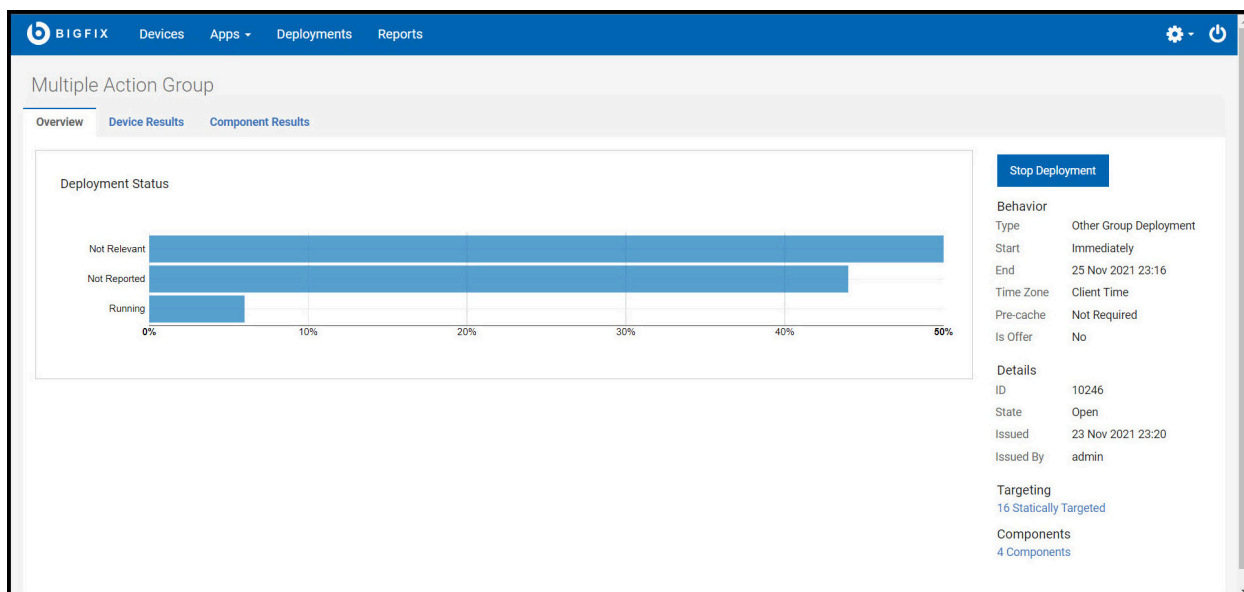
Note: You can use the **Target by Device** and **Target by Group** subtabs for selecting the targets.

5. Customize your deployment and click **Deploy**.

**Note:**

- Use the **Edit** icon in the subtabs (Run, Users, Messages, Offer, and Post-Action) on the left panel to further fine-tune the deployment. For more information on the subtabs, see [Configuration Options](#).
- Use the **Edit** icon in the Deployment Summary panel to modify tasks and targets.

The Deployment page displays details such as overview, device, and component results. You can also stop the deployment any time by clicking **Stop Deployment**.



- **Overview:** Detailed description of the selected deployment status, behavior, targeting, and more.
- **Device Results:** Target status, which is - the state of the deployment on each endpoint.
- **Component Results:** For content with multiple actions: the deployment status of each component on targeted devices is expressed as a percentage of completion.

You can also view the status of the current or previous deployments in WebUI by clicking **Deployments** in the navigation bar. For more information on deployments, see [The Deployment List](#).




Important:

SCM deployments are categorized under the **Other** application type. Use Deployment Name, Issued Date, or other criteria to find deployments.

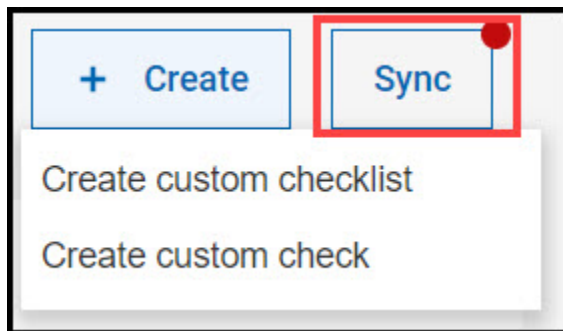
Synchronizing a custom checklists

Use Synchronize custom checklist to update custom checklists in your deployment whose sources (external checklists) have been updated.

An out of sync  icon is displayed on the custom checklist tile and those checklists must be synchronized with their sources (external checklists).

Perform the following steps to synchronize the custom checklist:

1. Navigate to the SCM App landing page and click **Sync**.



2. Click **View and sync** on any checklist to sync.

The Synchronize custom checklist page gives an overview of the checklists that are to be synchronized.

Security Configuration Management

Synchronize custom checklist

The following custom checklists have updates to be synced

Custom DISA for Windows 10	No. of checks: 20	Created : 2021-11-23T05:44:25.987Z	View and Sync
Includes updates from: DISA STIG Checklist for Windows 2008 R2 DC DISA STIG Checklist for Windows 2012 DC DISA STIG Checklist for Windows 2012 MS DISA Checklist for Windows 10 DISA STIG Checklist for RHEL 8	Bigfix version:24, Benchmark version: Windows Server 2008 R2 Domain Controller Security Technical Implementation Guide 1 Release 31 Bigfix version:15, Benchmark version: Windows 2012_and_2012_R2 Domain Controller Security Technical Implementation Guide Version 3 Release 2 Bigfix version:16, Benchmark version: Windows 2012_and_2012_R2 Member Server Security Technical Implementation Guide Version 3 Release 1 Bigfix version:18, Benchmark version: Windows 10 Security Technical Implementation Guide Version 2 Release 1 Bigfix version:2, Benchmark version: Red Hat Enterprise Linux 8 Security Technical Implementation Guide Version 1 Release 2		
KT session abc	No. of checks: 1	Created : 2021-10-07T06:08:35.670Z	View and Sync
Includes updates from: CIS Checklist for MS SQL Server 2012 DB Engine	Bigfix version:9, Benchmark version: CIS_Microsoft_SQL_Server_2012_Benchmark_v1.6.0		
Custom DISA for Mac	No. of checks: 10	Created : 2021-11-23T05:47:34.007Z	View and Sync
Includes updates from: DISA STIG Checklist for Windows 2012 DC	Bigfix version:15, Benchmark version: Windows 2012_and_2012_R2 Domain Controller Security Technical Implementation Guide Version 3 Release 2		

3. Select the required **Check** or use the **select all** option to select all available checks and click **Sync Selected**.

Security Configuration Management

CIS Checklist for Window 10

Contents Sync Subscribed Devices

Select any check and sync with your checklists.

430 checks View: 20 < 1 > 1 of 22 pages

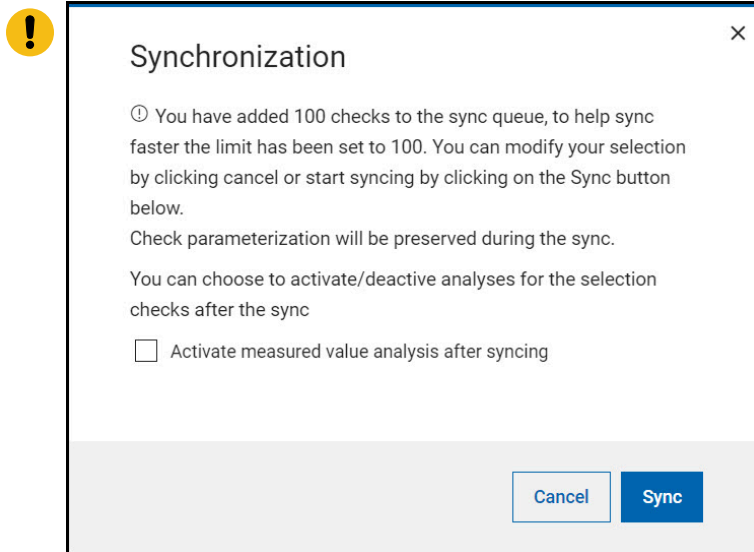
20 Items Selected ☐ View Selected only **Sync Selected**

Checks Name	Source chec...	Source ID	Category	Severity	Status
(L1) Ensure 'Access Cred...	CIS Checklist for ...	No CCEs provided	User Rights Assign...	N/A	Out Of Sync
(L1) Ensure 'Access this c...	CIS Checklist for ...	No CCEs provided	User Rights Assign...	N/A	Out Of Sync

☒ Activate measured value analysis after copying



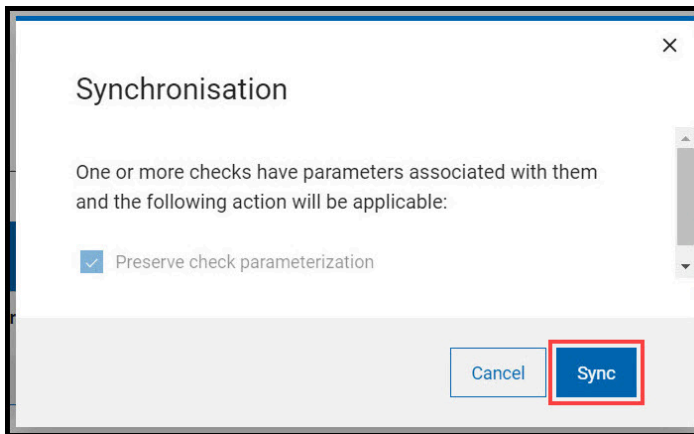
Important: You can select up to 100 checks at a time to synchronize. This limitation is to improve the performance of the operation.





4. If a selected check has no associated parameters, the synchronisation starts. If the checks have associated parameters, you are prompted with the following dialog box:


- Click **Sync**.

During synchronization, special indicators shows the status such as in progress or error of each individual check.



When synchronized, the status is displayed next to each individual checks. The results are as follows:

-  : Successfully updated the check to the custom site.
-  : Failed to updated the check to the custom site.

 **Note:** In some cases, successfully synchronized check will be removed from the data grid.

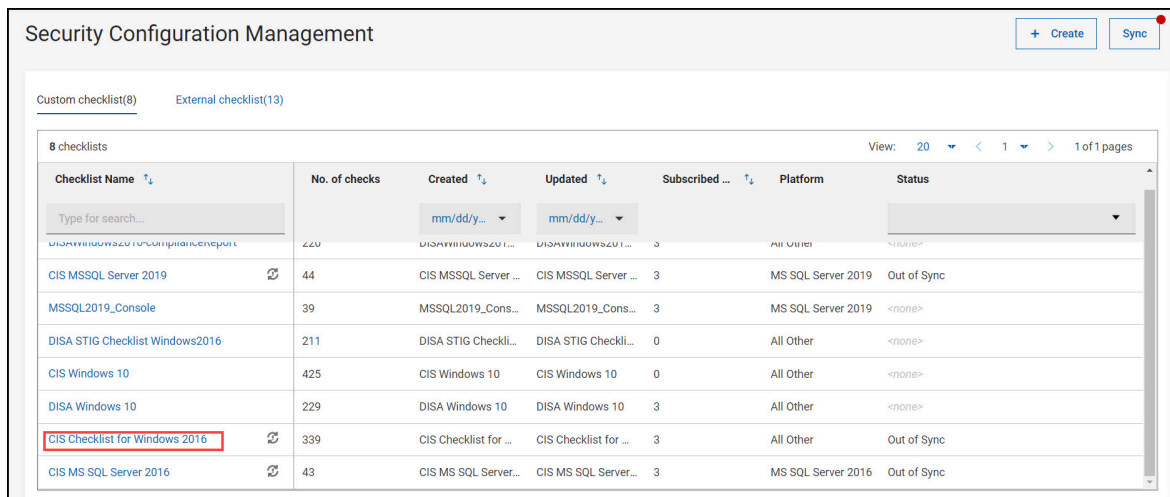
Modifying check parameters

Custom checklist contains multiple checks. You can only modify the copies of checks located in custom checklist. For example, in a **Account lockout threshold** check, you can set the maximum number of failed login attempts before the account is locked to any desired value.

You can modify only parameters of checks in custom checklists.

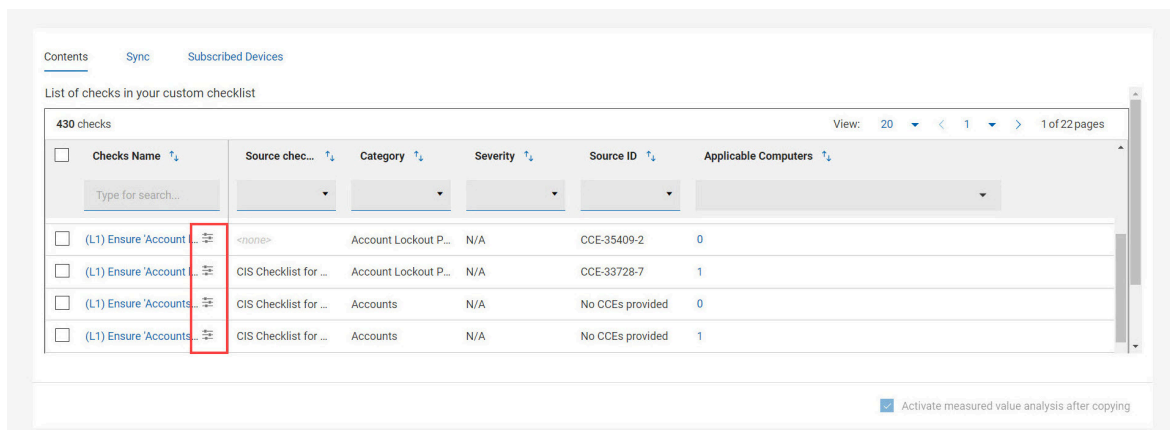
Perform the following steps to modify check in custom checklist:

1. Navigate to the SCM App landing page and click the **Custom checklist** from the data grid.



Checklist Name	No. of checks	Created	Updated	Subscribed	Platform	Status
CIS MSSQL Server 2019	44	CIS MSSQL Server ...	CIS MSSQL Server ...	3	MS SQL Server 2019	Out of Sync
MSSQL2019_Console	39	MSSQL2019_Cons...	MSSQL2019_Cons...	3	MS SQL Server 2019	<none>
DISA STIG Checklist Windows2016	211	DISA STIG Checkli...	DISA STIG Checkli...	0	All Other	<none>
CIS Windows 10	425	CIS Windows 10	CIS Windows 10	0	All Other	<none>
DISA Windows 10	229	DISA Windows 10	DISA Windows 10	3	All Other	<none>
CIS Checklist for Windows 2016	339	CIS Checklist for ...	CIS Checklist for ...	3	All Other	Out of Sync
CIS MS SQL Server 2016	43	CIS MS SQL Server...	CIS MS SQL Server...	3	MS SQL Server 2016	Out of Sync

2. Click **Edit Parameter** icon.



Checks Name	Source check	Category	Severity	Source ID	Applicable Computers
(L1) Ensure 'Account Lockout Threshold' is set to 5	<none>	Account Lockout P...	N/A	CCE-35409-2	0
(L1) Ensure 'Account Lockout Threshold' is set to 5	CIS Checklist for ...	Account Lockout P...	N/A	CCE-33728-7	1
(L1) Ensure 'Accounts' are locked out for 30 minutes	CIS Checklist for ...	Accounts	N/A	No CCEs provided	0
(L1) Ensure 'Accounts' are locked out for 30 minutes	CIS Checklist for ...	Accounts	N/A	No CCEs provided	1



Note: Not all checks in custom checklist can be parameterized. For example, checks such as **Ensure Latest SQL Server Service Packs and Hotfixes are Installed** will only confirm if the devices meet the described criteria. So this check cannot be parameterized.

3. Enter the **Desired value** on the **Edit Parameters** pop-up window and click **Save**.

CPEs
cpe:/o:microsoft:windows_10

Check compliance: (Condition 1 and Condition 2)

Condition 1: LockoutBadCount (A)
Details: security_database('LockoutBadCount')
Compliant if: values.oval?({all, :at_least_one_exists}) {is| s.to_i <= input.to_i }
Default value: 5

Desired value: ←

Condition 2: LockoutBadCount (B)
Details: security_database('LockoutBadCount')
Compliant if: values.oval?({all, :at_least_one_exists}) {is| s.to_i > input.to_i }
Default value: 0

Desired value: ←

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

Cancel Save

A success/failure toast notification appears on the top-right corner.

Custom check

A custom checklist includes many checks which enables the security teams to preserve the compliance standards of an organisation. Similarly, checks within a checklist perform various type of actions and ensures the pre-defined parameters of the checks are met.

Based on the roles and permissions in BigFix console Master operator (MO) and Non-master operator (NMO) can perform various activities.

With SCM App in WebUI you can create, edit, or delete one or more checks. You must meet the following prerequisites to create, edit, or delete a check:

- Ensure that you have a custom checklist that is created through **Create custom checklist** wizard in the SCM App.
- Ensure that the custom checks are up to date and that bug fixes are installed with the **Synchronize Custom Checks** wizard in the WebUI.
- Ensure that you have **Owner** and **Write** permission for the checklist to create, edit, and delete a check.

The following table lists the activities that a MO and NMO can perform under specific condition:

Activity	Master operator (MO)	Non-master operator (NMO)
Create a custom check	Yes	Yes ⁽¹⁾

Activity	Master operator (MO)	Non-master operator (NMO)
Delete or Edit a custom check	Yes	Yes ⁽¹⁾
View a custom check	Yes	Yes ⁽²⁾

**Note:**

1. Access to **custom content** must be "Yes" in BigFix console roles and permission. When roles and permission is set to "No", you cannot create, edit or delete a check even if you **owner** or **write** permission for the checklist.
2. You must have read permission to view a custom check.

Creating a custom check using relevance

This task helps you in creating a custom check using relevance.

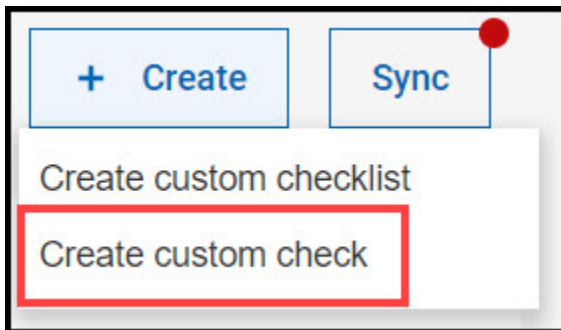
Ensure that you have **Owner** or **Write** permission for the checklist to add new checks.

Perform the following steps to create a custom check by using relevance method:



Note: At any point, if you decide to create custom check using Unix content, you can switch using the radio button available in the **Compliance check creation** wizard. The fields and field values in **Required information** and **Description** compliance creation wizard remains unchanged but, the values in the **Behavior** section will be deleted. For more information, see [Creating a custom check using Unix content \(on page 33\)](#).

1. Navigate to the SCM App landing page and click **Create > Create custom content**.



Compliance check creation wizard appears.



Note: **Create using relevance** is the default method in the **Compliance check creation** wizard.

Security Configuration Management

Compliance check creation

☒ Create using relevance
 ☐ Create Unix SCM checks using bourne shell script

▼ **Required Information**

Title

Placeholder Text

Site

Site

Applicability Fixlet

Fixlet

Source

Source

Source ID

Source ID

Source Release date

yyyy-mm-dd

Category

Select Category

Severity

Select Severity

2. In the **Required information** section, provide the following information:

- Title
- Site
- Source
- Source ID
- Source Release date
- Category
- Severity



Note:

- Based on the **Site** selection, the **Compliance check creation** wizard will auto-generate the required information for **Applicability Fixlet** and you can select the **Applicability Fixlet** from the drop-down if the site has more than one Fixlet.
- **SourceID** must be unique in the checklist.
- **SourceID** field must start with alphanumeric characters and may contain hyphen and underscore.
- If you want to add a new category which does not exist in the custom site, you can add it by clicking **Add new Category**.

3. In the Description section, enter the **Description** of the custom check.

▼ **Description**

B U I :: | = @

This is a required field.



Note:



- Description field is must be filled in order to create a custom check.
- You can customize the description field texts using text format option.

4. In the **Behavior** section, select **Relevance**.

5. Click **Check syntax** to validate the entered relevance.



Note:

- If the entered syntax is incorrect, an error appears.
- Use **Add new relevance** option to add multiple relevance to your custom check, **Delete this relevance** option to delete the added relevance and **Clear** to delete the client relevance.

6. Add **Analysis** to the custom check.



Note: You can add only one **Analysis** when creating custom check.

- Including **Analysis** to the custom check:

- Check **Include desired value**.
- Enter the **Title**, **Desired value**, and **Description** of the analysis.

7. If required, you can add **Remediation** to the custom check.



Note: You can add only one **Remediation** when creating custom check.

- Including **Remediation** to the custom check:

- Check **Include Remediation**.
- Enter the **Remediation script**.

8. Click **Create**.

9. In the **Create Custom Check** dialog box, click **Yes, create**.

When the custom check is created, **Compliance check creation** wizard navigates to the custom check details page. The details page contains Overview, Applicable Devices and Deployment sections.

Creating a custom check using Unix content

This task helps you in creating a custom check using Unix content.

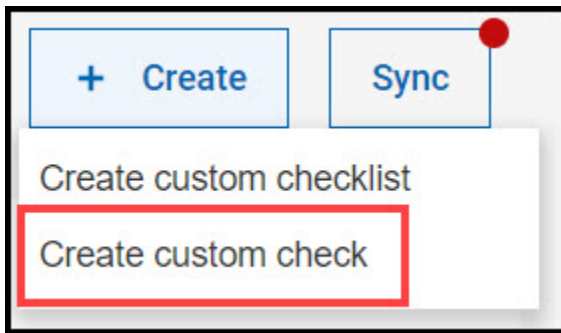
Ensure that you have **Owner** or **Write** permission for the checklist to add new checks.

Perform the following steps to create a custom check by using Unix content method:



Note: At any point, if you decide to create custom check using relevance, you can switch using the radio button available in the **Compliance check creation** wizard. The fields and field values in **Required information** and **Description** compliance creation wizard remains unchanged but, the values in the **Behavior** section will be deleted. For more information, see [Creating a custom check using relevance \(on page 30\)](#).

1. Navigate to the SCM App landing page and click **Create > Create custom content**.



A **Compliance check creation** wizard appears.



Note: Create using relevance is the default method in the **Compliance check creation** wizard.

 A screenshot of the 'Compliance check creation' wizard. At the top, there are two radio buttons: 'Create using relevance' (unselected) and 'Create Unix SCM checks using bourne shell script' (selected). Below this is a section titled 'Required Information' with a dropdown arrow. The form contains several input fields: 'Title' (with placeholder text), 'Site' (a dropdown menu), 'Applicability Fixlet' (a dropdown menu), 'Source' (a text input), 'Source ID' (a text input), 'Source Release date' (a date input with a calendar icon and placeholder 'yyyy-mm-dd'), 'Category' (a dropdown menu), and 'Severity' (a dropdown menu).

2. Check **Create Unix SCM checks using bourne shell script**.
3. Click **OK** when **Switch to Create Unix check using Script?** is prompted.
4. In the **Required information** section, provide the following information:
 - Title
 - Site
 - Source
 - Source ID
 - Source Release date
 - Category
 - Severity



Note:

- Based on the **Site** selection, the **Compliance check creation** wizard will auto-generate the required information for **Applicability Fixlet** and you can select the **Applicability Fixlet** from the drop-down if the site has more than one Fixlet.
- **SourceID** must be unique in the checklist.



- **SourceID** field must start with alphanumeric characters and may contain hyphen and underscore.
- If you want to add a new category which does not exist in the custom site, you can add it by clicking **Add new Category**.

5. In the **Description** section, enter the **Description** of the custom check.



Note:

- Description field is must be filled in order to create a custom check.
- You can customize the description field texts using text format option.

6. In the **Behavior** section, Enter the **Compliance script**.



Note: Relevance will be added automatically once the custom check is created.

7. If required, you can add **Remediation** to the custom check.



Note: You can add only one **Remediation** when creating custom check.

- Including **Remediation** to the custom check:

- a. Check **Include remediation**.
 - b. Enter the **Remediation script**.
8. Click **Create**.
9. In the **Create Custom Check** dialog box, click **Yes, create**.

When the custom check is created, **Compliance check creation** wizard navigates to the custom check details page. The details page contains Overview, Applicable Devices and Deployment sections.

Applicability

Overview | Applicable Devices | Deployments

0 applicable devices reported ▲
 0 open deployments
 0 deployments with > 10% failed
 0 deployments in the last 24 hours

[Deploy Custom Content](#)

Details
 Category Surface Area Reduction
 Site CIS SQL Server 2019 WebUI
 Source Applic_1
 Source ID 123
 Size 1024.00 KB
 Modified 14 days ago
 Modified By admin
[Edit Custom Content](#)

The default Windows configuration caches the last logon credentials for users who log on interactively to a system. This feature is provided for system availability reasons, such as the user's machine being disconnected from the network or domain controllers being unavailable. Even though the credential cache is well-protected, if a system is attacked, an unauthorized individual may isolate the password to a domain user account using a password-cracking program and gain access to the domain.

Editing a custom check

Understand how to edit a custom copy of a check or the checks which are created and added to the custom checklist.

Ensure that you have **Owner** or **Write** permission for the checklist to edit check.

Perform the following steps to edit a custom check:

1. Navigate to the SCM App landing page and click the **Custom checklist**.

Security Configuration Management

[+ Create](#) [Sync](#)

Custom checklist(8) | External checklist(13)

8 checklists





Checklist Name	No. of checks	Created	Updated	Subscribed ...	Platform	Status
DISAWindows2016-complianceReport	220	DISAWindows201...	DISAWindows201...	3	All Other	<none>
CIS MSSQL Server 2019	44	CIS MSSQL Server ...	CIS MSSQL Server ...	3	MS SQL Server 2019	Out of Sync
MSSQL2019_Console	39	MSSQL2019_Cons...	MSSQL2019_Cons...	3	MS SQL Server 2019	<none>
DISA STIG Checklist Windows2016	211	DISA STIG Checkli...	DISA STIG Checkli...	0	All Other	<none>
CIS Windows 10	425	CIS Windows 10	CIS Windows 10	0	All Other	<none>
DISA Windows 10	229	DISA Windows 10	DISA Windows 10	3	All Other	<none>
CIS Checklist for Windows 2016	339	CIS Checklist for ...	CIS Checklist for ...	3	All Other	Out of Sync
CIS MSSQL Server 2016	43	CIS MSSQL Server ...	CIS MSSQL Server ...	3	MS SQL Server 2016	Out of Sync

2. In the **custom checklist details** page, click **Edit** on the check.

Contents Sync Subscribed Devices

List of checks in your custom checklist

229 checks View: 20 < 1 > 1 of 12 pages

<input type="checkbox"/> Checks Name ↑	Source chec... ↑	Content ID ↑	Category ↑	Severity ↑	Source ID ↑	Applicable C... ↑	Deployment % ↑	Undeployed ...
<input type="checkbox"/> Anonymous access... 	DISA Windows 10	64387	SRG-OS-000138-G...	high	No CCEs provided	0	<none>	<none>
<input type="checkbox"/> Anonymous enume... 	DISA Windows 10	64265	SRG-OS-000480-G...	high	No CCEs provided	0	<none>	<none>
<input type="checkbox"/> Anonymous enume... 	DISA Windows 10	64471	SRG-OS-000138-G...	high	No CCEs provided	0	<none>	<none>
<input type="checkbox"/> Anonymous SID/N... 	DISA Windows 10	64306	SRG-OS-000480-G...	high	No CCEs provided	0	<none>	<none>

Compliance check creation wizard appears.

Compliance check creation

Required Information

Title
Anonymous access to Named Pipes and Shares must be restricted.

Site
DISA Windows 10

Applicability Fixlet
Fixlet

Source
Windows 10 Security Technical Implementation Guide Version 2 Rel

Source ID
No CCEs provided

Source Release date
2022-04-08

Category
SRG-OS-000138-GPOS-00069 (xccdf_mil.disa.stig_group_V-220#32)

Severity
high

> Description

> Behavior

Delete Cancel Update



Note:

- When you edit a custom check, you cannot change the custom check type that is, relevance to Unix content or vice versa.
- You can add multiple relevance script and remediation for both check type (Relevance and Unix content).

3. Edit the required fields in the **Required Information**, **Description**, and **Behavior** sections.

4. Click **Update**.

5. In the **Update Custom Check** dialog box, click **Update**.

A success/failure toast notification appears on the top-right corner.

Deleting a custom check or checks

Understand how to delete a custom copy of a check or the checks which are created and added to the custom checklist. You can delete multiple custom checks or an individual custom check from the custom checklist details page.



Important: Ensure that you have **Read** or **None** permission to the checklist to delete a checks.

Perform the following steps to delete multiple custom checks:

1. Navigate to the SCM App landing page and click the **Custom checklist**.

Security Configuration Management

Custom checklist(8) External checklist(13)

8 checklists

View: 20 < 1 > 1 of 1 pages

Checklist Name	No. of checks	Created	Updated	Subscribed	Platform	Status
DISA Windows 2016 compliance Report	220	DISA Windows 201...	DISA Windows 201...	3	All Other	<None>
CIS MSSQL Server 2019	44	CIS MSSQL Server ...	CIS MSSQL Server ...	3	MS SQL Server 2019	Out of Sync
MSSQL 2019 Console	39	MSSQL 2019 Cons...	MSSQL 2019 Cons...	3	MS SQL Server 2019	<None>
DISA STIG Checklist Windows 2016	211	DISA STIG Checkli...	DISA STIG Checkli...	0	All Other	<None>
CIS Windows 10	425	CIS Windows 10	CIS Windows 10	0	All Other	<None>
DISA Windows 10	229	DISA Windows 10	DISA Windows 10	3	All Other	<None>
CIS Checklist for Windows 2016	339	CIS Checklist for ...	CIS Checklist for ...	3	All Other	Out of Sync
CIS MS SQL Server 2016	42	CIS MS SQL Server ...	CIS MS SQL Server ...	2	MS SQL Server 2016	Out of Sync

2. In the **custom checklist details** page, select the **checks** and click **Delete**.

Contents Sync Subscribed Devices

List of checks in your custom checklist

229 checks

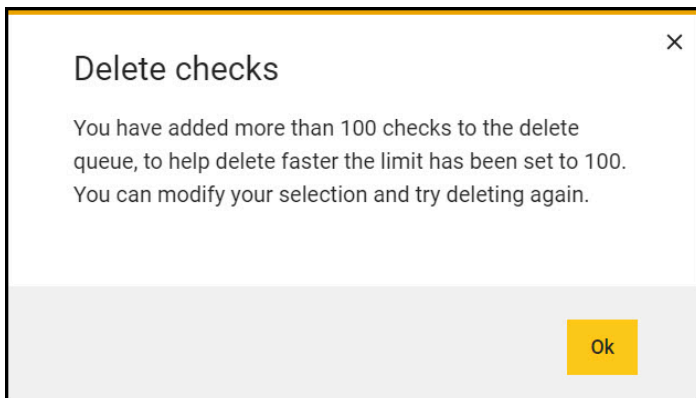
View: 20 < 1 > 1 of 12 pages

2 Items Selected View Selected only Deploy (2) Delete

Checks Name	Source chec...	Content ID	Category	Severity	Source ID	Applicable C...	Deployment %	Undeployed
<input checked="" type="checkbox"/> Accounts must be conf...	DISA Windows 10	64534	SRG-OS-000076-G...	medium	No CCEs provided	0	<None>	<None>
<input checked="" type="checkbox"/> Administrator acco...	DISA Windows 10	64336	SRG-OS-000134-G...	medium	No CCEs provided	0	<None>	<None>
<input type="checkbox"/> Anonymous access...	DISA Windows 10	64387	SRG-OS-000138-G...	high	No CCEs provided	0	<None>	<None>



Important: You can select up to 100 checks at a time to delete. This limitation is to improve the performance of the operation.



3. In the **Delete checks** dialog box, click **Yes**.

Result: A success/failure toast notification appears on the top-right corner.

Perform the following steps to delete an individual custom check:

1. Navigate to the SCM App landing page and click the **Custom checklist**.

Checklist Name	No. of checks	Created	Updated	Subscribed	Platform	Status
DISA Windows 2016-complianceReport	220	DISA Windows 201...	DISA Windows 201...	3	All Other	<none>
CIS MSSQL Server 2019	44	CIS MSSQL Server ...	CIS MSSQL Server ...	3	MS SQL Server 2019	Out of Sync
MSSQL2019_Console	39	MSSQL2019_Conso...	MSSQL2019_Conso...	3	MS SQL Server 2019	<none>
DISA STIG Checklist Windows2016	211	DISA STIG Checkli...	DISA STIG Checkli...	0	All Other	<none>
CIS Windows 10	425	CIS Windows 10	CIS Windows 10	0	All Other	<none>
DISA Windows 10	229	DISA Windows 10	DISA Windows 10	3	All Other	<none>
CIS Checklist for Windows 2016	339	CIS Checklist for ...	CIS Checklist for ...	3	All Other	Out of Sync
CIS.MS.SQL.Server.2016	42	CIS.MS.SQL.Server...	CIS.MS.SQL.Server...	2	MS SQL Server 2016	Out of Sync

2. In the **custom checklist details** page, click **Edit**.

Checks Name	Source chec...	Content ID	Category	Severity	Source ID	Applicable C...	Deployment %	Undeployed %
<input type="checkbox"/> Accounts must be confi...	DISA Windows 10	64534	SRG-OS-000076-G...	medium	No CCEs provided	0	<none>	<none>
<input type="checkbox"/> Administrator acco...	DISA Windows 10	64336	SRG-OS-000134-G...	medium	No CCEs provided	0	<none>	<none>
<input type="checkbox"/> Anonymous access...	DISA Windows 10	64387	SRG-OS-000138-G...	high	No CCEs provided	0	<none>	<none>

Compliance check creation wizard appears.

Compliance check creation

> Required Information

> Description

> Behavior

Delete Cancel Update

3. Click **Delete**.
4. In the **Delete check** dialog box, click **OK**.

Result: You are navigated to the custom checklist details page when the check is successfully deleted.

External checklist

SCM App in WebUI uses various benchmark checklists to ensure that the device meet the compliance standards. You can use these external checklists to manage devices or create custom checklist as per the requirement. For more information about external checklist, see [Supported Benchmarks \(on page 9\)](#).

Viewing an external checklist

Understand how to view an external checklist and its overview.

Perform the following steps to view an external checklist:

1. Navigate to the SCM App landing page and click the **External checklist** tab.



Note: The **Custom checklist** tab is selected by default.

2. Click an **External checklist** tile to view.

Checklist Name	No. of checks	Created	Updated	Benchmark versi...	Platform	Benchmark	Status
DISA STIG Checklist for Windows 2008 R2 MS	262	04/26/2019	10/25/2019	<none>	All Other	DISA	<none>
DISA STIG Checklist for Windows 2012 MS	284	03/05/2021	06/30/2021	<none>	All Other	DISA	<none>
CIS Checklist for Windows 10	425	07/12/2021	12/24/2021	<none>	All Other	CIS	<none>
DISA Checklist for Windows 10	229	04/08/2022	07/22/2022	<none>	All Other	DISA	<none>
CIS Checklist for CentOS Linux 6	196	01/30/2017	06/22/2020	<none>	All Other	CIS	<none>
CIS Checklist for Mac OS X 10.12	80	11/04/2016	04/24/2019	<none>	OSX 10.12	CIS	<none>
CIS Checklist for Windows 2016 DC	351	07/12/2021	08/12/2022	<none>	All Other	CIS	<none>
CIS Checklist for Windows 2016 MS	354	07/12/2021	08/12/2022	<none>	All Other	CIS	<none>

You are directed to the external checklist details page. This page contains **Inline reports**, **Selected external checklist tab** and **Custom Checklists Affected tab** and BigFix site version information.

Figure 4. External checklist details page

Security Configuration Management Export Show summary

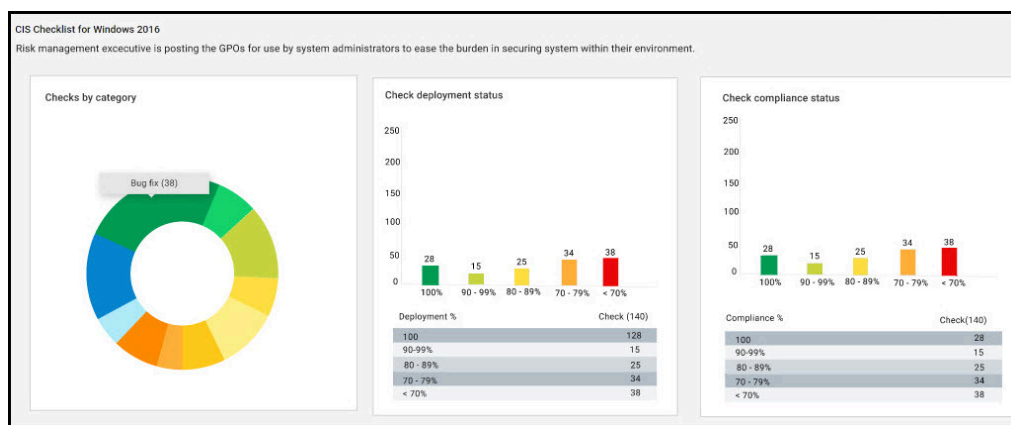
DISA checklist for Windows server 2019 STIG Custom Checklists Affected (0) BigFix site version: 9, Benchmark: Windows Server 2019 Security Technical Implementation Guide Ve...

217 content items View: 20 < 1 > 1 of 11 pages

<input type="checkbox"/> Checks Name	Content ID	Category	Severity	Source ID	Applicable C...	Release Date	Deployment %	Undeploye...
<input type="checkbox"/> Applicability - HKU	150151	<none>	<none>	cpe/o.microsoft.w...	0	<none>	0	0
<input type="checkbox"/> Applicability - Microsoft ...	149959	<none>	<none>	cpe/o.microsoft.w...	0	<none>	0	0
<input type="checkbox"/> Applicability - Windows S...	149958	<none>	<none>	xccdf_mil.disa.stig...	0	<none>	0	0
<input type="checkbox"/> Applicability - Windows S...	149957	<none>	<none>	xccdf_mil.disa.stig...	0	<none>	0	0
<input type="checkbox"/> Applicability - Windows S...	149961	<none>	<none>	xccdf_mil.disa.stig...	0	<none>	0	0
<input type="checkbox"/> Task - Windows Server 20...	141234	<none>	<none>	<none>	0	<none>	0	0
<input type="checkbox"/> Task - Windows Server 20...	141077	<none>	<none>	<none>	0	<none>	0	0

The external checklist page contains the following elements:

- **Export:** Use this feature to download reports of an individual custom checklist. For more information, see [Exporting report \(on page 46\)](#).
- **Show/Hide summary:** Use this feature to display or hide the inline reports.
- **Inline reports:**



Donut chart and bar graphs, such as **checks by category**, **check deployment status**, and **check compliance status** shows the status of the selected custom checklist. These chart and graphs are updated dynamically when you apply filters in contents tab. You can also click on any of the chart or graphs to see information related to specific set of checks.

Inline reports chart and graphs:

- **Checks by category:** The checks are grouped together based on the custom site they belong to. For example, bug fixes, password policies, auditing and logging are the few category of checks.
 - **Check deployment status:** This graph is generated based on the deployment percentage checks.
 - **Check compliance status:** This graph is generated based on the compliance percentage of the checks.
- **Selected External checklist:**

The checks in this tab are represented in a data grid format. Each column has a search or filter feature, which you can use to find checks by entering text or a keyword. The pagination allows you to navigate between pages. Use the checkbox in each row to select the required checks or select all the checks using the checkbox available in header section of **Checks Name** column. To view only the checks that you have selected, use **View Selected only**. To know more about data grid, see [Grid view](#).

You can select the checks and deploy them to the target devices by clicking **deploy**. For more information deploying external content, see [Deploying a custom checklist \(on page 21\)](#).

- **Custom Checklists Affected:** This tab contains the list of custom checklist that are to be synchronized with their source checklist (external checklist).

Security Configuration Management			
DISA Checklist for Windows 10	Custom Checklists Affected (1)	BigFix site version: 22, Benchmark: Windows 10 Security Technical Implementation Guide Versi...	
DISA Windows 10	No. of checks: 229	Windows 10 Security Technical Implementation Guide Version 2 Release 4	Updated : 8/28/2022 View and Sync

By default, a custom checklist is created by using one or more external checklists. When an external checklist is updated and the created custom checklists are not synchronized with an external checklist, those checklists are listed in custom checklist affected tab. The number in parentheses indicates the number of custom checklists that are affected by the selected external checklist.

Each list contains checklist name, number of checks, benchmark name and version, and creation date.

Deploying an external checklist

Use this task to deploy an external checklist to one or more targets.

Perform the following steps to deploy an external checklist:

1. Navigate to the SCM App landing page and click the **External checklist** tab.



Note: The **Custom checklist** tab is selected by default.

2. Click an **External checklist** tile to deploy.

Security Configuration Management

+ Create Sync

Custom checklist (16) External checklist (17)

Search

11 content items View: 20 < 1 > 1 of 2 pages

Checklist Name	No. of checks	Created	Updated	Benchmark
<input type="text" value="Type for search..."/>				
RHEL windows 10 checklist	180	02/02/2022	12/02/2022	v.3.0
RHEL windows 10 checklist	479	06/04/2022		v.3.0
RHEL windows 10 checklist	32	02/02/2022	15/02/2022	v.3.0
RHEL windows 10 checklist	54	06/04/2022	10/04/2022	v.2.0
RHEL windows 10 checklist	90	06/04/2022		v.3.0
CIS checklist for Android 2.3	56	02/02/2022	16/02/2022	v.4.0
RHEL windows 10 checklist	120	03/03/2022	05/03/2022	v.3.0
CIS checklist for Android 2.3	345	02/02/2022		v.2.0
RHFI windows 10 checklist	32	04/03/2022	08/03/2022	v.3.0

3. Select the **Checks** and click **deploy**.

BIGFIX Devices Apps Deployments Reports

Security Configuration Management

Export Show summary

CIS Checklist for MS SQL Server 2019 BigFix site version: 4, Benchmark: CIS_Microsoft_SQL_Server_2019_Benchmark...

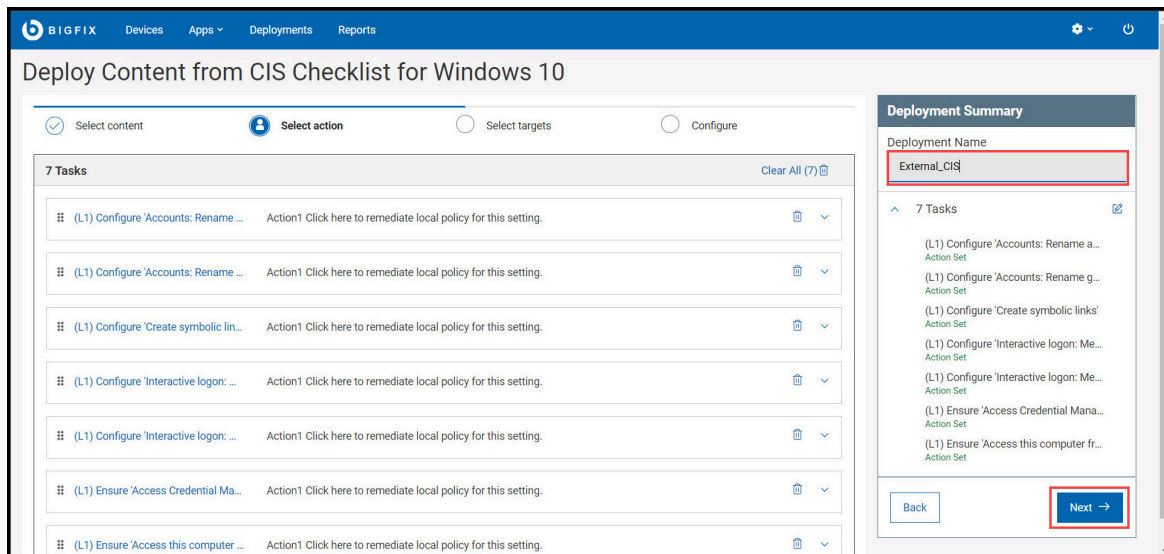
Custom Checklists Affected (6)

39 content items View: 20 < 1 > 1 of 2 pages

4 Items Selected
☐ View Selected only
Deploy (4)

Checks Name	Content ID	Category	Severity	Source	Applicable C...	Release Date	Deployment %	Undeploye
<input checked="" type="checkbox"/> Applicability Fixlet - SQL ...	990002	Applicability Fixlet	<none>	<none>	0	<none>	0	0
<input checked="" type="checkbox"/> Ensure 'Ad Hoc Distribute...	2014	Surface Area Redu...	Level 1	cis-2.1	0	a year ago	0	0
<input checked="" type="checkbox"/> Ensure 'AUTO_CLOSE' is s...	2164	Surface Area Redu...	Level 1	cis-2.15	0	a year ago	0	0
<input checked="" type="checkbox"/> Ensure 'CHECK_EXPIRATI...	4024	Password Policies	Level 1	cis-4.2	0	a year ago	0	0
<input type="checkbox"/> Ensure 'CHECK_POLICY' ...	4034	Password Policies	Level 1	cis-4.3	0	a year ago	0	0

4. Review the available tasks and click **Next**.

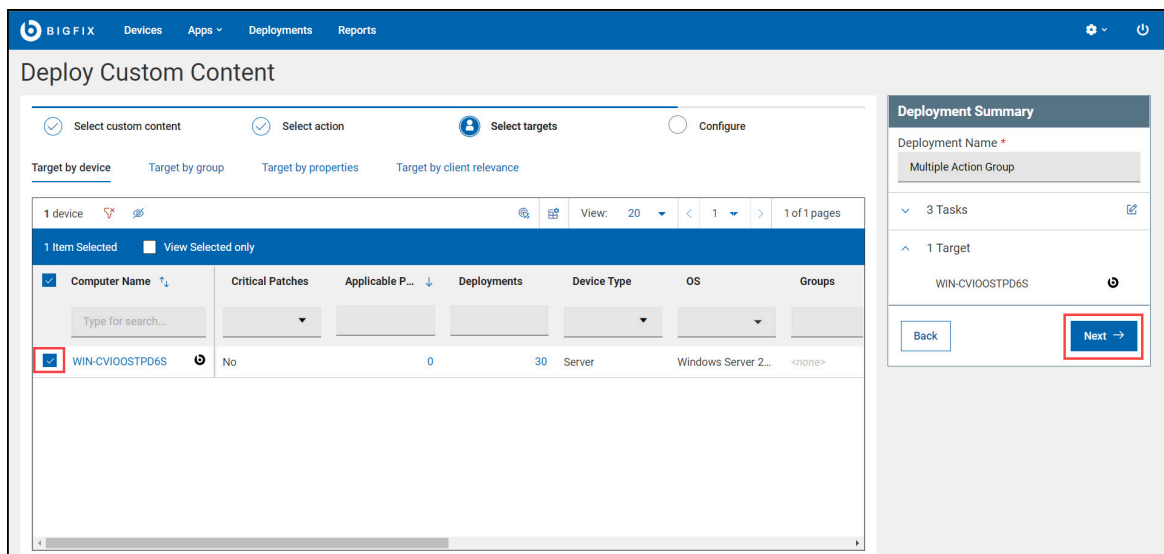
**Note:**

- You can also rename the **Deployment Name** in **Deployment Summary** panel.



- A warning icon indicates that the task is not associated with the action.

5. Select the **Target** and click **Next**.

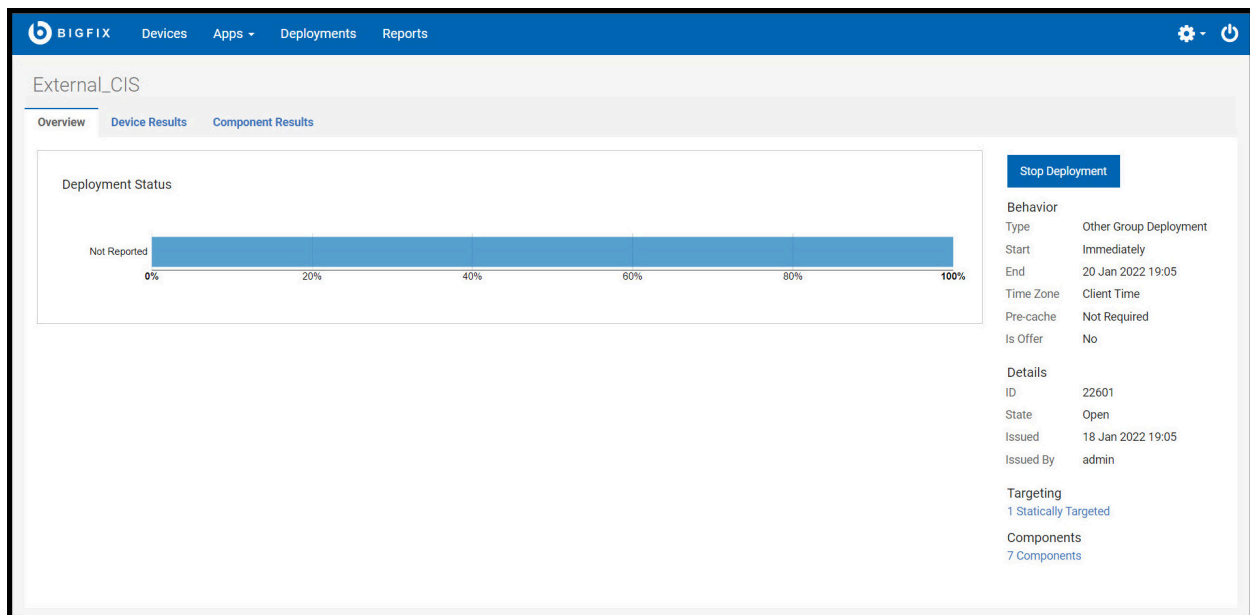


6. Configure your deployment and click **Deploy**.

**Note:**

- Use the **Edit** icon in the subtabs (Run, Users, Messages, Offer, and Post-Action) on the left panel to further fine-tune the deployment. For more information on the subtabs, see [Configuration Options](#).
- Use the **Edit** icon in the Deployment Summary panel to modify tasks and targets.

The Deployment page displays details such as overview, device, and component results. You can also stop the deployment any time by clicking **Stop Deployment**.



- **Overview:** Detailed description of the selected deployment status, behavior, targeting, and more.
- **Device Results:** Target status, which is - the state of the deployment on each endpoint.
- **Component Results:** For content with multiple actions: the deployment status of each component on targeted devices is expressed as a percentage of completion.

You can also view the status of the current or previous deployments in WebUI by clicking **Deployments** in the navigation bar. For more information on deployments, see [The Deployment List](#).



Important:

SCM deployments are categorized under the **Other** application type. Use Deployment Name, Issued Date, or other criteria to find deployments.

Exporting report

Use export feature to save report for a particular custom or external checklist.

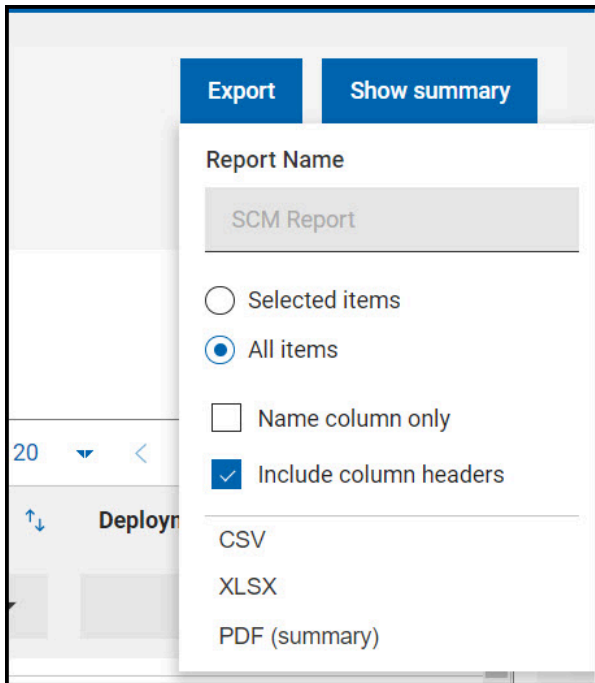
Perform the following steps to export report of a custom or external checklist:

1. Navigate to the SCM App landing page and click **Custom checklist**.

Checklist Name	No. of checks	Created	Updated	Subscribed ...	Platform	Status
DISAWindows2016-complianceReport	220	DISAWindows201...	DISAWindows201...	3	All Other	<none>
CIS MSSQL Server 2019	44	CIS MSSQL Server ...	CIS MSSQL Server ...	3	MS SQL Server 2019	Out of Sync
MSSQL2019_Console	39	MSSQL2019_Cons...	MSSQL2019_Cons...	3	MS SQL Server 2019	<none>
DISA STIG Checklist Windows2016	211	DISA STIG Checkli...	DISA STIG Checkli...	0	All Other	<none>
CIS Windows 10	425	CIS Windows 10	CIS Windows 10	0	All Other	<none>
DISA Windows 10	229	DISA Windows 10	DISA Windows 10	3	All Other	<none>
CIS Checklist for Windows 2016	339	CIS Checklist for ...	CIS Checklist for ...	3	All Other	Out of Sync
CIS MS SQL Server 2016	12	CIS MS SQL Server ...	CIS MS SQL Server ...	3	MS SQL Server 2016	Out of Sync

2. In the **custom or external checklist details** page, click **Export**.

3. Enter the **Report Name** and click the desired **file format**. (**CSV**, **XLSX**, or **PDF**).



Note: You can use the following options to refine and export the required information:

- Selected items
- All items
- Name column only
- Include column headers

The report is generated and saved in the default download location of your device.

Inline reports

Inline reports provide the status of selected custom or external checklist in the form of chart and graphs which assess the available checks in the selected checklist.

Various status of a check

Inline report consists of **Checks by category**, **Check deployment status**, and **Check compliance status** chart and graphs. To generate these chart and graphs, inline report assesses all the checks and then categorise the checks in the following status:

Deployed

Taking a deployment action on a device. - Deployment on a device.

Success

Deployment on a device and the action is successfully completed (Fixed).

Failed

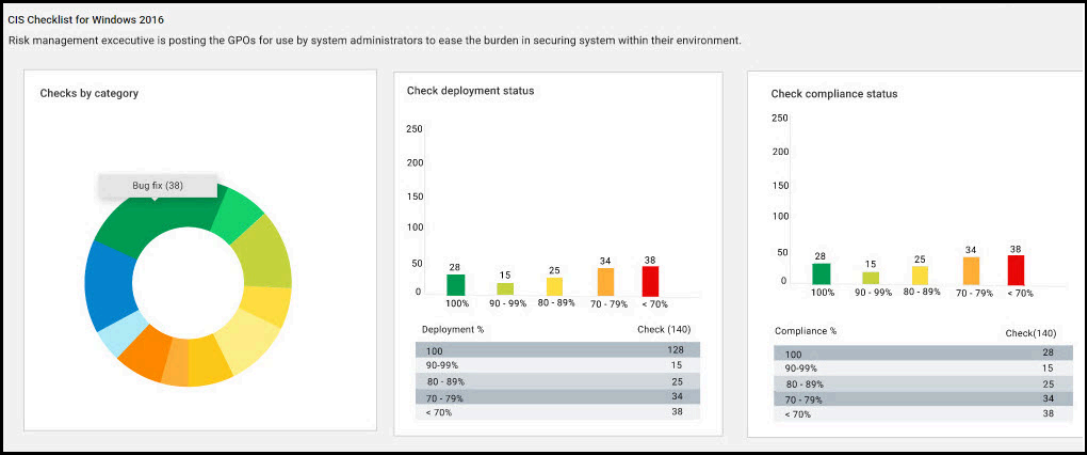
Deployment on a device and the action is unsuccessful (Failed).

Undeployed

Devices on which the deployment has not yet been performed. This does not include the failed checks.

These category helps in calculating the deployment percentage, undeployed device count, compliance percentage, and non-compliant devices count.

Figure 5. Inline reports



To understand how inline reports works, let us consider the following case:

Table 2. Assumptions for Inline reports calculation

Subscribed devices	12
Applicable devices	10 ⁽¹⁾
Deployed devices	8 ⁽²⁾
Undeployed devices	2 ⁽³⁾
Success (Compliant)	5
Failed (Non-compliant)	3



Note:

1. The two devices out of 12 subscribed devices are not applicable as they did not pass the relevance check.
2. The deployment to the device must be explicitly done.
3. The check is not deployed on these two devices.

Deployment percentage

The percentage of devices on which the check was deployed (Success or Failed) out of the total number of subscribed devices (12).

Deployment percentage = Number of devices on which check was success or failed divided by the total Number of Subscribed devices for that check

Number of devices on which check was successful or failed is obtained from grouped data, such as **Actions, Action Results, Computers, and Computer sites**.

Deployment percentage = 8/12

Undeployed Devices

The number of devices on which the deployment has not yet been performed. This data is obtained from the Computer Fixlets table for the check with `isRelevant=1` and excluding the failed ones from result.

Compliance Percentage

The percentage of devices on which the check is compliant (success) or non-relevant out of the total number of subscribed devices (12).

When applicable devices is equal to zero and subscribed count is greater than zero, then the compliance percentage is 100% or else compliance percentage is equal to number of complaint devices (success) divided by the number of subscribed devices.

where,

Number of complaint devices = Subscribed devices - applicable computer count

Compliance percentage = 7/12

Non-compliant Devices

Number of non-compliant devices is equal to the value of applicable computer - count of that check.

Chapter 6. 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 7. 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.