BigFix Compliance
Configuration Management (SCM) User Guide

Special notice

Before using this information and the product it supports, read the information in Notices *(on page 53)*.

Edition notice

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

Contents

Chapter 1. Configuration Management (SCM) User Guide

This guide describes a portfolio of security configuration content called Configuration Management. This content is organized through checklists, which assess and manage the configurations of desktops, laptops, and servers. The Configuration Management solution has achieved Security Content Automation Protocol (SCAP) validation certification with the National Institute of Standards and Technology (NIST) for both misconfiguration assessment and remediation. By offering an extensive library of technical checks, Configuration Management detects and enforces security configuration policies using industry best practices.

This guide serves as a resource for IT personnel responsible for managing and enforcing corporate system configuration policies on endpoints. The Configuration Management checklists allow security teams to define the security parameters and configurations required by corporate policy. IT managers use the Configuration Management checklists to enforce security policies and document the current state of compliance against corporate policies. BigFix console operators focus on the detailed day-to-day configuration management of all systems to use detailed information for each endpoint. Auditors use Configuration Management checklists to determine the current state of compliance for systems within the entire organization.

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 13)*.

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	• Console 8.0 or later • Windows Client 8.0 • UNIX Client: ◦ 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.

USGBC replaced the Federal Desktop Core Configuration (FDCC).

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

Using checks and checklists

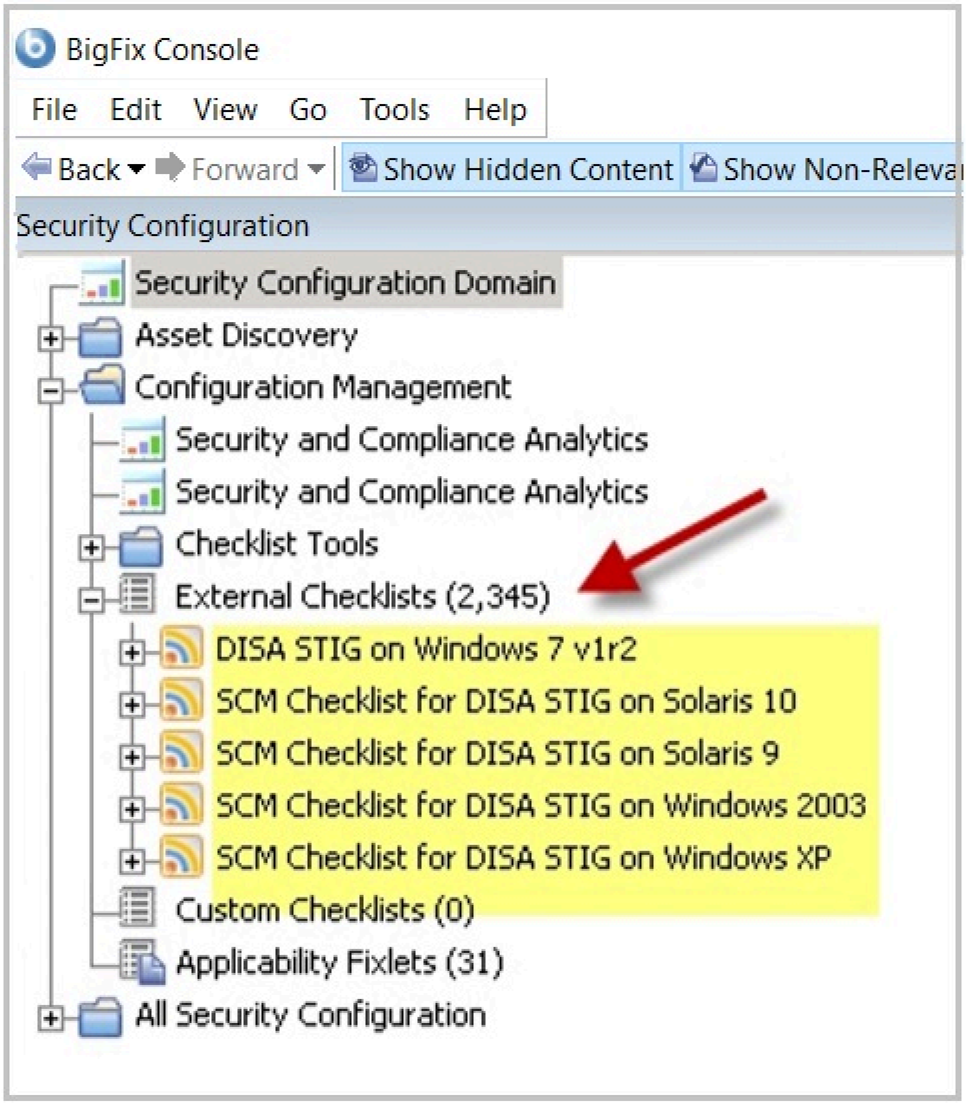
Check Fixlets in Configuration Management checklists assess an endpoint against a configuration standard. Many check Fixlets have a corresponding analysis, sometimes referred to as *measured values*, which report the value of the element that the check Fixlet evaluates.

Check Fixlets

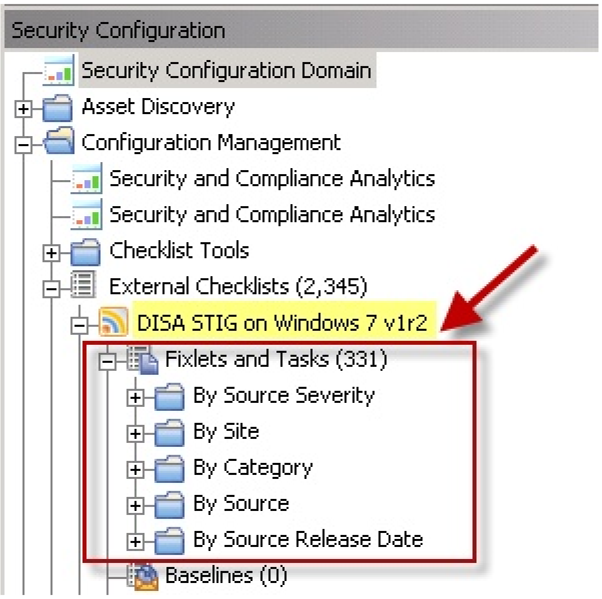
A check Fixlet becomes relevant when a client computer is out of compliance with a configuration standard. By viewing the Configuration Management Fixlets, you can identify non-compliant computers and the corresponding standards.

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.

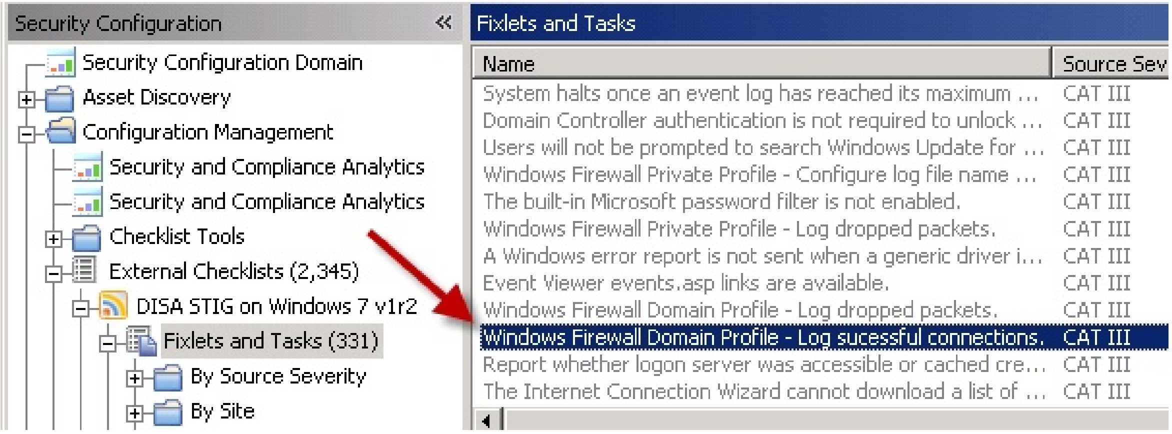

BigFix Console
File Edit View Go Tools Help
Back Forward Show Hidden Content Show Non-Releva
Security Configuration
Security Configuration Domain
Asset Discovery
Configuration Management
Security and Compliance Analytics
Security and Compliance Analytics
Checklist Tools
External Checklists (2,345)
DISA STIG on Windows 7 v1r2
SCM Checklist for DISA STIG on Solaris 10
SCM Checklist for DISA STIG on Solaris 9
SCM Checklist for DISA STIG on Windows 2003
SCM Checklist for DISA STIG on Windows XP
Custom Checklists (0)
Applicability Fixlets (31)
All Security Configuration

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



Security Configuration
- Security Configuration Domain
- Asset Discovery
- Configuration Management
  - Security and Compliance Analytics
  - Security and Compliance Analytics
  - Checklist Tools
  - External Checklists (2,345)
    - DISA STIG on Windows 7 v1r2
      - Fixlets and Tasks (331)
        - By Source Severity
        - By Site
        - By Category
        - By Source
        - By Source Release Date
      - Baselines (0)

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.

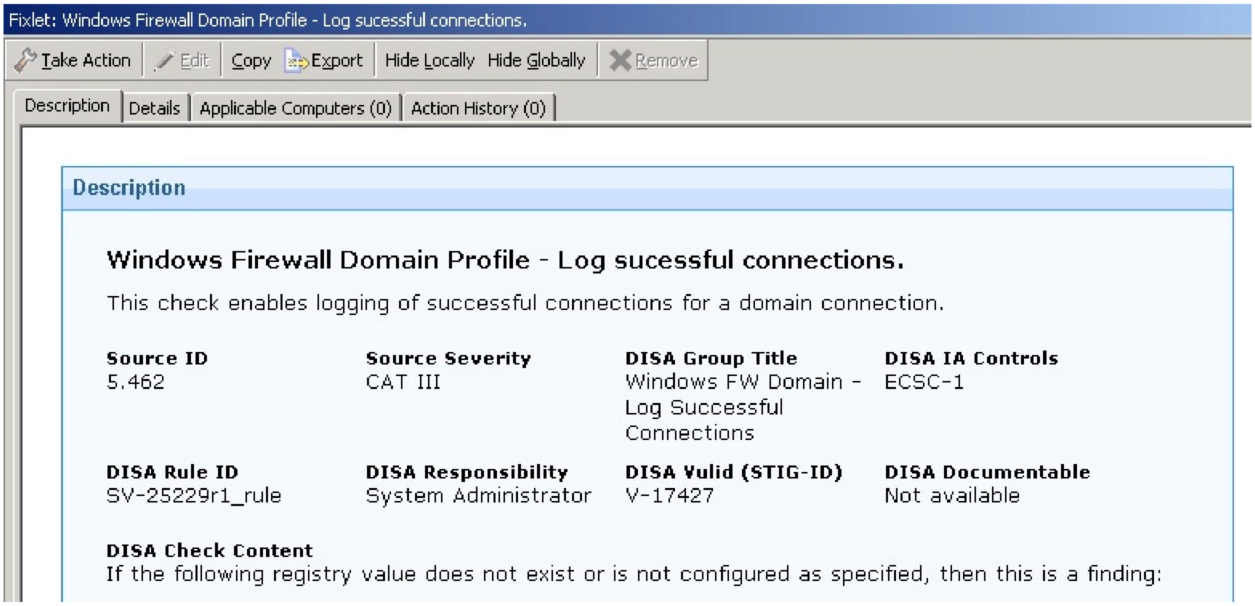


Security Configuration
- Security Configuration Domain
- Asset Discovery
- Configuration Management
  - Security and Compliance Analytics
  - Security and Compliance Analytics
  - Checklist Tools
  - External Checklists (2,345)
    - DISA STIG on Windows 7 v1r2
      - Fixlets and Tasks (331)
        - By Source Severity
        - By Site

Fixlets and Tasks

Name	Source Sev
System halts once an event log has reached its maximum ...	CAT III
Domain Controller authentication is not required to unlock ...	CAT III
Users will not be prompted to search Windows Update for ...	CAT III
Windows Firewall Private Profile - Configure log file name ...	CAT III
The built-in Microsoft password filter is not enabled.	CAT III
Windows Firewall Private Profile - Log dropped packets.	CAT III
A Windows error report is not sent when a generic driver i...	CAT III
Event Viewer events.asp links are available.	CAT III
Windows Firewall Domain Profile - Log dropped packets.	CAT III
Windows Firewall Domain Profile - Log sucessful connections.	CAT III
Report whether logon server was accessible or cached cre...	CAT III
The Internet Connection Wizard cannot download a list of ...	CAT III

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.



Windows Firewall Domain Profile - Log sucessful connections.

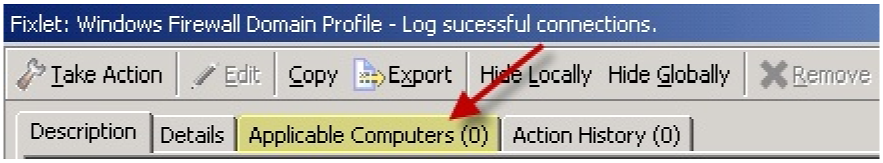
This check enables logging of successful connections for a domain connection.

Source ID	Source Severity	DISA Group Title	DISA IA Controls
5.462	CAT III	Windows FW Domain - Log Successful Connections	ECSC-1
DISA Rule ID	**DISA Responsibility**	**DISA Vulid (STIG-ID)**	**DISA Documentable**
SV-25229r1_rule	System Administrator	V-17427	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.



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

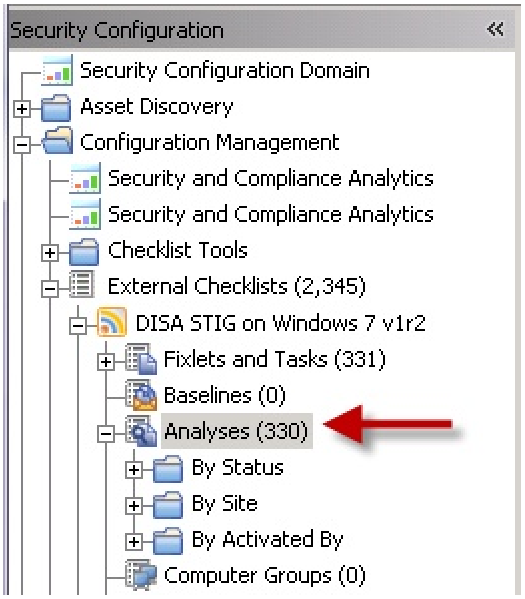
Modifying check parameters

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.

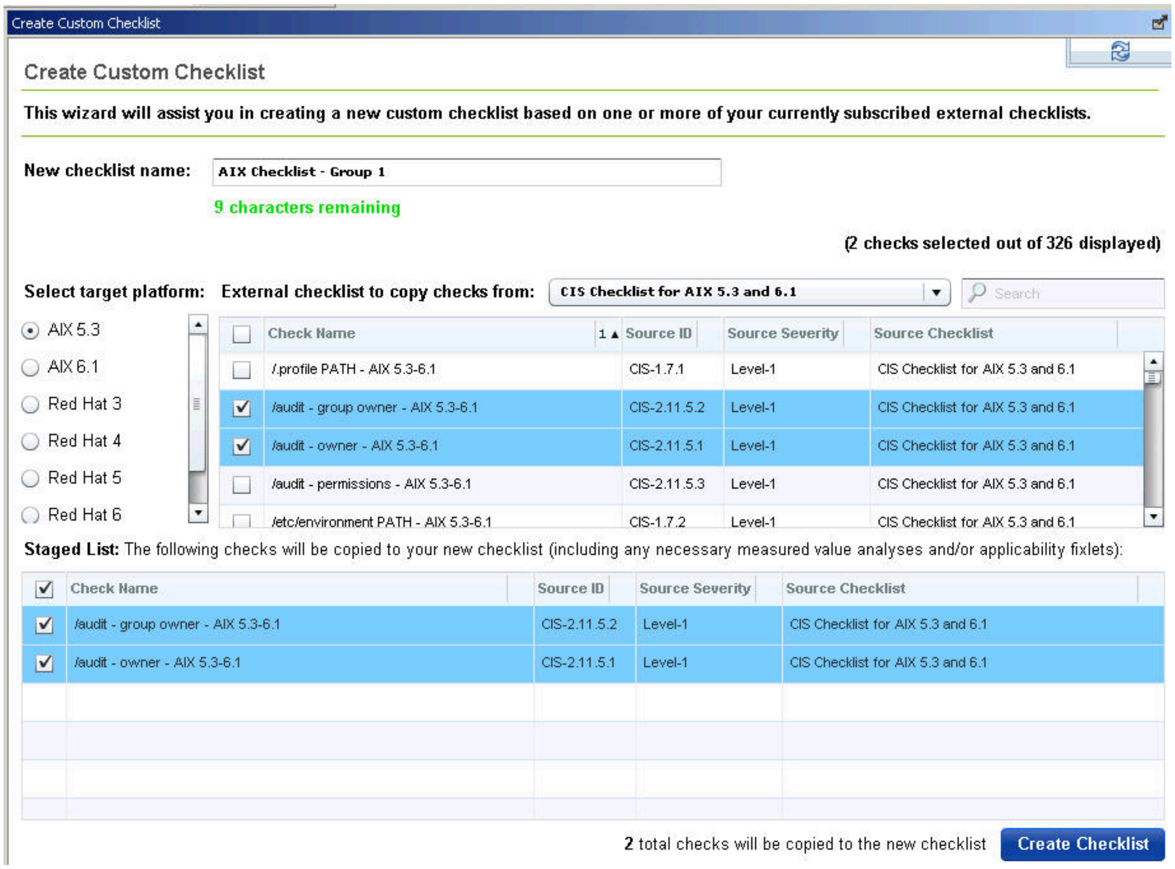
- Step 1: Create a custom checklist from an existing external checklist
- Step 2: Customize Fixlets using built-in parameterization
- Step 3: Subscribe the proper computers to the custom checklist

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

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: AIX Checklist - Group 1

9 characters remaining

(2 checks selected out of 326 displayed)

Select target platform: External checklist to copy checks from: CIS Checklist for AIX 5.3 and 6.1

● AIX 5.3
○ AIX 6.1
○ Red Hat 3
○ Red Hat 4
○ Red Hat 5
○ Red Hat 6

☐	Check Name	1 ▲ Source ID	Source Severity	Source Checklist
☐	/.profile PATH - AIX 5.3-6.1	CIS-1.7.1	Level-1	CIS Checklist for AIX 5.3 and 6.1
☑	/audit - group owner - AIX 5.3-6.1	CIS-2.11.5.2	Level-1	CIS Checklist for AIX 5.3 and 6.1
☑	/audit - owner - AIX 5.3-6.1	CIS-2.11.5.1	Level-1	CIS Checklist for AIX 5.3 and 6.1
☐	/audit - permissions - AIX 5.3-6.1	CIS-2.11.5.3	Level-1	CIS Checklist for AIX 5.3 and 6.1
☐	/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):

☑	Check Name	Source ID	Source Severity	Source Checklist
☑	/audit - group owner - AIX 5.3-6.1	CIS-2.11.5.2	Level-1	CIS Checklist for AIX 5.3 and 6.1
☑	/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.

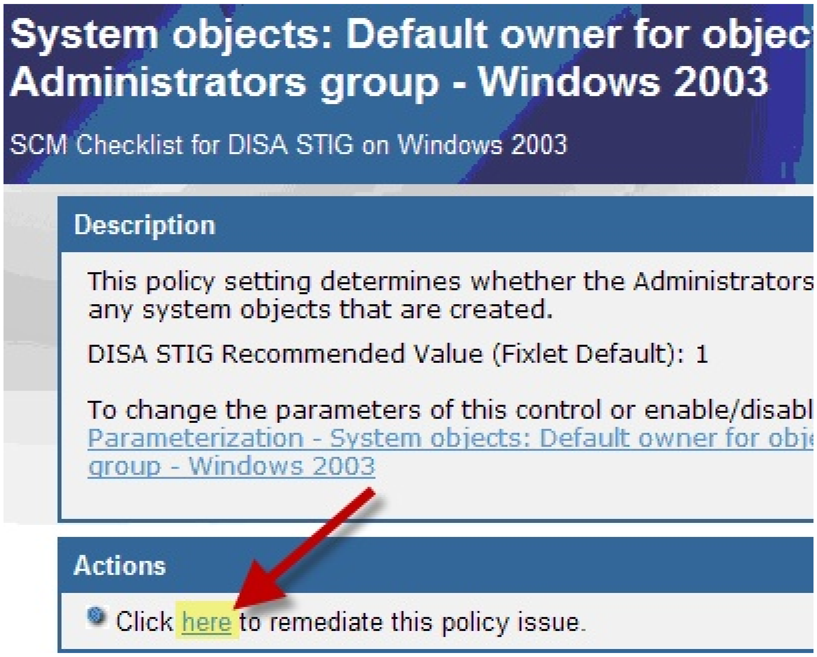
Normally, synchronizing a custom check overwrites the existing remediation action, if there are any, with the latest from the external source. However, if you manually edited the remediation action script for checks in your custom checklists, you can preserve this custom action after synchronizing.

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.



System objects: Default owner for objec
Administrators group - Windows 2003

SCM Checklist for DISA STIG on Windows 2003

Description

This policy setting determines whether the Administrators
any system objects that are created.

DISA STIG Recommended Value (Fixlet Default): 1

To change the parameters of this control or enable/disabl
Parameterization - System objects: Default owner for obj
group - Windows 2003

Actions

Click here to remediate this policy issue.

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.

Configuring Windows checklists

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

Viewing checks

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 noncompliant computers and the corresponding standards.

You need a masthead for the appropriate Configuration Management site. For a list of SCM Checklists, see the SCM Checklists. From the BigFix console, gather the site and do the following steps to view the checks.

1. Select a Configuration Management checklist from the navigation tree.
2. Expand a checklist.
3. Click **Fixlets and Tasks**. The **Fixlets and Tasks** section opens on the right.
4. Click one of the Fixlets that is 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 the text that describes the Fixlet. The Fixlet window typically the following details: 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. The Fixlet is applicable to a subset of endpoints on your network. The size of that subset is shown in the Applicable Computers tab.

Activating prerequisite Fixlet tasks

Some Fixlets require you to activate tasks before you can use the Fixlets.

Some Fixlets require that you activate a task before you can use the Fixlet. You can identify these tasks by the word 'Task' that appends the Fixlet name. For example, if the Fixlet name is Accounts: Rename Administrator Account, the task that is associated with that Fixlet is called Task - Accounts: Rename Administrator Account.

1. From the Security Configuration domain, go to **All Security Configuration > Sites**.
2. Select the site.
3. Select the task. The word Task appends tasks that are associated to Fixlets that require prerequisite tasks before use.
4. You can do any of the following steps:
    - Click **Take Action**.
    - From the **Description** tab, go to **Actions** and click the appropriate Action link.
5. Click **OK**.

Apply the Fixlet that initially required the task to be activated.

Modifying Windows check parameters

Modify check parameters by changing the desired value in the check description.

You can modify only parameters of checks in custom sites.

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

In some cases, you can modify the parameters used in determining the compliance of checks. For example, you can set the minimum password length on an endpoint to be 14 characters. You can customize the password-length parameter to your specific policy.

Not all checks can be parameterized. Only copies of checks located in custom sites can be parameterized.

1. Open the check and click the **Description** tab.
2. Scroll down to the **Desired value for this parameter:** field and enter the value.
3. Click **Save**.

Remediation of Windows configuration settings

Follow these steps to remediate configuration settings.

You can audit, assess, and remediate configuration settings using HCL BigFix Compliance Configuration Management. For Fixlet checks that can be automatically remediated, you receive an action displayed in the relevant Fixlet. Not all Fixlets have a remediation action.

1. From the **Security Configuration Domain**, go to **All Security Configuration > Fixlets and Tasks**.
2. Expand the sub-folders to search for the Fixlet you want to enable.
3. In the Fixlet window, click the **Description** tab and scroll down to the Actions box.
4. Click in the Actions box link to remediate the specified policy issue.
5. Set your parameters in the Take Action dialog and click *OK*.

Configuring UNIX checklists

You can configure checklists for the superseded and non-superseded UNIX content.

Differences between superseded and non-superseded UNIX content

The Configuration Management UNIX content has superseded and non-superseded versions for every site. In the License Overview dashboard, superseded content have 'Superseded' appended to the site name. For example, the site name for the earlier content for the DISA STIG for Red Hat Enterprise Linux 6 is 'SCM Checklist for DISA STIG on RHEL 6 (superseded)'.

The superseded or earlier content uses client settings for parameter values so you could set different values on different endpoints. The non-superseded or later content has the parameter values scoped to the site's subscription so all endpoints subscribed to that site must use the same parameter values.

Table 2. Comparison between superseded and non-superseded UNIX content

	Superseded or earlier content	Non-superseded or newer content
Setting parameters	Sets different values on different endpoints	Stores parameters on a per-Fixlet basis
	Requires applicability Fixlets which are in the SCM Reporting site. All endpoints must subscribe to the SCM Reporting site.	Requires an applicability Fixlet in the custom site to work with SCA.
Content	Downloads the related scripts	Each Fixlet contains the related shell script
		Placed in different directories
Synchronization	Synchronized in the same way as other sites such as Patch Management sites or the BES Support site	Runs from a custom site and uses the Synchronization wizard

Configuring checklists

Use HCL BigFix for Configuration Management to configure your checklists by using the -F option in the action scripts or by parametizing checks from the console or at the system level.

Select checks via task

Follow these steps to run subsets of the checks on your own schedule.

The default behavior for UNIX Configuration Management deployment is to run the scripts as a single batch. However, you can also run any subset of the checks on your own defined schedule. Each time you do this, the batch that you deploy overwrites any previous batch commands. The `runme.sh` master script provides a '-F' option, which takes a file name as its argument. It has the following form:

```
      ./runme.sh -F <FILE>
```

This command causes runme.sh to perform *only* the set of checks specified in <FILE>. This is a 7-bit ASCII file with UNIX newlines containing a list of the specific checks you want to run, of the form:

```
GEN000020

GEN000480

GEN000560
```

This function allows you to run only the scripts you need when you need them. To enable this function, create a custom action. This action creates the file containing the list of checks and then deploys it to your chosen BigFix clients. This action is similar to creating a custom parameter file.

1. In the BigFix console, go to **Tools > Take Custom Action**. The Take Action dialog opens.
2. Click the **Target** tab and select the endpoints on which you want to create checks.
3. Click the **Applicability** tab and click the second button to run this action on computers with a custom relevance clause.
4. In the text box, enter a relevance clause to identify a subset of computers you want to target. For example, to restrict the action to Solaris 10 systems, enter the following expression:

```
name of operating system = “SunOS 5.10 (not exists last
active time of it or (now - last active time of it) > (15
*minute)) of action
```

5. Click the **Action Script** tab to create a script that copies your file onto the target computers. Click the second button and then enter a script. The script creates the target directory with the file containing the checks to run and then moves the file into the appropriate directory. The following sample script, which you can copy and paste, specifies three checks, GEN000020, GEN000480, and GEN000560.

```
// create a script that will create the necessary directory
delete __appendfile
appendfile #!/bin/sh
appendfile mkdir –p ../../scm_preserve/SunOS/5.10
delete createdir.sh
move __appendfile createdir.sh
wait /bin/sh ./createdir.sh

// create the file containing the checks that you wish to run
delete __appendfile
appendfile GEN000020
appendfile GEN000480
appendfile GEN000560
delete ../../scm_preserve/SunOS/5.10/daily.txt
move __appendfile ../../scm_preserve/SunOS/5.10/daily.txt
```

Parametizing checks of UNIX content

Use the task that is associated with a particular Fixlet to modify parameters for content from the console.

You can customize security policies and change the values for defined configuration settings to meet specific corporate policies. Use Endpoint Manager to customize the content in the default Fixlet site by special targeting, customizing parameters, and disabling checks. Custom sites offer greater flexibility.

Fixlet checks can be parameterized to suit each individual situation. Because parameters are stored as site settings, you can parameterize the same check differently for each site containing a copy of the check.

1. To open a task, click the **Check Parameterization** link under the **Description** tab.
2. Go to the Actions box and see the two actions that are associated with the task. Use the first action to toggle the evaluation and the second action to modify the parameter that is associated with the check.
3. Click the second link to configure the parameter for the check. The recommended parameter is the default value or the last value that you entered if you previously customized the parameter. Enter a new value or click **OK** to accept the existing value.
4. Select the parameters of your action in the Take Action dialog and click **OK**.

You have now set a parameter for the specified Fixlet, which propagates to the targeted computers to align them with your corporate policy.

Running checklists

When you run the Deploy and Run Security Checklist, the Master Run script `runme.sh` runs all the check scripts. When you run the Deploy and Run Security Checklist task, the Master Run script runs the individual check scripts located on the UNIX system.

You can modify the this behavior using the –F option to schedule specific checks. Use -G to run global checks. The Master Run script also creates a file named `/var/opt/BESClient/SCM/mytmp/results/master.results` which contains the overall results of running the various OS-specific scripts.

Understanding the output

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

With most BigFix content, Fixlets constantly evaluate conditions on each endpoint. The console shows the results when the relevance clause of the Fixlet evaluates to true.

With UNIX content, a task initiates a scan of the endpoints, which can be run on an ad hoc basis each time a scan is required. It can also be run as a recurring policy from the console.

The endpoint scan is accomplished by a series of UNIX Bourne shell scripts. While each script runs, it detects a setting or condition. The script writes the information to an output file that is made available to the corresponding Fixlet check for evaluation. When the log files are written to disk, the Fixlets read each log file and show the results in the console. Although the result is similar, this method of detection provides greater accessibility to UNIX system administrators.

After you run the Deploy and Run Security Checklist task, the scripts are in a directory under `/var/opt/BESClient/SCM`.

The following image is a graphical representation of the directory structure.

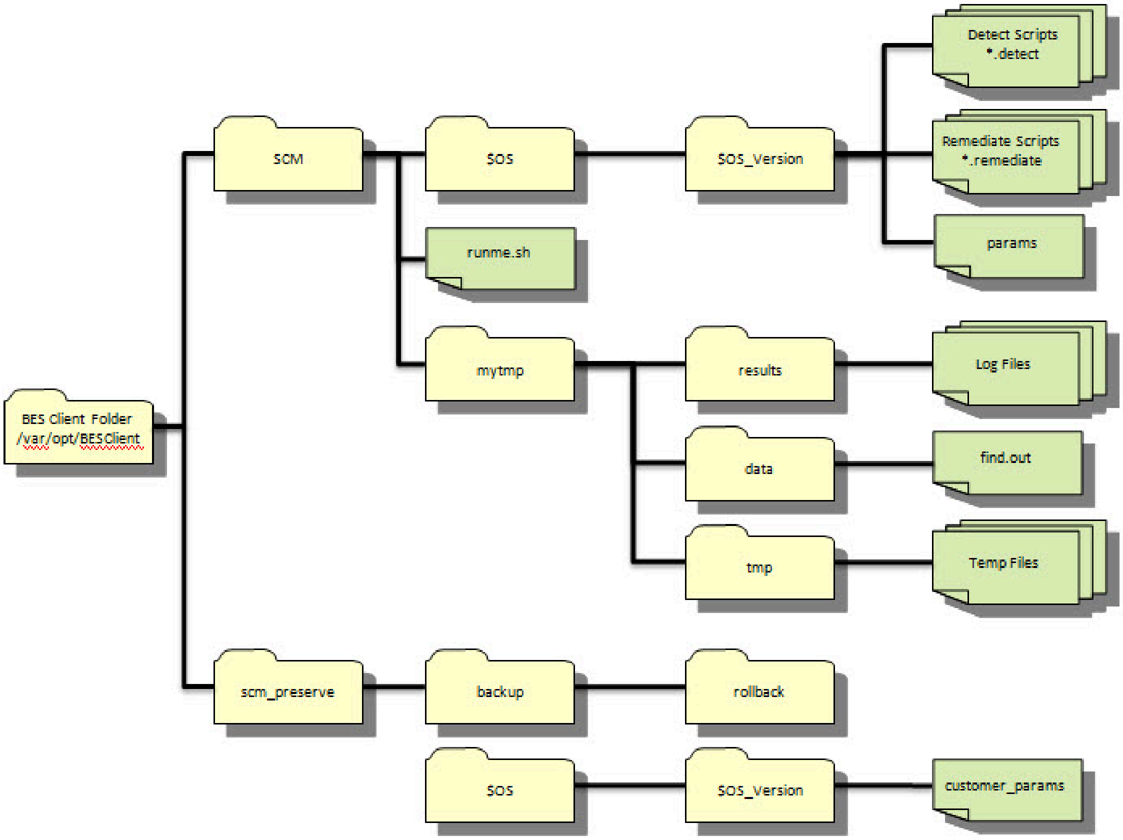


Table 3. Description of directories, subdirectories, and files

Directory/Script	Description
<BES Client Folder> / SCM	This directory is the base directory for the OS-specific check scripts and the master script (runme.sh). The contents of this directory are overwritten each time the 'Deploy and Run Security Checklist' task is run from the Endpoint Manager console.
../SCM/util	A subdirectory of the BES Client Folder / SCM directory, this subdirectory contains utility scripts that are used by the master script and in the individual detection and remediation scripts. The primary utility that is found in this directory is the 'globalfind' script.
../SCM/$OS/	This directory is specific to the platform on which it runs, as specified by $OS and $OS version. For example, the Red Hat Enterprise Linux 4 shows as (../SCM/Linux/4). This directory path contains the specific detection scripts, remediation scripts, and the base parameter file that is used by the scripts. Each check

Table 3. Description of directories, subdirectories, and files

(continued)

Directory/Script	Description
$OS_version	script is named with the corresponding control ID that is used to describe the check. Each corresponding Fixlet also references the check ID.
../SCM/runme.sh	This script is the master script that is called by the Deploy and Run Security Checklist task within the Endpoint Manager console. This script runs the 'globalfind' script and the individual check scripts.
../SCM/mytmp/results	This folder is where the OS-specific detection scripts write their log files. These logs are examined by Fixlets and used to determine if a check is compliant or non-compliant. Each log file corresponds to the check ID for the given check.
../SCM/mytmp/data	This folder contains the **find.out** file. This file is generated by the **globalfind** script and contains a directory listing of all local file systems and other information. This file is used by many of the OS-specific scripts and is updated only when the **globalfind** script is run.
<BES Client Folder>/scm_preserve	This directory is the base directory that is used to retain the rollback scripts, custom checks, parameters, and other information that is not intended to be overwritten each time the 'Deploy and Run Security Checklist' task is run.
../scm_preserve/backup/rollback	Each time a remediation script is run, a corresponding rollback script is created. This script allows the administrator to roll back to the previous setting associated with the specific check.
../scm_preserve/$OS/$OS_version	This directory might contain custom scripts that are produced by the administrator and not provided by Endpoint Manager. Scripts that are in this directory must conform to the input or output specifications are run with out-of- the-box checks when running the 'Deploy and Run Security Checklist' task.

Table 3. Description of directories, subdirectories, and files

(continued)

Directory/Script	Description
../scm_preserve/$OS/$OS_version /customer_params	This file is used to store any custom parameters that are defined by the administrator. Any parameters defined in this file override the default parameters specified in the **params** file stored in <BES Client Folder>/SCM/$OS/$OS_version/params).

Each operating system-specific script writes two files in **/var/opt/BESClient/mytmp/results**. The filenames correspond to the name of the OS-specific script. For example GEN000020.detect writes two files GEN000020.detect.log and GEN000020.results.

The file with the .log extension contains the STDOUT and STDERR of the operating system-specific script. Under normal conditions, this file is empty. When **runme.sh** is run with the **–t** option, this file contains the trace output of the operating system-specific script.

When created, the files with the **.results** extension are read by a Fixlet and the result becomes available through the Endpoint Manager console. The Fixlets examine the [STATUS] section to determine relevance.

The following is an example of a results file:

```
[RUN_DATE]
01 Apr 2008
[RUN_DATE_EOF]
[DESCRIPTION]
The UNIX host is configured to require a password for access to single-user
and maintenance modes
[DESCRIPTION_EOF]
[FIXLET_DESCRIPTION]
This UNIX host is not configured to require a password for access to single-user
and maintenance modes
[FIXLET_DESCRIPTION_EOF]
[CHECK_COVERAGE]
DISA-STIG-GEN000020
```

```
[CHECK_COVERAGE_EOF]
[STATUS]
PASS
[STATUS_EOF]
[PARAMETERS]
CONFIG_FILE=/etc/default/sulogin;SETTING=PASSREQ;OP='=';VALUE=NO
[PARAMETERS_EOF]
[TIMETAKEN]
0
[TIMETAKEN_EOF]
[REASON]
The /etc/default/sulogin file does not exist, the system will default to
requiring a password for single-user and maintenance modes
[REASON_EOF]
```

Each of the sections found within the log file output are described in the following table:

Table 4. Descriptions of sections found within the log file output

Section Name	Description
[RUN_DATE]	Contains the date that the script was run.
[DESCRIPTION] and [FIXLET_DESCRIPTION] Deprecated	No longer used – deprecated file
[CHECK_COVERAGE]	Contains the names of the regulations to which this Fixlet applies. (No longer used – deprecated files)
[STATUS]	Used by the associated Fixlet to determine relevance. It contains one of the following strings: PASS, FAIL, or NA. If this section contains the string FAIL, then the associated Fixlet becomes relevant.
[PARAMETERS]	Contains the parameters associated with the script. Spaces display as a semicolon. On output into this file, spaces are converted to semicolons for display purposes. This is not representative of how the parameters are set.
[TIMETAKEN]	Contains the number of seconds of wall-clock time that the script took to run.
[REASON]	Contains a description of why the script passed or failed. This section provides information needed to construct analysis properties and return specific information to the Endpoint Manager Console.

The **runme.sh** script also creates a file containing the overall results of running the various OS-specific scripts.

This file, named **/var/opt/BESClient/SCM/mytmp/results/master.results**,displays as follows:

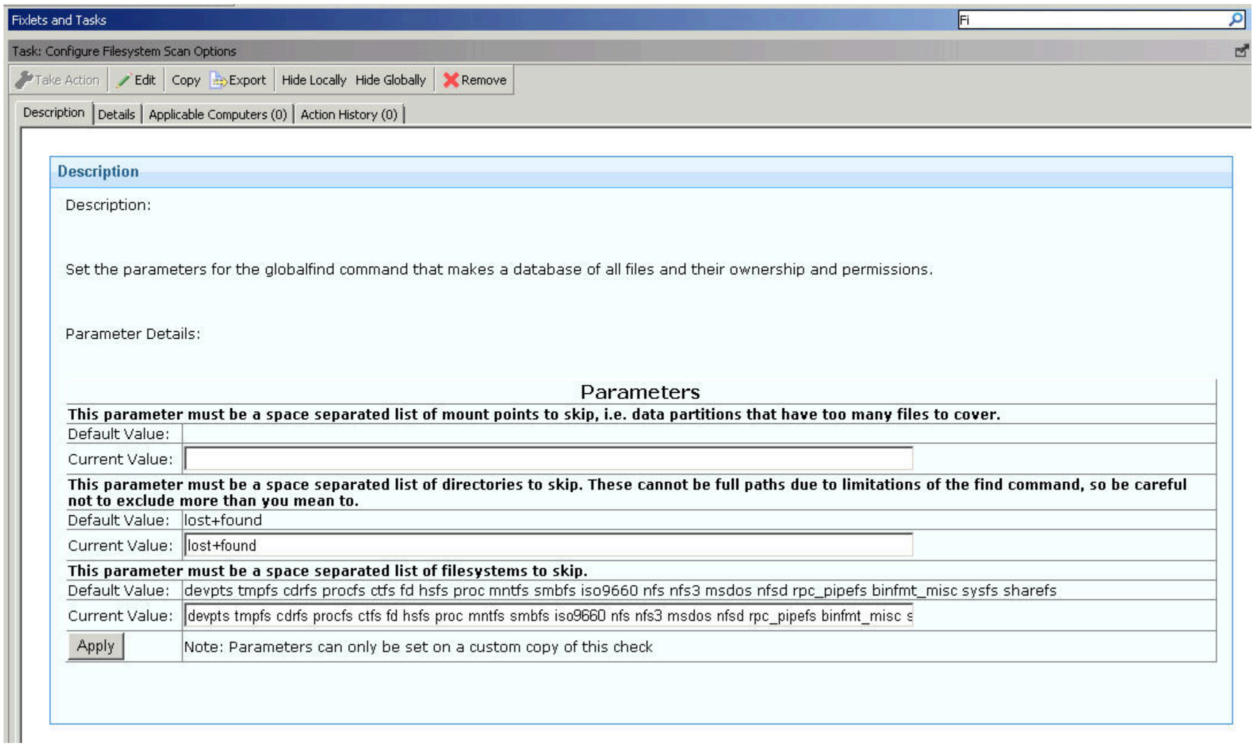
```
TOTAL_SCRIPTLETS_RUN:69

TOTAL_SCRIPTLETS_PASS:33

TOTAL_SCRIPTLETS_FAIL:36

TOTAL_SCRIPTLETS_NA:0

TOTAL_SCRIPTLETS_ERR:0

TOTAL_TIME_TAKEN:1367
```

Modifying global scan options

You can control the behavior of the global scan through the Configure Filesystems Scan Options task.

UNIX content includes a global scan script that is used to do a full system scan. The results of this scan are used in a number of 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.

The global scan script runs by default when you are using the Endpoint Manager Deploy and Run Security Checklist task. It is used by the Master Run script with the use of the –g option. The behavior of the global scan script can be controlled through the Configure Filesystems Scan Options task.



Description

Description:

Set the parameters for the globalfind command that makes a database of all files and their ownership and permissions.

Parameter Details:

Parameters

This parameter must be a space separated list of mount points to skip, i.e. data partitions that have too many files to cover.	
Default Value:	
Current Value:	
This parameter must be a space separated list of directories to skip. These cannot be full paths due to limitations of the find command, so be careful not to exclude more than you mean to.	
Default Value:	lost+found
Current Value:	lost+found
This parameter must be a space separated list of filesystems to skip.	
Default Value:	devpts tmpfs cdrfs procfs ctfs fd hsfs proc mntfs smbfs iso9660 nfs nfs3 msdos nfsd rpc_pipefs binfmt_misc sysfs sharefs
Current Value:	devpts tmpfs cdrfs procfs ctfs fd hsfs proc mntfs smbfs iso9660 nfs nfs3 msdos nfsd rpc_pipefs binfmt_misc s
Apply	Note: Parameters can only be set on a custom copy of this check

Table 5. Parameters and their descriptions

Parameter	Description
EXCLUDE-FS	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. By default, the global find script excludes the following file system types from its search: • cdrfs • procfs • ctfs • fd • hsfs • proc • mntfs • smbfs • iso9660 • nfs • msdos • devpts • tmpfs • cdrfs • procfs • ctfs • fd • hsfs • proc • mntfs • smbfs • iso9660 • nfs • cifs • msdos • nfsd • rpc_pipefs • binfmt_misc • sysfs

Table 5. Parameters and their descriptions

(continued)

Parameter	Description
	• sharefs • cgroup
EXCLUDEMOUNTS	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. 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" By default, this parameter is not used and is represented as an empty value.
EXCLUDEDIRS	List of directories to exclude from scanning. Any directory names specified in EXCLUDEDIRS are omitted from the directory listing. By default, this parameter excludes the lost+found directory.

Note: When you exclude a directory, you exclude all directories with that name. For example, if you specify EXCLUDEDIRS="foo", you exclude /usr/foo and /var/opt/foo.

Scheduling specific checks

You can create a custom action to run a subset of checks on your own schedule.

The default behavior for a UNIX deployment is to run the scripts as a single batch. However, you can also run any subset of the checks on your own defined schedule. Each time that you do, the batch that you deploy overwrites any previous batch commands. The runme.sh master script provides a ‘-F’ option, which takes a file name as its argument. It has the following form:

./runme.sh -F <FILE>

This command causes runme.sh to run *only* the set of checks that are specified in <FILE>. This file is a 7-bit ASCII file with UNIX newlines that contains a list of the specific checks you want to run, as follows:

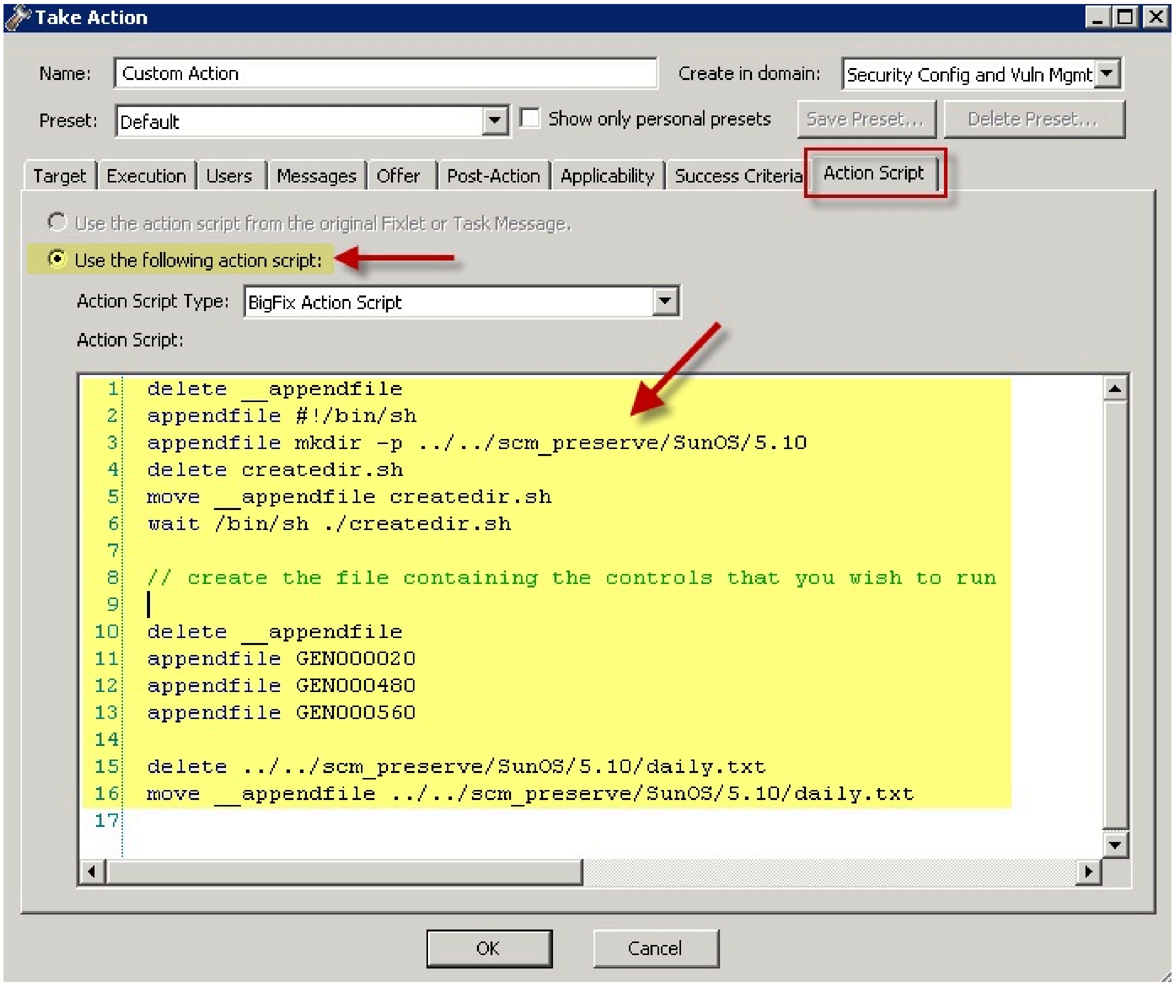
```
GEN000020

GEN000480

GEN000560
```

To select a specific script and run schedule, create a custom action. This action creates the file that contains the list of checks and deploys it to Endpoint Manager clients. This action is similar to the creation of a custom parameter file.

1. In the console, go to **Tools > Take Custom Action** to access the Take Action dialog.
2. To run the action on computers with a custom relevance clause, click the **Applicability** tab and select **...the following relevance clause evaluates to true.**.
3. In the text box, enter a relevance clause to identify the subset of computers you want to target.
   For example, to restrict the action to Solaris 10 systems, enter the following expression:

```
name of operating system = “SunOS 5.10 (not exists

last active time of it or (now - last active time of

it) > (15 *minute)) of action
```

4. Click the **Action Script** tab to create a script that copies your file onto target computers. Click the second button and enter a script like the one in the following screen capture.



Name: Custom Action

Create in domain: Security Config and Vuln Mgmt

Preset: Default

□ Show only personal presets

○ Use the action script from the original Fixlet or Task Message.

● Use the following action script:

Action Script Type: BigFix Action Script

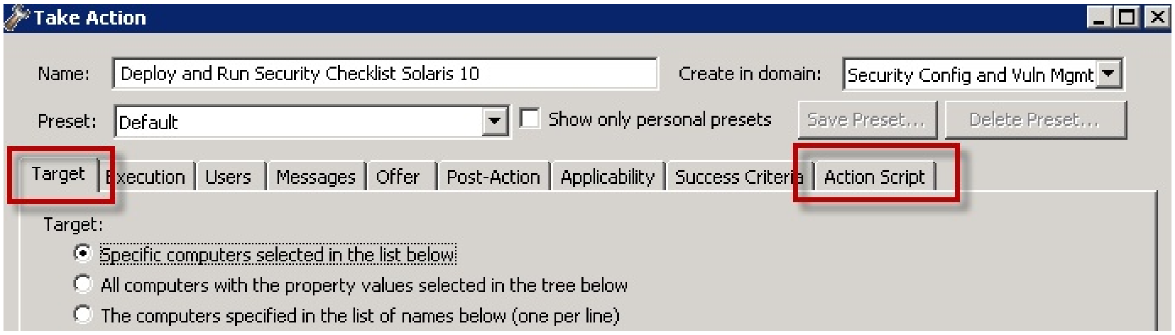
Action Script:

```
delete __appendfile
appendfile #!/bin/sh
appendfile mkdir -p ../../scm_preserve/SunOS/5.10
delete createdir.sh
move __appendfile createdir.sh
wait /bin/sh ./createdir.sh

// create the file containing the controls that you wish to run

delete __appendfile
appendfile GEN000020
appendfile GEN000480
appendfile GEN000560

delete ../../scm_preserve/SunOS/5.10/daily.txt
move __appendfile ../../scm_preserve/SunOS/5.10/daily.txt
```

5. This script creates the target directory with the file that contains the checks that you want to run and moves the file into the appropriate directory. You can copy and paste the following sample script that specifies three checks, GEN000020, GEN000480, and GEN000560.

```
// create a script that will create the necessary directory
delete __appendfile
appendfile #!/bin/sh
appendfile mkdir –p ../../scm_preserve/SunOS/5.10
delete createdir.sh
move __appendfile createdir.sh
wait /bin/sh ./createdir.sh

// create the file containing the checks that you wish to run
delete __appendfile
appendfile GEN000020
appendfile GEN000480
appendfile GEN000560
delete ../../scm_preserve/SunOS/5.10/daily.txt
move __appendfile ../../scm_preserve/SunOS/5.10/daily.txt
```

6. Run the runme.sh script with the –F option. Modify the Deploy and Run Security Checklist task to run the script.



Name: Deploy and Run Security Checklist Solaris 10

Create in domain: Security Config and Vuln Mgmt

Preset: Default

☐ Show only personal presets

Target:

● Specific computers selected in the list below

○ All computers with the property values selected in the tree below

○ The computers specified in the list of names below (one per line)

   a. Find and select the Deploy and Run Security Checklist task.
   b. Click **Take Action**
   c. In the **Target** tab, then select the endpoints.

7. Click the **Action Script** tab. Modify the Action Script to make runme.sh use the –F option and point to the file that contains the check list. The file in the example is named `daily.txt`.
8. You can copy, paste, and modify the following sample script.

```
prefetch DISA.zip sha1:99c90759cc496c506222db55bd864eba4063b955 size:108089
http://software.bigfix.com/download/SCM/SunOS-20080417.zip
delete __appendfile
delete run_SCM.sh
appendfile #!/bin/sh
if {exists folder ((pathname of parent folder of parent folder of folder
(pathname of client folder of current site)) & "/SCM")}
 appendfile rm -rf {((pathname of parent folder of parent folder of folder
(pathname of client folder of current site)) & "/SCM")}
endif
appendfile mv __Download/DISA.zip {((pathname of parent folder of parent
folder of folder (pathname of client folder of current site)))}
appendfile cd {((pathname of parent folder of parent folder of folder
(pathname of client folder of current site)))}
appendfile gzip -dvS .zip DISA.zip
appendfile FILE=`ls -1 DISA* | grep -v zip`
appendfile tar xf $FILE
appendfile rm -rf $FILE
appendfile cd {((pathname of parent folder of parent folder of folder
(pathname of client folder of current site)) & "/SCM")}
appendfile ./runme.sh -F ../scm_preserve/SunOS/5.10/daily.txt
move __appendfile run_SCM.sh
wait sh ./run_SCM.sh
```

Analyses

Each check Fixlet in the DISA UNIX content has an associated analysis. Check Fixlets display the compliance state, and analyses display the state of each configuration item.

These analyses are provided to enable the display of Measured Values in HCL Endpoint Manager Security and Compliance Analytics. If you are using only a subset of the available check Fixlets for your implementation, activate only the analyses that are associated with the check Fixlets you are using.

Using the Create Custom Relevance SCM content wizard

Follow these steps to incorporate custom checks into an existing SCM custom site.

- You must have a custom site that is created through the **Create Custom Checklist** wizard in the SCM Reporting site.
- Check that the custom checks are up to date and that bug fixes are installed with the **Synchronize Custom Checks** wizard.

Use this dashboard to incorporate custom checks into an existing SCM Custom site.

1. In the **Security Configuration Domain**, go to **All Security Configuration > Wizards > Create Custom Relevance SCM Content**. The **Create Custom Relevance SCM checks** wizard opens
2. Enter the following required information:
    - Site
    - Applicability Fixlet
    - Fixlet title
    - SourceID
    - Source

- Source Release Date
- Category
- Severity

3. Enter the Fixlet description. You can use simple HTML format to create your description.
4. Enter the Compliance Relevance.
5. Enter the Analysis Relevance.
    a. Optional: Select the box if you want to include the desired value.
    b. Enter the title of the desired value.
    c. Enter the desired value.
6. Enter the Remediation Action Script.
7. Click **Create Fixlet**.

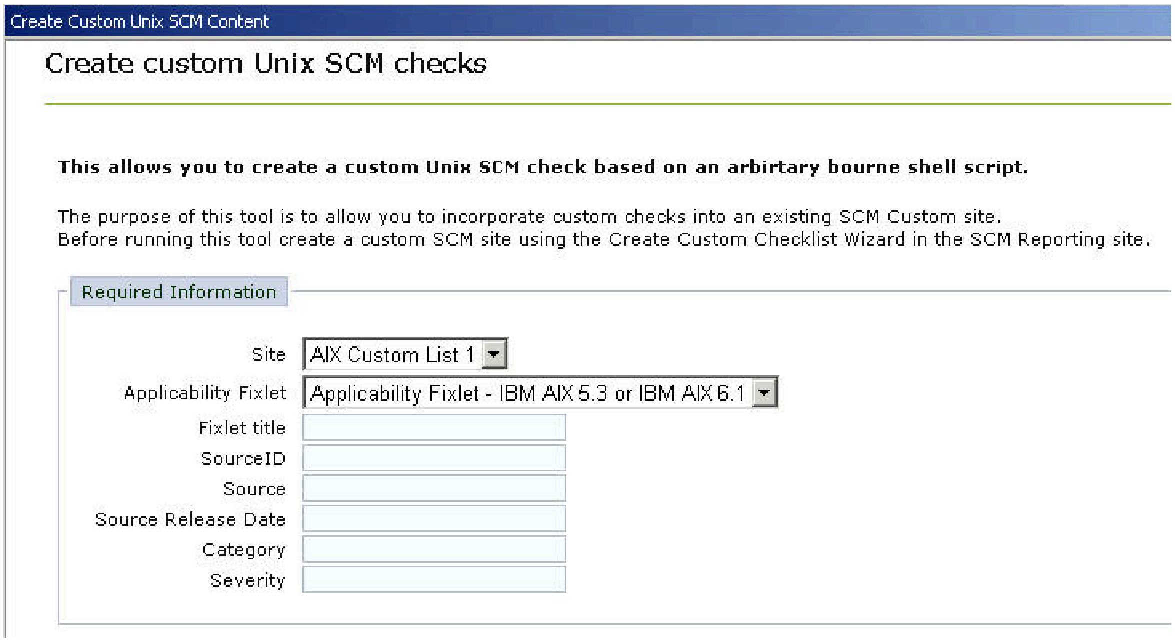
Creating custom UNIX Security Configuration Management content

Follow these steps to create custom check for UNIX Security Configuration Management.

- You must have a custom site that is created through the **Create Custom Checklist** wizard in the SCM Reporting site.
- Check that the custom checks are up to date and that bug fixes are installed with the **Synchronize Custom Checks** wizard.

Use this dashboard to incorporate custom checks into an existing SCM Custom site based on an arbitrary bourne shell script.

1. Go to **Wizards > Create Custom Unix SCM Content**. The **Create custom Unix SCM checks** dashboard opens.
2. Enter the following required information:
    - Site
    - Applicability Fixlet
    - Fixlet title
    - SourceID
    - Source
    - Source Release Date
    - Category
    - Severity



Create Custom Unix SCM Content

Create custom Unix SCM checks

This allows you to create a custom Unix SCM check based on an arbirtary bourne shell script.

The purpose of this tool is to allow you to incorporate custom checks into an existing SCM Custom site.
Before running this tool create a custom SCM site using the Create Custom Checklist Wizard in the SCM Reporting site.

Required Information

Site	AIX Custom List 1
Applicability Fixlet	Applicability Fixlet - IBM AIX 5.3 or IBM AIX 6.1
Fixlet title	
SourceID	
Source	
Source Release Date	
Category	
Severity	

3. Enter the Fixlet description. You can use simple HTML format to create your description.
4. Enter the Compliance Relevance.
5. Enter the Analysis Relevance.
    a. Optional: Select the box if you want to include the desired value.
    b. Enter the title of the desired value.
    c. Enter the desired value.
6. Enter the Remediation Action Script.
7. Click **Create Fixlet**.

Once the scan is complete, customers can start an import to the Security and Compliance Analytics.

Importing SCAP content

Learning about 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

HCL BigFix takes the SCAP checklist XML, generates BigFix content from it, and makes it available through subscription. Users load the external site mastheads for each of the available SCAP checklists in the BigFix console. The BigFix server downloads the content and makes it available to the BigFix administrator to begin evaluating on systems.

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

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

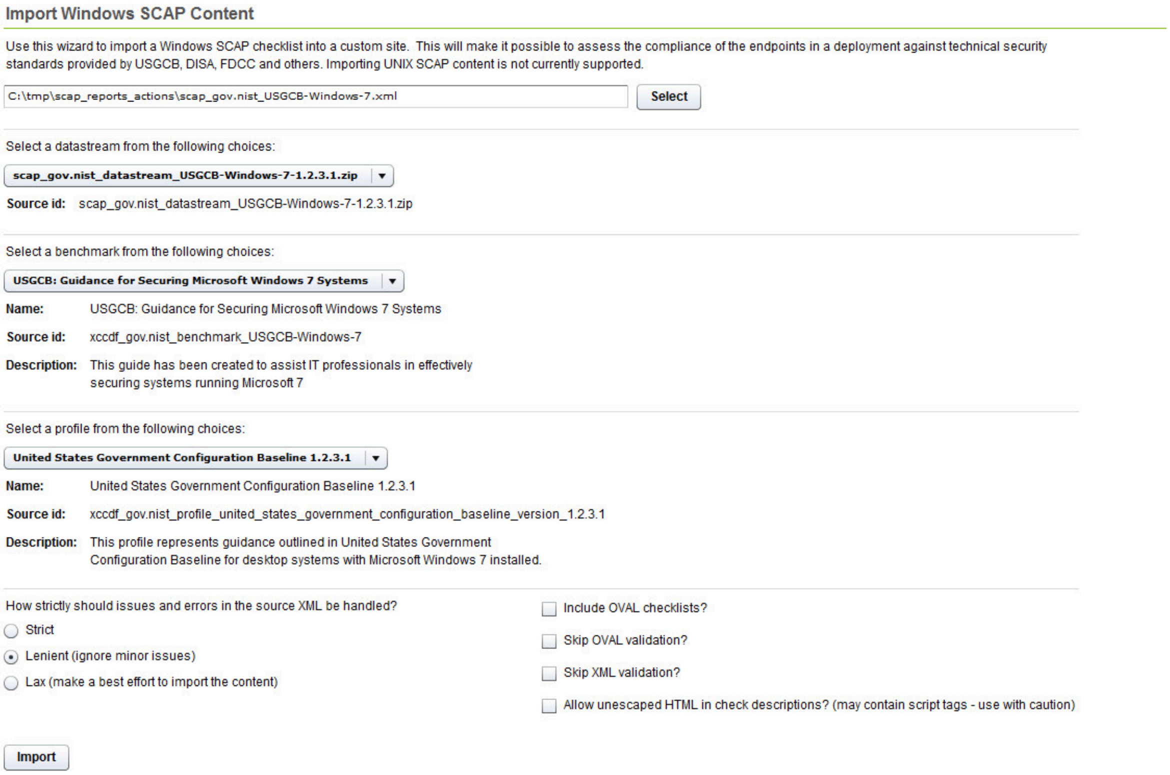
Note: These values are examples of the file checksum function for the SCAP Tools. The value varies with each published release version of the SCAP Tools. For values that are applicable to new SCAP releases, see SCAP Release Notes.

- **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)

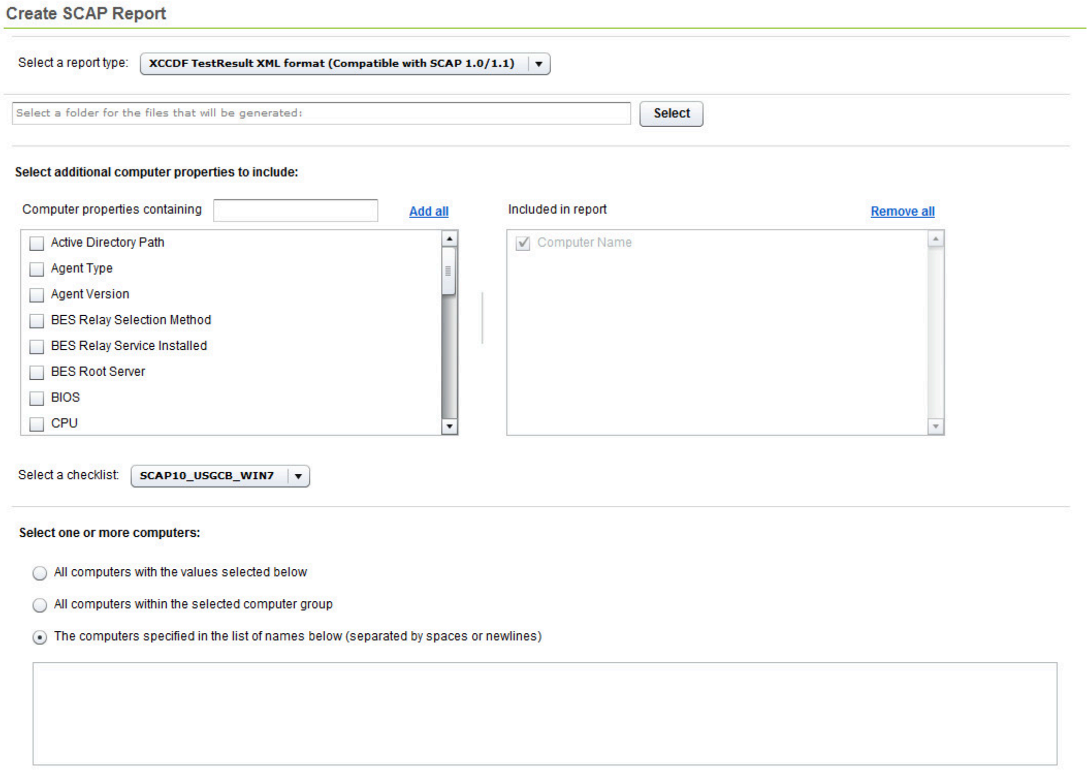
3. When the source content has more than one data stream, you can choose the data stream options from the dropdown menu. Select the data stream to import.
4. When the source content has more than one benchmark, you can choose the benchmark options from the dropdown menu. Select the benchmark to import.
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 Create SCAP Compatible Report wizard

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 additional computer properties to include:

Computer properties containing

Included in report

☐ Active Directory Path
☐ Agent Type
☐ Agent Version
☐ BES Relay Selection Method
☐ BES Relay Service Installed
☐ BES Root Server
☐ BIOS
☐ CPU

☑ Computer Name

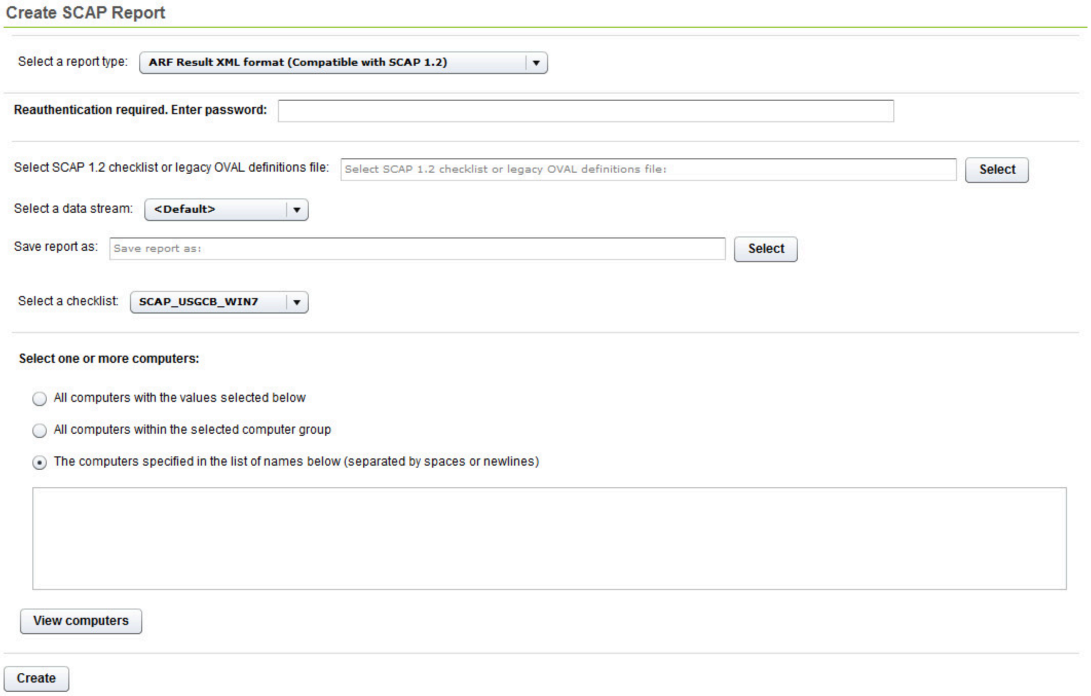
Select a checklist: SCAP10_USGCB_WIN7

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 SCAP 1.2 checklist or legacy OVAL definitions file:

Select a data stream: <Default>

Save report as: Save report as:

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)

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 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.

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.

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.

Glossary

This glossary provides terms and definitions for the Modern Client Management for BigFix software and products.

The following cross-references are used in this glossary:

- *See* refers you from a nonpreferred term to the preferred term or from an abbreviation to the spelled-out form.
- *See also* refers you to a related or contrasting term.

A *(on page 43)* B *(on page 44)* C *(on page 44)* D *(on page 46)* E *(on page 47)* F *(on page 47)* G *(on page 48)* L *(on page 48)* M *(on page 48)* N *(on page 49)* O *(on page 49)* P *(on page 49)* R *(on page 49)* S *(on page 50)* T *(on page 51)* U *(on page 52)* V *(on page 52)* W *(on page 52)*

A

action

1. See Fixlet *(on page 47)*.
2. A set of Action Script commands that perform an operation or administrative task, such as installing a patch or rebooting a device.

Action Script

Language used to perform an action on an endpoint.

agent

See BigFix agent *(on page 44)*.

ambiguous software

Software that has an executable file that looks like another executable file, or that exists in more than one place in a catalog (Microsoft Word as a standalone product or bundled with Microsoft Office).

audit patch

A patch used to detect conditions that cannot be remediated and require the attention of an administrator. Audit patches contain no actions and cannot be deployed.

automatic computer group

A computer group for which membership is determined at run time by comparing the properties of a given device against the criteria set for group membership. The set of devices in an automatic group is dynamic, meaning that the group can and does change. See also computer group *(on page 45)*.

B

baseline

A collection of actions that are deployed together. A baseline is typically used to simplify a deployment or to control the order in which a set of actions are applied. See also deployment group *(on page 46)*.

BigFix agent

The BigFix code on an endpoint that enables management and monitoring by BigFix.

BigFix client

See BigFix agent *(on page 44)*.

BigFix console

The primary BigFix administrative interface. The console provides a full set of capabilities to BigFix administrators.

BYOD

Bring Your Own Device (BYOD) refers to employees using personal devices to connect to their organizational networks and access work-related systems and potentially sensitive or confidential data.

C

client

A software program or computer that requests services from a server. See also server *(on page 50)*.

client time

The local time on a BigFix client device.

Cloud

A set of compute and storage instances or services that are running in containers or on virtual machines.

Common Vulnerabilities and Exposures Identification Number (CVE ID)

A number that identifies a specific entry in the National Vulnerability Database. A vendor's patch document often includes the CVE ID, when it is available. See also National Vulnerability Database *(on page 49)*.

Common Vulnerabilities and Exposures system (CVE)

A reference of officially known network vulnerabilities, which is part of the National Vulnerabilities Database (NVD), maintained by the US National Institute of Standards and Technology (NIST).

component

An individual action within a deployment that has more than one action. See also deployment group *(on page 46)*.

computer group

A group of related computers. An administrator can create computer groups to organize systems into meaningful categories, and to facilitate deployment of content to multiple computers. See also automatic computer group *(on page 44)* and manual computer group *(on page 48)*.

console

See BigFix console *(on page 44)*.

content

Digitally-signed files that contain data, rules, queries, criteria, and other instructions, packaged for deployment across a network. BigFix agents use the detection criteria (Relevance statements) and action instructions (Action Script statements) in content to detect vulnerabilities and enforce network policies.

content relevance

A determination of whether a patch or piece of software is eligible for deployment to one or more devices. See also device relevance *(on page 47)*.

Coordinated Universal Time (UTC)

The international standard of time that is kept by atomic clocks around the world.

corrupt patch

A patch that flags an operator when corrections made by an earlier patch have been changed or compromised. This situation can occur when an earlier service pack or application overwrites later files, which results in patched files that are not current. The corrupt patch flags the situation and can be used to re-apply the later patch.

custom content

BigFix code that is created by a customer for use on their own network, for example, a custom patch or baseline.

CVE

See Common Vulnerabilities and Exposures system *(on page 45)*.

CVE ID

See Common Vulnerabilities and Exposures Identification Number *(on page 45)*.

D

data stream

A string of information that serves as a source of package data.

default action

The action designated to run when a Fixlet is deployed. When no default action is defined, the operator is prompted to choose between several actions or to make an informed decision about a single action.

definitive package

A string of data that serves as the primary method for identifying the presence of software on a computer.

deploy

To dispatch content to one or more endpoints for execution to accomplish an operation or task, for example, to install software or update a patch.

deployment

Information about content that is dispatched to one or more endpoints, a specific instance of dispatched content.

deployment group

The collection of actions created when an operator selects more than one action for a deployment, or a baseline is deployed. See also baseline *(on page 44)*, component *(on page 45)*, deployment window *(on page 46)*, and multiple action group *(on page 49)*.

deployment state

The eligibility of a deployment to run on endpoints. The state includes parameters that the operator sets, such as 'Start at 1AM, end at 3AM.'

deployment status

Cumulative results of all targeted devices, expressed as a percentage of deployment success.

deployment type

An indication of whether a deployment involved one action or multiple actions.

deployment window

The period during which a deployment's actions are eligible to run. For example, if a Fixlet has a deployment window of 3 days and an eligible device that has been offline reports in to BigFix within the

3-day window, it gets the Fixlet. If the device comes back online after the 3-day window expires, it does not get the Fixlet. See also deployment group *(on page 46)*.

device

An endpoint, for example, a laptop, desktop, server, or virtual machine that BigFix manages; an endpoint running the BigFix Agent.

device holder

The person using a BigFix-managed computer.

device property

Information about a device collected by BigFix, including details about its hardware, operating system, network status, settings, and BigFix client. Custom properties can also be assigned to a device.

device relevance

A determination of whether a piece of BigFix content applies to applies to a device, for example, where a patch should be applied, software installed, or a baseline run. See also content relevance *(on page 45)*.

device result

The state of a deployment, including the result, on a particular endpoint.

Disaster Server Architecture (DSA)

An architecture that links multiple servers to provide full redundancy in case of failure.

DSA

See Disaster Server Architecture *(on page 47)*.

dynamically targeted

Pertaining to using a computer group to target a deployment.

E

endpoint

A networked device running the BigFix agent.

F

filter

To reduce a list of items to those that share specific attributes.

Fixlet

A piece of BigFix content that contains Relevance and Action Script statements bundled together to perform an operation or task. Fixlets are the basic building blocks of BigFix content. A Fixlet provides instructions to the BigFix agent to perform a network management or reporting action.

Full Disk Encryption

To reduce a list of items to those that share specific attributes.

G

group deployment

A type of deployment in which multiple actions were deployed to one or more devices.

L

locked

An endpoint state that prevents most of the BigFix actions from running until the device is unlocked.

M

MAG

See multiple action group *(on page 49)*.

management rights

The limitation of console operators to a specified group of computers. Only a site administrator or a master operator can assign management rights.

manual computer group

A computer group for which membership is determined through selection by an operator. The set of devices in a manual group is static, meaning they do not change. See also computer group *(on page 45)*.

master operator

A console operator with administrative rights. A master operator can do everything that a site administrator can do, except creating operators.

masthead

A collection of files that contain the parameters of the BigFix process, including URLs to Fixlet content. The BigFix agent brings content into the enterprise based on subscribed mastheads.

MCM and BigFix Mobile

Refers to the offering by Bigfix that is common for both Modern Client Management to manage laptops (Windows and macOS) and BigFix Mobile to manage mobile devices (Android, iOS, and iPadOS).

mirror server

A BigFix server required if the enterprise does not allow direct web access but instead uses a proxy server that requires password-level authentication.

Multicloud

The utilization of distinct sets of cloud services, typically from multiple vendors, where specific applications are confined to a single cloud instance.

multiple action group (MAG)

A BigFix object that is created when multiple actions are deployed together, as in a baseline. A MAG contains multiple Fixlets or tasks. See also deployment group *(on page 46)*.

N

National Vulnerability Database (NVD)

A catalog of officially known information security vulnerabilities and exposures, which is maintained by the National Institute of Standards and Technology (NIST). See also Common Vulnerabilities and Exposures Identification Number *(on page 45)*.

NVD

See National Vulnerability Database *(on page 49)*.

O

offer

A deployment option that allows a device holder to accept or decline a BigFix action and to exercise some control over when it runs. For example, a device holder can decide whether to install a software application, and whether to run the installation at night or during the day.

open-ended deployment

A deployment with no end or expiration date; one that runs continuously, checking whether the computers on a network comply.

operator

A person who uses the BigFix WebUI, or portions of the BigFix console.

P

patch

A piece of code added to vendor software to fix a problem, as an immediate solution that is provided to users between two releases.

patch category

A description of a patch's type and general area of operation, for example, a bug fix or a service pack.

patch severity

The level of risk imposed by a network threat or vulnerability and, by extension, the importance of applying its patch.

R

relay

A client that is running special server software. Relays spare the server and the network by minimizing direct server-client downloads and by compressing upstream data.

Relevance

BigFix query language that is used to determine the applicability of a piece of content to a specified endpoint. Relevance asks yes or no questions and evaluates the results. The result of a Relevance query determines whether an action can or should be applied. Relevance is paired with Action Script in Fixlets.

S

SCAP

See Security Content Automation Protocol *(on page 50)*.

SCAP check

A specific configuration check within a Security Content Automation Protocol (SCAP) checklist. Checks are written in XCCDF and are required to include SCAP enumerations and mappings per the SCAP template.

SCAP checklist

A configuration checklist that is written in a machine-readable language (XCCDF). Security Content Automation Protocol (SCAP) checklists have been submitted to and accepted by the NIST National Checklist Program. They also conform to a SCAP template to ensure compatibility with SCAP products and services.

SCAP content

A repository that consists of security checklist data represented in automated XML formats, vulnerability and product name related enumerations, and mappings between the enumerations.

SCAP enumeration

A list of all known security related software flaws (CVEs), known software configuration issues (CCEs), and standard vendor and product names (CPEs).

SCAP mapping

The interrelationship of enumerations that provides standards-based impact measurements for software flaws and configuration issues.

Security Content Automation Protocol (SCAP)

A set of standards that is used to automate, measure, and manage vulnerability and compliance by the National Institute of Standards and Technology (NIST).

server

A software program or a computer that provides services to other software programs or other computers. See also client *(on page 44)*.

signing password

A password that is used by a console operator to sign an action for deployment.

single deployment

A type of deployment where a single action was deployed to one or more devices.

site

A collection of BigFix content. A site organizes similar content together.

site administrator

The person who is in charge of installing BigFix and authorizing and creating new console operators.

software package

A collection of Fixlets that install a software product on a device. Software packages are uploaded to BigFix by an operator for distribution. A BigFix software package includes the installation files, Fixlets to install the files, and information about the package (metadata).

SQL Server

A full-scale database engine from Microsoft that can be acquired and installed into the BigFix system to satisfy more than the basic reporting and data storage needs.

standard deployment

A deployment of BigFix that applies to workgroups and to enterprises with a single administrative domain. It is intended for a setting in which all Client computers have direct access to a single internal server.

statistically targeted

Pertaining to the method used to target a deployment to a device or piece of content. Statically targeted devices are selected manually by an operator.

superseded patch

A type of patch that notifies an operator when an earlier version of a patch has been replaced by a later version. This occurs when a later patch updates the same files as an earlier one. Superseded patches flag vulnerabilities that can be remediated by a later patch. A superseded patch cannot be deployed.

system power state

A definition of the overall power consumption of a system. BigFix Power Management tracks four main power states Active, Idle, Standby or Hibernation, and Power Off.

T

target

To match content with devices in a deployment, either by selecting the content for deployment, or selecting the devices to receive content.

targeting

The method used to specify the endpoints in a deployment.

task

A type of Fixlet designed for re-use, for example, to perform an ongoing maintenance task.

U

UTC

See Coordinated Universal Time *(on page 45)*.

V

virtual private network (VPN)

An extension of a company intranet over the existing framework of either a public or private network. A VPN ensures that the data that is sent between the two endpoints of its connection remains secure.

VPN

See virtual private network *(on page 52)*.

vulnerability

A security exposure in an operating system, system software, or application software component.

W

Wake-from-Standby

A mode that allows an application to turn a computer on from standby mode during predefined times, without the need for Wake on LAN.

Wake on LAN

A technology that enables a user to remotely turn on systems for off-hours maintenance. A result of the Intel-IBM Advanced Manageability Alliance and part of the Wired for Management Baseline Specification, users of this technology can remotely turn on a server and control it across the network, thus saving time on automated software installations, upgrades, disk backups, and virus scans.

WAN

See wide area network *(on page 52)*.

wide area network (WAN)

A network that provides communication services among devices in a geographic area larger than that served by a local area network (LAN) or a metropolitan area network (MAN).

Support

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

- BigFix Support Portal
- BigFix Developer
- BigFix Playlist on YouTube

- BigFix Tech Advisors channel on YouTube
- BigFix Forum

Notices

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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.