Security Configuration Management

User's Guide

July, 2010

All inquiries regarding the foregoing should be addressed to:

BigFix, Inc.
1480 64th Street, Suite 200
Emeryville, California 94608

Contents

CONTENTS

Part 1

Getting Started

This document describes a portfolio of security configuration content from BigFix called Security Configuration Management (SCM). This content comes in the form of benchmarks (also referred to as 'checklists' or 'baselines'), which allow organizations to assess and manage the configurations of desktops, laptops, and servers. BigFix SCM is one of the few products to have achieved Security Content Automation Protocol (SCAP) Validation through the National Institute of Standards and Technology (NIST) for both misconfiguration assessment and remediation. By offering a comprehensive library of technical controls, SCM detects and enforces security configuration policies using industry best practices.

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

For information specifically related to setup or installation of SCM, please refer to the *BigFix SCM Setup Guide* located on the BigFix Support website.

System Requirements

Configure your BigFix deployment according to the following requirements:

Minimum supported browser versions:

- IE 6.0

Minimum Adobe Flash player version:

- Flash Player 9.0

Minimum BigFix component versions:

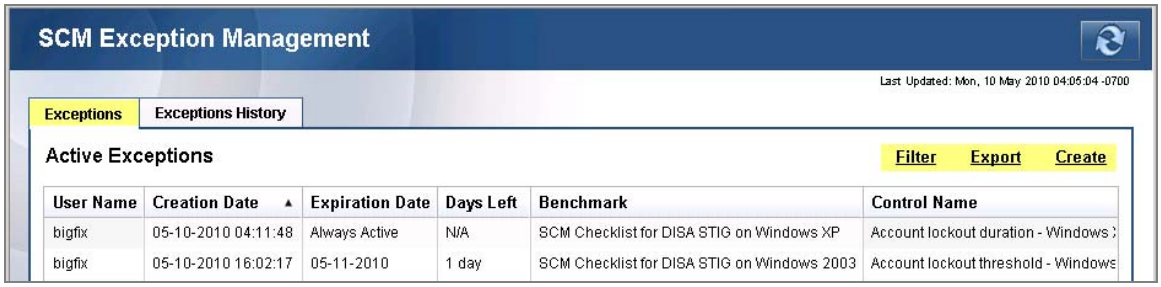
- Console 7.2.5.21
- Web Reports 7.2.5.21
- Windows Client 7.2.5.21
- UNIX Client 7.2.5.21

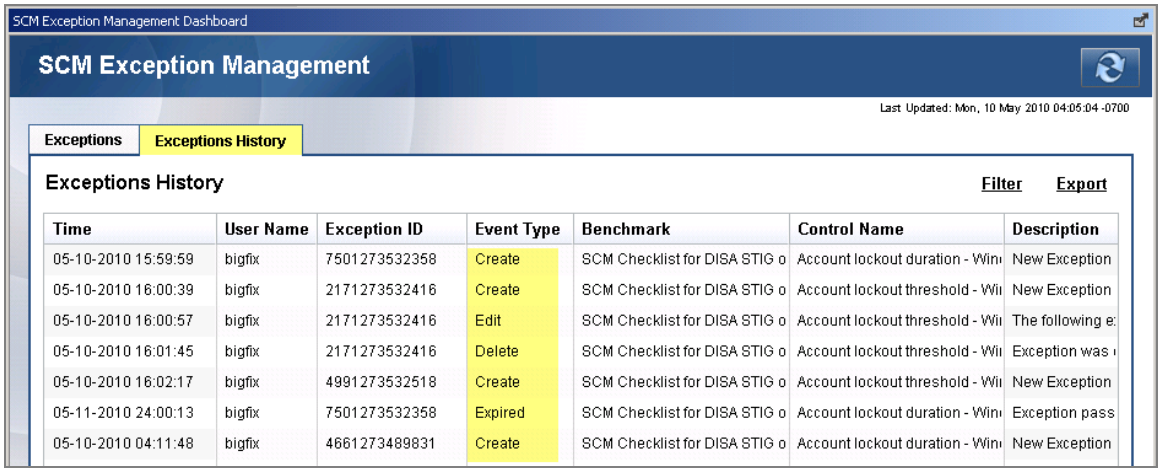
New Features

Exception Management Dashboard

The newly designed SCM Exception Management Dashboard enables you to create, customize, modify and manage rules or “exceptions” that will designate a set of computers as *compliant* based on some common details.

The Exception Management Dashboard contains *Exceptions* and *Exceptions History* tabs, which enable you to create, customize and manage exceptions.





For detailed information about managing exceptions, see the Exception Management Dashboard section of this document.

Using the New BigFix Console

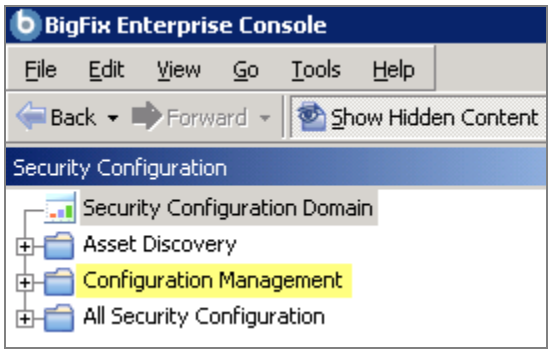
This version of BigFix SCM encompasses a host of new and upgraded features. In addition, the BigFix Console changed after version 7.2, which resulted in several new navigation updates for accessing your data. This section will address how to get around SCM in the new BigFix Console.

The navigation tree in the BigFix Console, which is available for all BigFix products, will serve as your central command for all SCM functionality. The navigation tree gives you easy access to all reports, wizards, Fixlet messages, analyses and tasks related to managing the power settings in your network.

The BigFix Console organizes content into four parts:

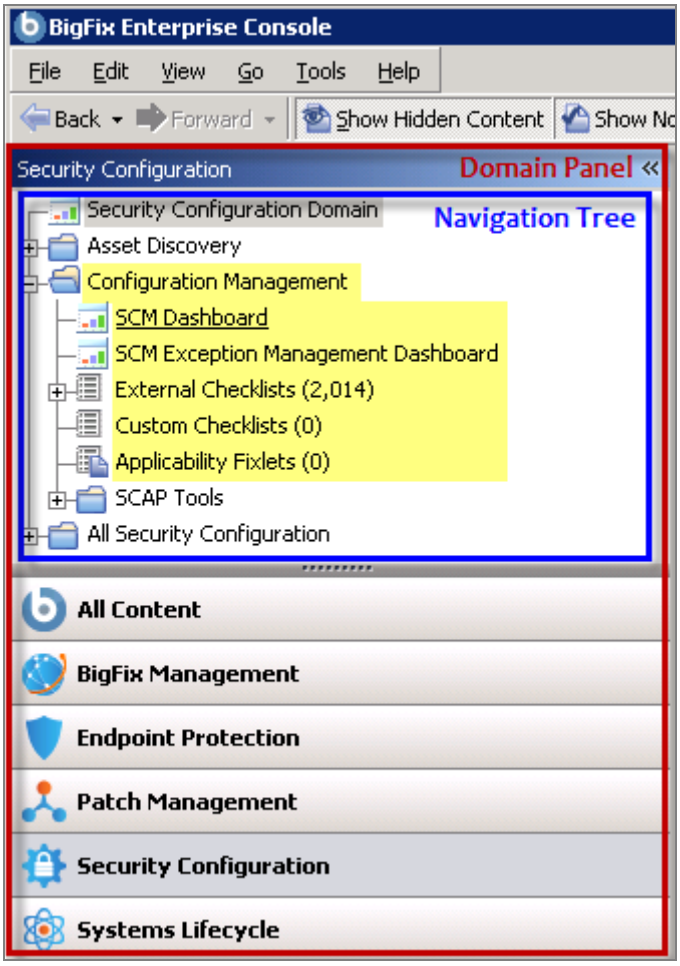
- *Domain Panel – Includes navigation tree and list of all domains*
- *Navigation Tree – Includes list of nodes and sub-nodes containing site content*
- *List Panel – Contains listing of tasks and Fixlets*
- *Work Area – Work window where Fixlet and dialogs display*

In the context of the BigFix Console, products or *sites* are grouped by categories or *domains*. For example, Configuration Management is one of the sites contained within the *Security Configuration* domain, along with Asset Discovery, among others.



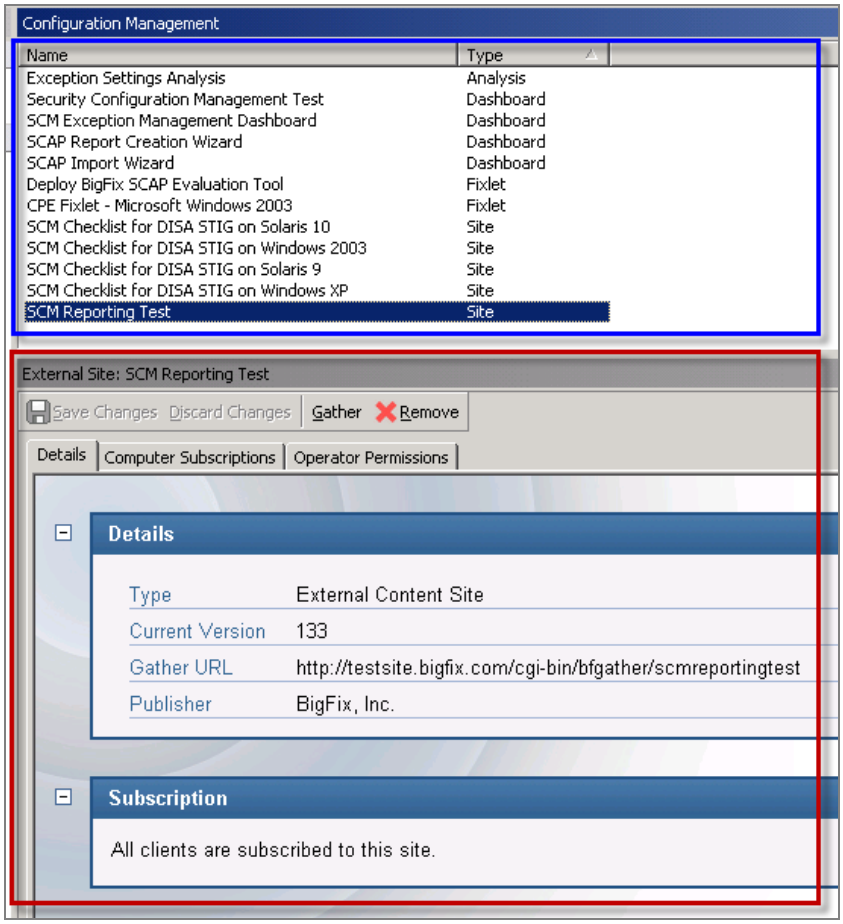
The domain panel is the area on the left side of the Console that includes a navigation tree and a list of all domains. The navigation tree includes a list of nodes and sub-nodes containing site content.

In the image below, you will see a navigation “tree” at the top with expandable and collapsible nodes, and a list of domains at the bottom. By clicking the *Security Configuration* domain from the domain panel, a list of sites associated with that particular domain will display in the navigation tree at the top.



The red-outlined area represents the entire Domain Panel (including the navigation tree and list of domains), and the blue box contains just the Navigation Tree for the *Security Configuration* domain.

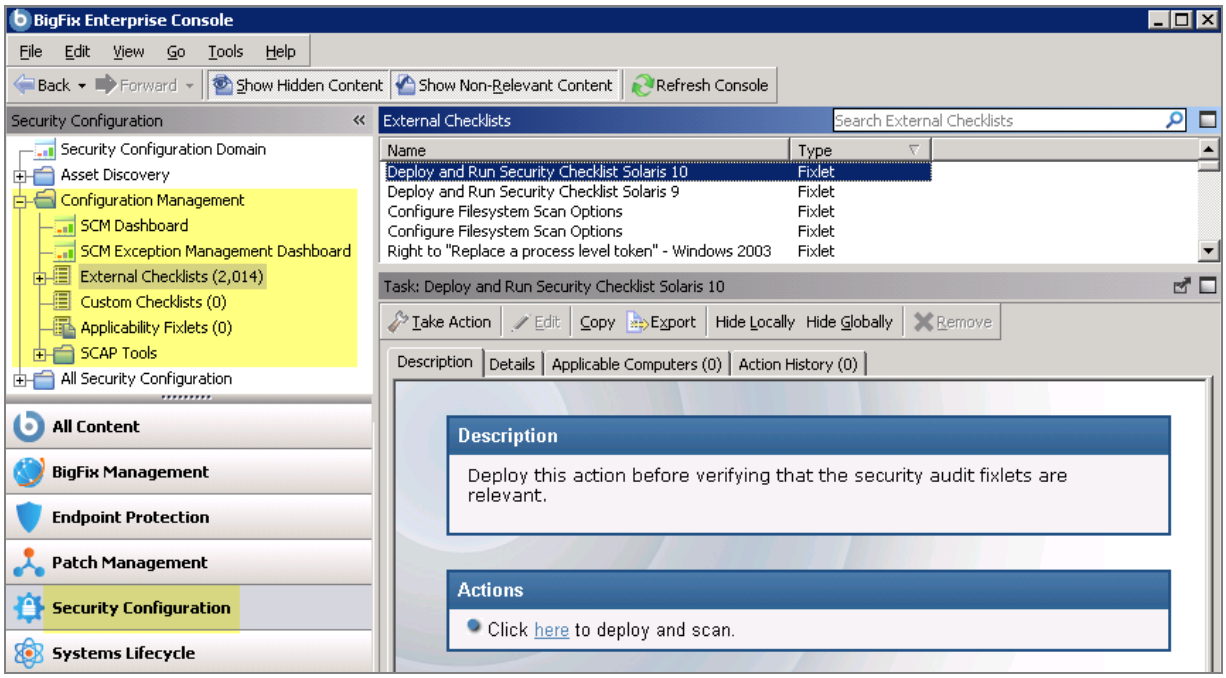
SCM tasks are sorted through upper and lower task windows, which are located on the right side of the Console.



The upper panel, called the *List Panel* (blue), contains columns that sort data according to Name, Type, Applicable Computer Count, etc.

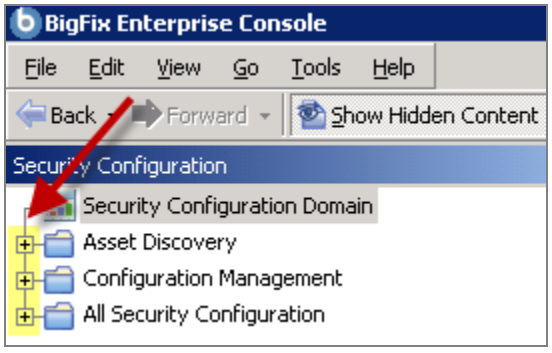
The lower panel or *Work Area* (red) presents the Fixlet, task screen or Wizard from which you will be directed to take specific actions to customize the content in your deployment.

Here's how it all looks together:

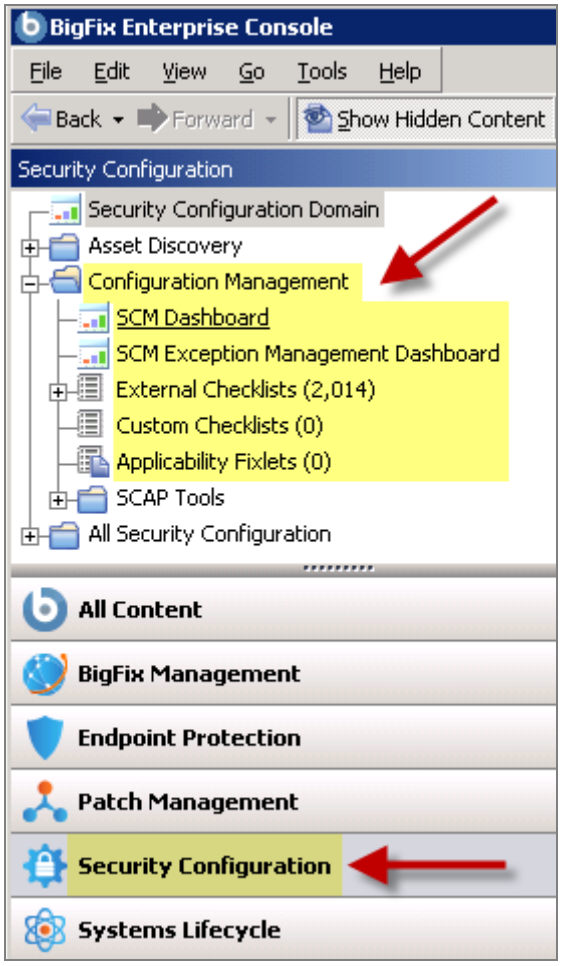


Working with Content

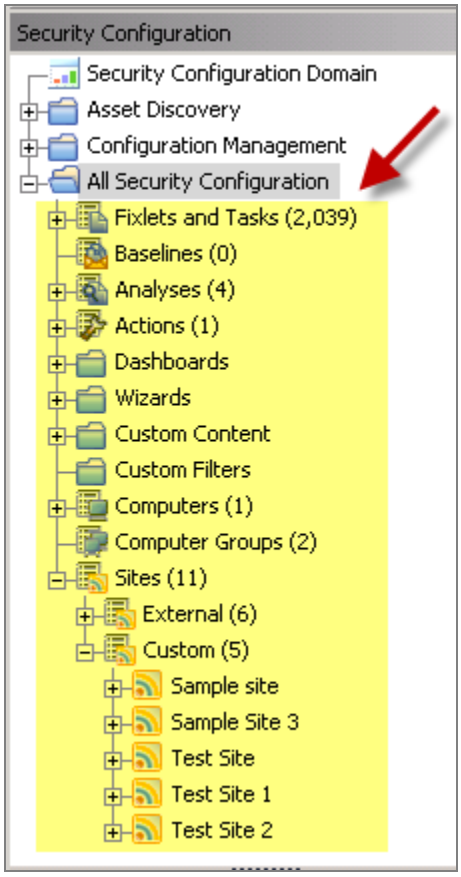
The navigation tree organizes SCM content into expandable and collapsible folders that enable you to easily navigate and manage relevant components in your deployment. Click the plus sign (+) to expand the navigation tree nodes and the minus sign (-) to collapse them.



When you click on the *Security Configuration* domain at the bottom of your screen, you will see content related to the Configuration Management "site" organized into expandable nodes.



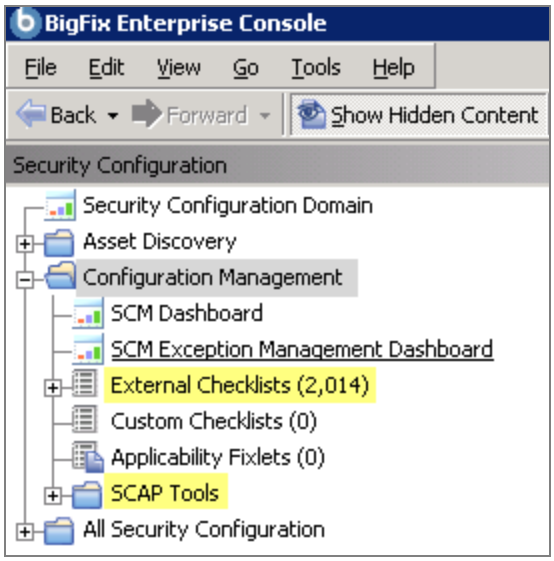
The *All Security Configuration* node includes content (analyses, dashboards, wizards, etc.) related to the entire Security Configuration domain as a whole, including all of its related "sites".



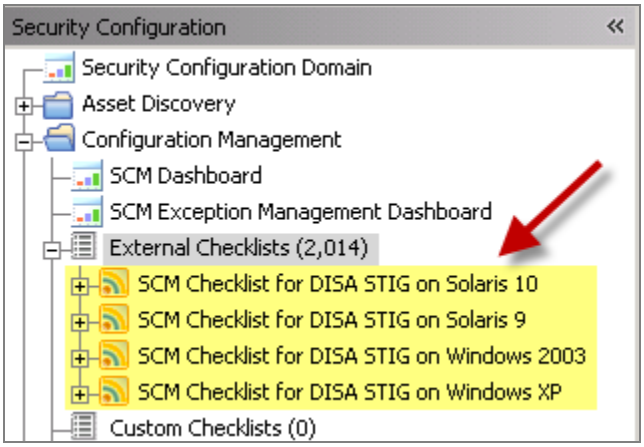
You will use this same expand/collapse method to move through the entire navigation tree.

> **Note:** Depending on your operating system, your system may display the "+" and "-" buttons in the navigation tree as triangles. Specifically, the "+" and "-" icons will display on Windows XP/2003/2008/2008R2 machines, and triangles will display on Windows Vista/7. This feature was designed so that the Console matches the standards and conventions of your specific operating system. Regardless of the particular icon, the functionality of these buttons works the same way to either expand or collapse content.

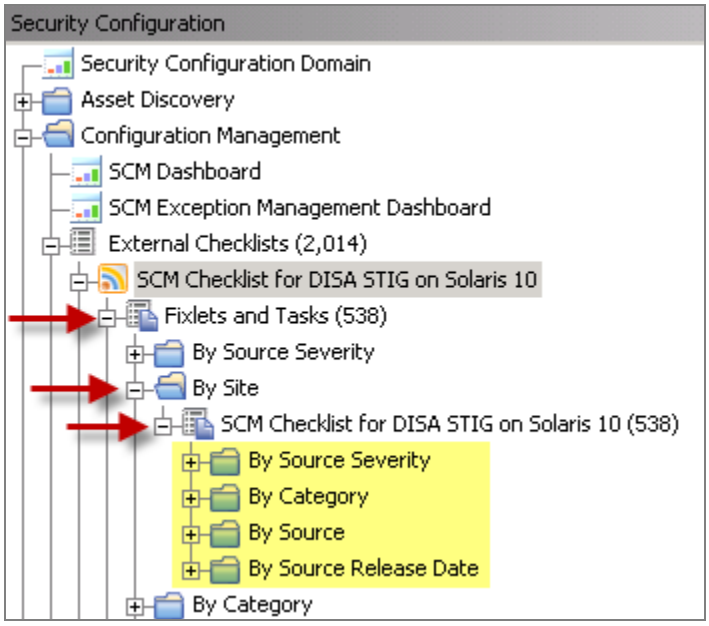
Configuration Management content is organized with dashboards in the top of the navigation tree, and below that you will find two primary "nodes" – *External Checklists* and *SCAP Tools*.



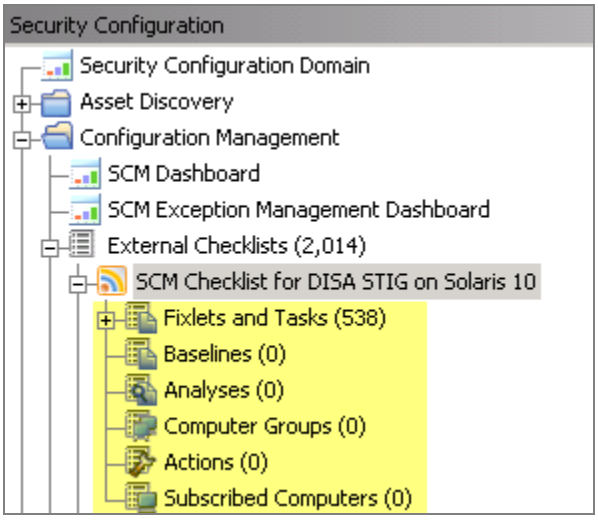
Each node expands to reveal additional content, including sub-nodes.



Some nodes, including External Checklists, expand to reveal additional levels of content, as shown below:



Each of the SCM Checklist for DISA STIG sub-nodes contain the same content organization: *Fixlets and Tasks, Baselines, Analyses, Computer Groups, Actions,* and *Subscribed Computers*.

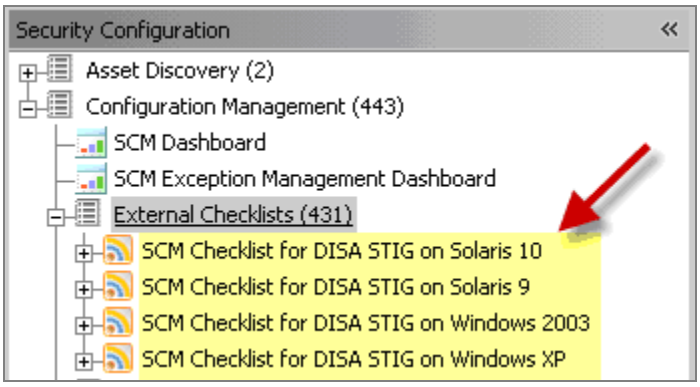


Fixlet Controls

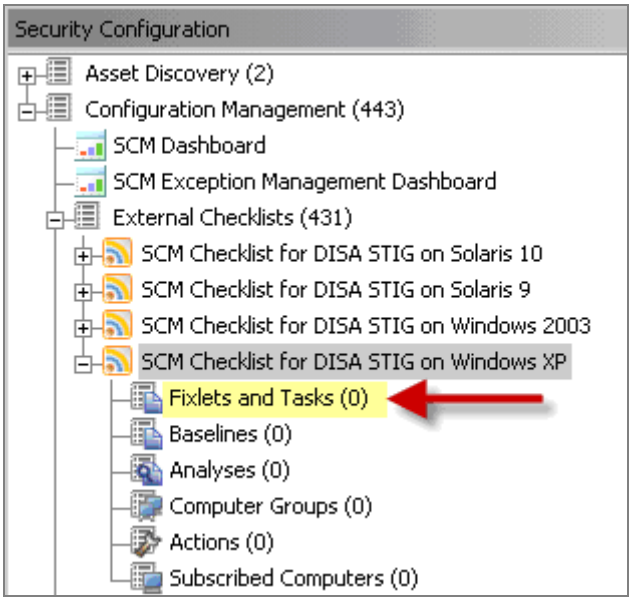
The Fixlet controls in SCM sites are designed to assess an endpoint against the desired configuration standard. A Fixlet message becomes relevant when a client computer is found to be out of compliance with a configuration standard. By viewing the SCM Fixlet messages within the BigFix Console, you can quickly identify non-compliant computers and the corresponding standards.

To start using the SCM checklists and other controls, obtain a masthead for the appropriate SCM site and open it within the BigFix Console. This will immediately initiate a download of the latest content. Once you have gathered the entire Fixlet library, follow the steps below to view the controls:

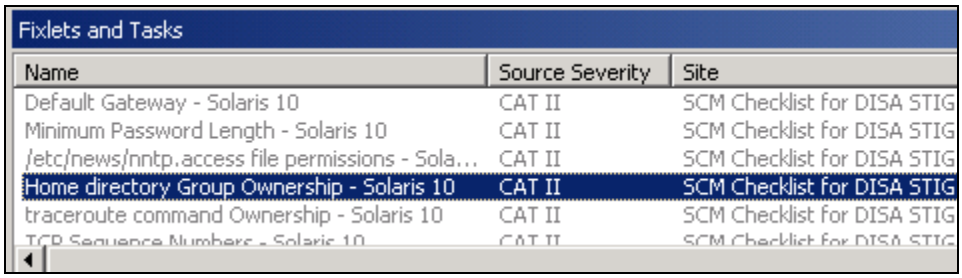
1. Select an SCM checklist from the navigation tree.



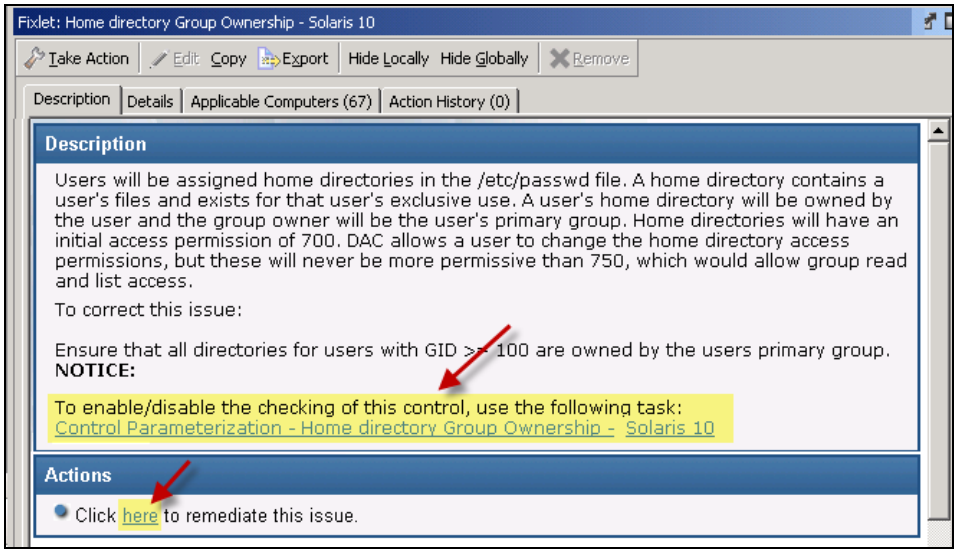
2. Choose one of the existing checklists and click the corresponding "+" to display the available content. Click *Fixlets and Tasks.*



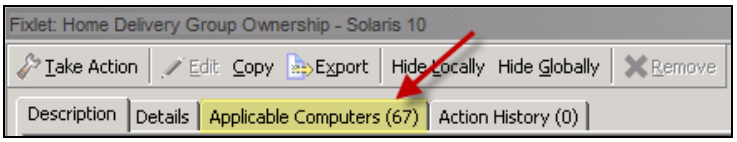
3. Select a Fixlet from the displayed list and double-click it. This will display the Fixlet in the work area below.



4. The Fixlet window typically contains a description of the control, links to customize the configuration setting, and a related Action that enables you to remediate one or more systems to the expected configuration value.



The Fixlet message will generally be applicable to a subset of endpoints on your network. The size of that subset is shown in the "Applicable Computers" tab in the top of the work area window.



5. To customize the parameters of the control, click the link at the bottom of the description. This feature allows you to change the parameter that determines whether or not a device is in compliance.

Note: UNIX controls also provide custom parameterization, but through a different mechanism. For more information on this, review the *SCM Guide to Customizing UNIX and Windows Benchmarks* document listed on the BigFix support site.

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

   This opens the Take Action dialog, which allows you to target the computers you wish to remediate. For more information on the Take Action dialog, see the BigFix Console Operator's Guide.

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

On either platform, applying this remediation value brings the client computer into compliance with that specified control. Once every affected computer has been remediated, this particular Fixlet message will disappear from the relevant Fixlet list. If any computer ever falls out of compliance or if non-compliant computers are added to your network, the Fixlet control will instantly become relevant again and will, in turn, re-appear in the relevant Fixlet list.

The SCM Dashboard collects statistics based on the status of these Fixlet messages, letting you quickly see which computers are compliant for any given control. (Dashboards are addressed in greater detail in the Dashboards section of this document.)

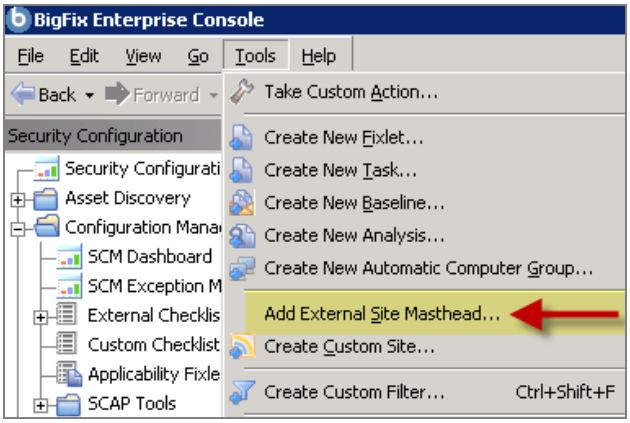
Subscribing Clients to SCM Sites

When deploying an SCM benchmark (checklist), special consideration should be given to the selection of configuration settings that are implemented on a given system. In many cases, organizations define a single benchmark for a *class* or *type* of systems and apply that benchmark for both assessment and remediation. SCM benchmarks should be subscribed to *only* the systems that should be evaluating the configuration settings defined within the site. This will ensure that the reporting dashboard only reports on the configuration settings that you want to be evaluated on those systems. Not subscribing the sites may lead to a distortion in the reporting dashboard.

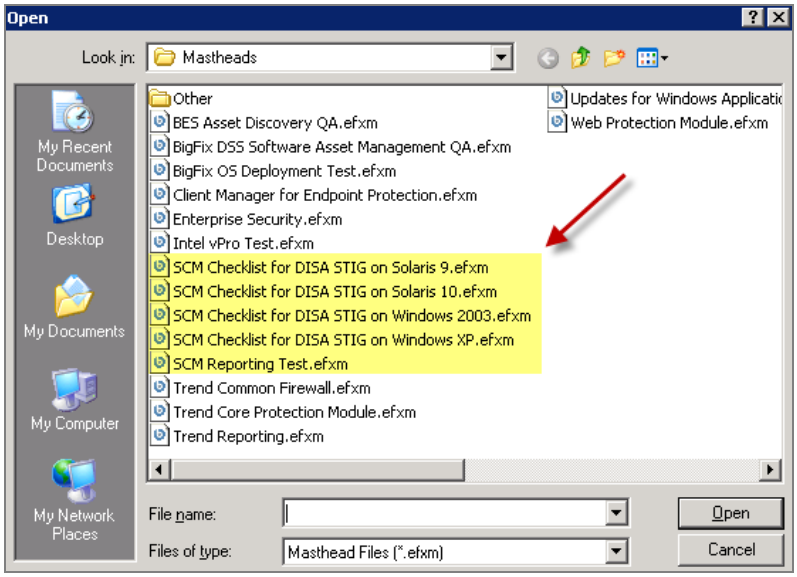
When you subscribe to a Fixlet site, the Console distributes the sites to all BigFix Clients by default.

To properly target your Clients, follow the steps below:

1. From the BigFix Console, click the *Tools* pull-down menu and select *Add External Site Masthead*.

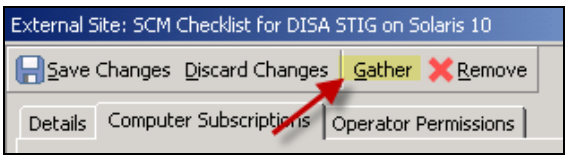


2. Browse to locate the desired masthead file, then click *Open.* Select a security site from the list that is targeted to a specific OS, such as the *SCM Checklist for DISA STIG on Windows 2003*.

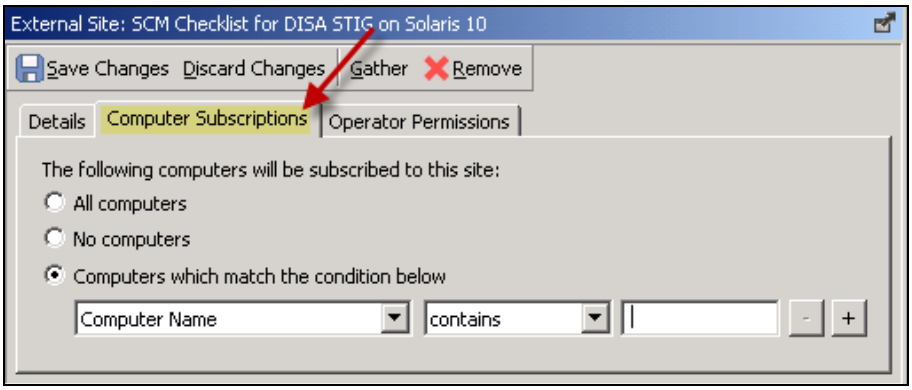


3. Click *Yes* to add the site, enter your Private Key Password, then click *OK*..

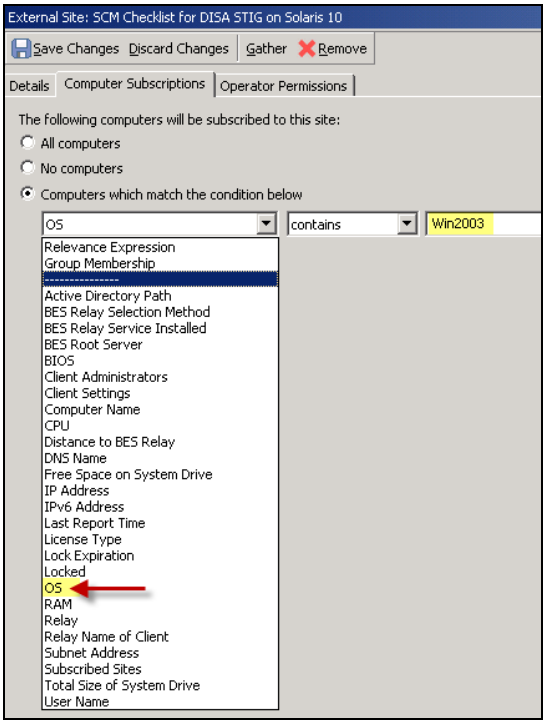
4. At the *External Site* dialog that displays, click *Gather* to gather the site. This will send the Gather request to the BES server. The BigFix Server will begin the gathering process, during which time tasks and analyses will be gathered from the central BigFix Hosted Content Server.



5. Click the *Computer Subscriptions* tab. This will allow you to set parameters for the computers that will be subscribed to this site.



6. Click the *Computers which match the condition below* button and review the dropdown list to select filter criteria.



7. From this dialog, you need to distinguish the group of computers you wish to target. For this example, select *OS* from the pull-down property list, then enter *Win2003* in the property value box. This will only subscribe Win2003 OS computers to this particular site. Follow this procedure with each site to ensure that only the appropriate computers are subscribed to each out-of-the-box SCM site.

Follow this procedure with each site to ensure that only the appropriate computers are subscribed to each out-of-the-box SCM site.

See the table below for group definitions for other operating systems:

Operating System	String
Windows XP	WinXP
Windows Vista	WinVista
Windows 2003	Win2003
Sun Solaris 10	SunOS 5.10
Sun Solaris 9	SunOS 5.9
Sun Solaris 8	SunOS 5.8
IBM AIX 5.1	AIX 5.1
IBM AIX 5.2	AIX 5.2
IBM AIX 5.3	AIX 5.3
HP-UX 11.0	HP-UX B.11.00
HP-UX 11.11	HP-UX B.11.11
HP-UX 11.23	HP-UX B.11.23
Red Hat Enterprise Linux 3	Linux Red Hat Enterprise AS 3
	Linux Red Hat Enterprise ES 3
	Linux Red Hat Enterprise WS 3
Red Hat Enterprise Linux 4	Linux Red Hat Enterprise AS 4
	Linux Red Hat Enterprise ES 4
	Linux Red Hat Enterprise WS 4
Red Hat Enterprise Linux 5	Linux Red Hat Enterprise AS 5
	Linux Red Hat Enterprise ES 5
	Linux Red Hat Enterprise WS 5

This is the basic procedure for viewing and using an SCM benchmark on all supported platforms. However, there are differences between the Windows and UNIX platforms and how to set parameters. For detailed information on setting Windows and UNIX parameters, see the *SCM Guide to Configuring Windows and UNIX Benchmarks* or the relevant *Parameter Guides* on the BigFix support website.

Creating and Managing Custom Sites

The ability to customize SCM parameters and exclude specific computers from an analysis gives you a great deal of control over your security posture. However, you can go even farther by creating custom sites and repurposing SCM benchmarks to fine-tune your deployment. Custom sites allow you to target specific sets of computers with tailored content using the subscription mechanism. This allows highly accurate statistics to be created with finer granularity. To create your own policy with custom sites, follow the four-step process below.

Here's what you're about to do:

***Step 1*: Create** a custom site

***Step 2*: Copy** the desired Fixlet messages into the custom site

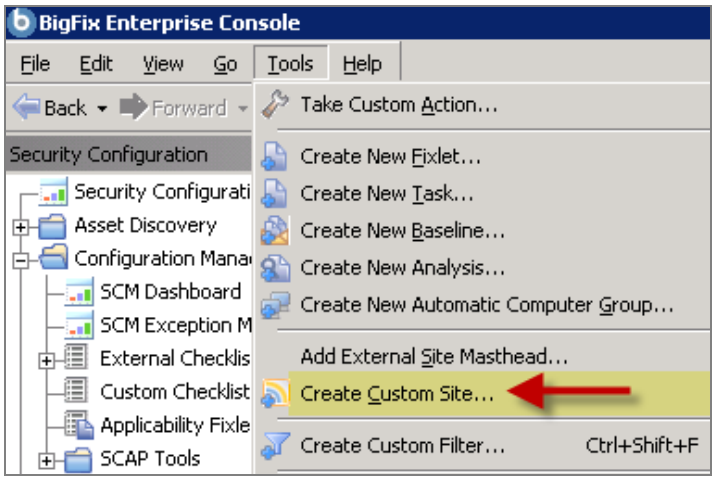
***Step 3*: Customize** Fixlet messages using parameters and exceptions

***Step 4*: Subscribe** the proper clients to the custom site

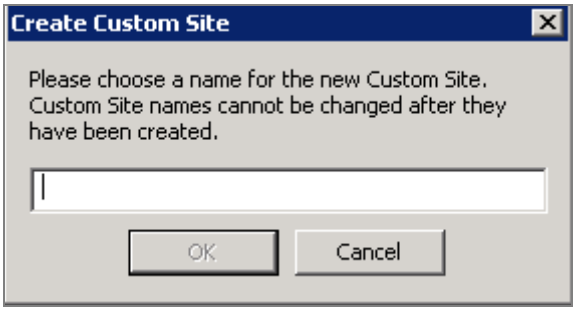
Creating Custom Sites

Grouping Fixlet content into custom sites is a powerful and convenient functionality. Once you have defined a custom site, you can also incorporate security-based Fixlet controls from other sites. For instance, BigFix Patches for Windows may address certain issues that you want to include in a high-level grouping of security items. This section describes how to set up a custom site, set permissions on it and populate it with customized Fixlet messages.

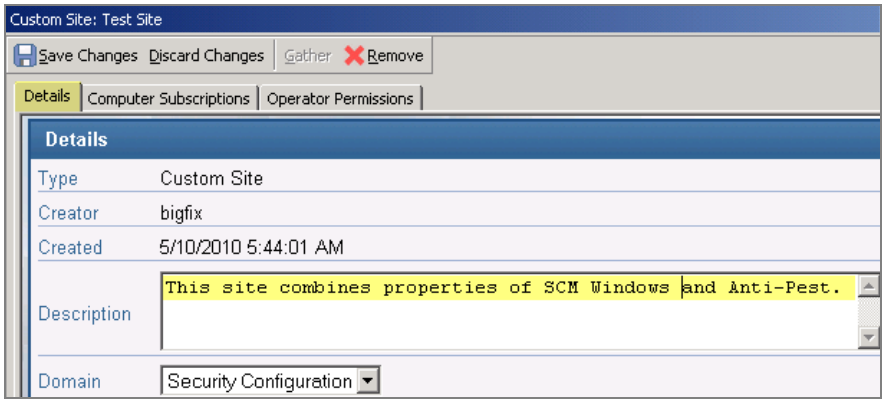
1. From the Tools menu, select *Create Custom Site*.



2. In the dialog box that appears, enter the name of your site. Click *OK*.



3. When the Custom Site dialog opens, enter a description of your site in the text box under the Details tab.

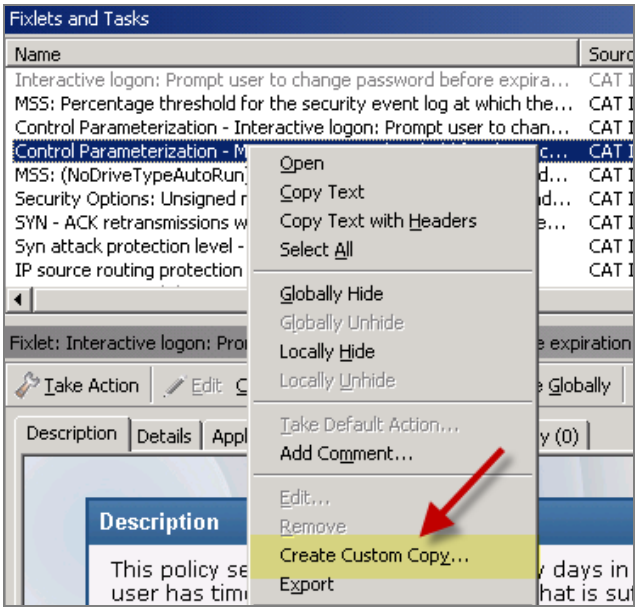


4. Click on the other tabs to subscribe computers and set permissions, then click *OK*.

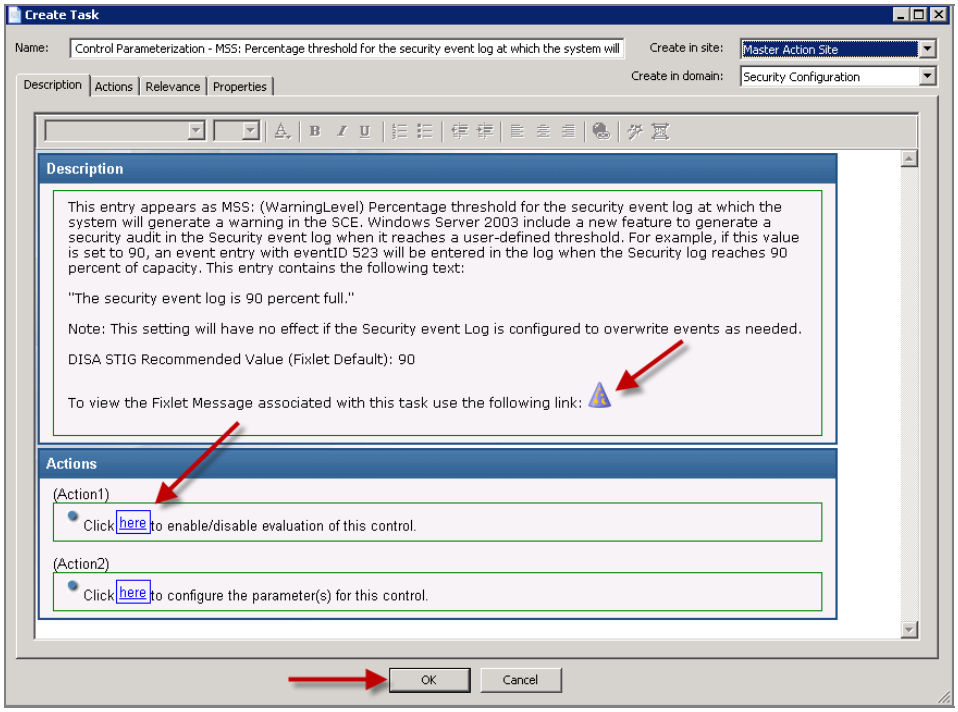
Copying and Customizing Content

Now that you have a custom site, you need to populate it with Fixlet messages and Tasks. To add content from SCM sites either one at a time or as a batch, follow the steps below:

1. Right-click any item in the Fixlet list and select *Create Custom Copy*.



2. When the Create Task dialog opens, click as indicated in the Actions box to configure parameters for this control.



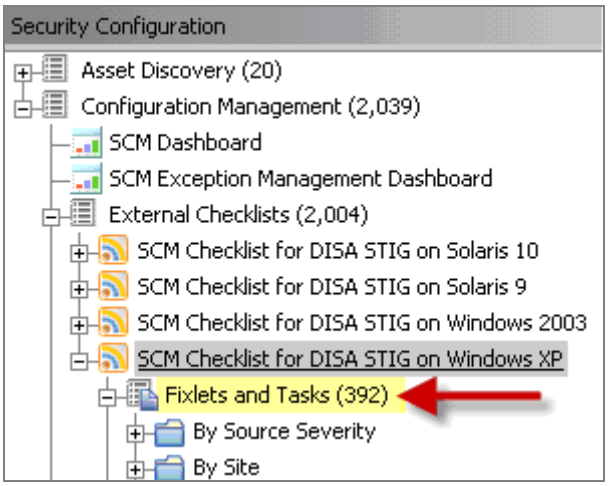
3. Click *OK* and enter your Private Key Password. Repeat this process for each Fixlet message you wish to add to your custom site.

To display non-SCM content in the SCM Dashboards:

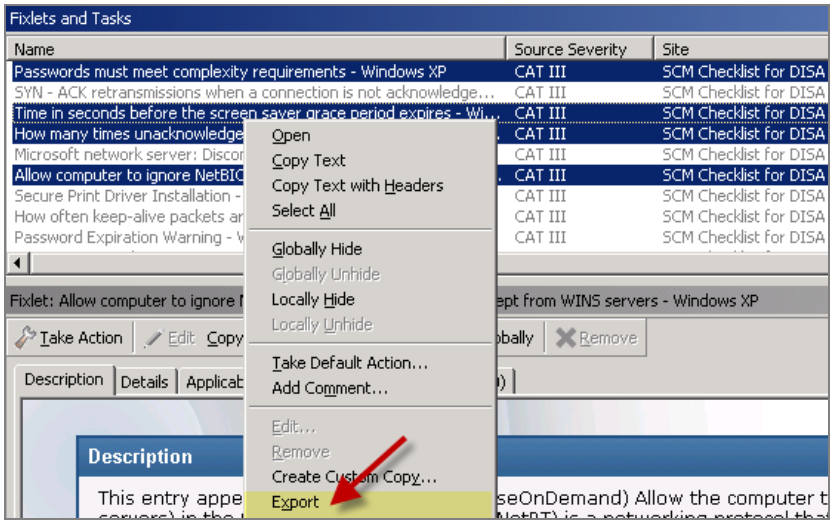
SCM content is displayed within the SCM and Exception Management dashboards. In order to make non-SCM content display in the dashboards, you will add the Name/Value pairs of information below into the Fixlets to make the dashboards aware of the content. By adding this information, the dashboards will use and display these new controls.

To create new SCM controls or to make other controls seen by the dashboards, modify the Fixlets as follows:

1. Select one of the checklist folders from the SCM navigation tree and click the "+" to display the sub-folders. Click *Fixlets and Tasks.*



2. Select the Fixlet messages or Tasks you would like to move, and then right-click the set. From the right-click menu, click *Export*.



3. At the Save As dialog, select a name for the file and click *Save.*
4. Open the exported .bes file using a text editor. (It is an XML document.)
5. On the line below every <SourceSeverity></SourceSeverity> tag, add a section as shown below:

```
<MIMEField>
<Name>x-fixlet-scm-control</Name>
<Value>PlaceAnyValueHere</Value>
</MIMEField>
<MIMEField>
<Name>x-fixlet-scm-os</Name>
<Value>Windows XP</Value>
</MIMEField>
```

In addition to these MIME fields, the Category field on each control can be updated from within the BigFix Console to allow you to change the categorization of the control. The defined category will be displayed within the SCM Dashboard for each control. If you don't populate these fields, the SCM Dashboard will generate an error message when trying to use it.

> **Note:** When creating a new custom Fixlet, be sure to fill out the *category, download size*, and *source ID* fields on the property tab of the Fixlet from within the Console. These fields are used as well by the SCM Dashboard.

6. After editing the XML to add the tags above, save the .bes file and double-click to import it into the BigFix Console.
7. From the Import Content dialog that appears, select your custom site from the *Create in site* pull-down menu on the right. Click *OK* and enter your Private Key Password.

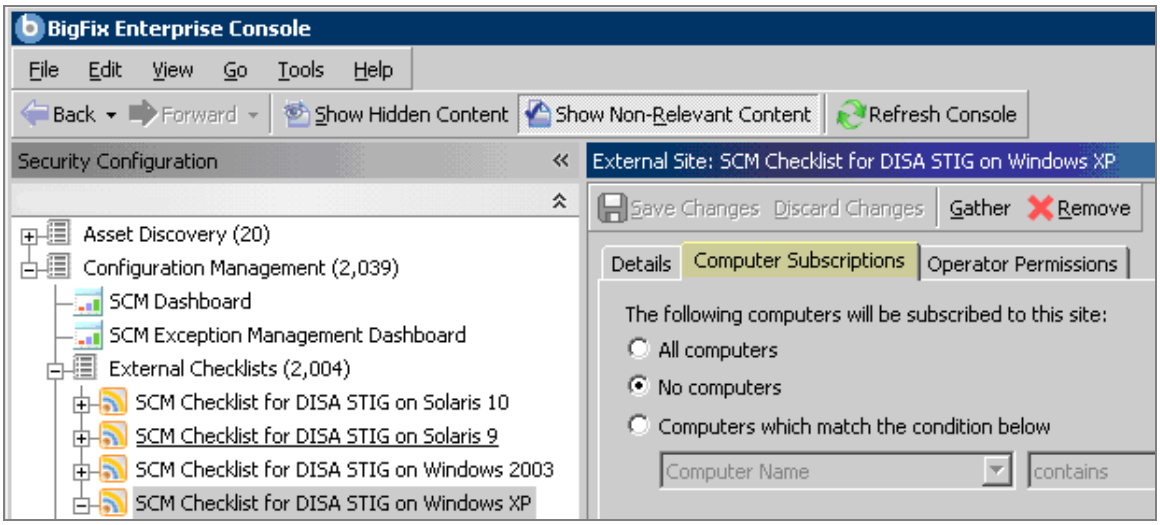
Subscribing Computers to your Custom Site

Now that you have created your custom site, you need to subscribe computers to it. Remember that the proper collection of statistics depends on targeting the content to the appropriate computers. Make sure that Windows computers are subscribed to Windows content only, and follow this same rule for UNIX computers.

You can subscribe computers to your site by subscribing either specific computers or properties.

Subscribing Specific Computers

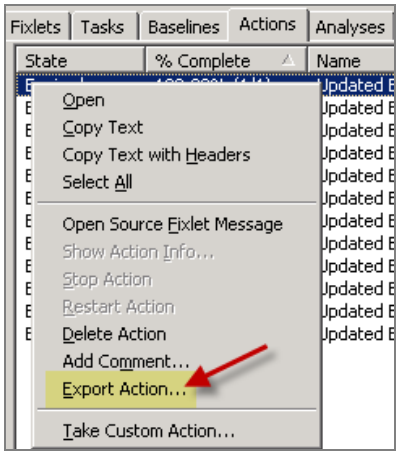
1. Click an SCM checklist from the navigation tree. An *External Site* dialog will display on the right.
2. Click the *Computer Subscriptions* tab of the dialog to select computers to subscribe to this site. Click either *All computers* or *Computers which match the condition below.*



Subscribing by Properties

Targeting computers by their properties is a highly efficient technique for controlling site subscriptions. Through this functionality, a computer's OS (or other characteristic) will be examined and automatically subscribed to the appropriate site whenever a computer is added.

1. Using the steps outlined above, subscribe a computer to the desired site. This creates an Action that you can find by clicking the Actions folder under the *All Security Configuration* node in the navigation tree.
2. From the list of Actions, locate the Action you just created from the List Panel, and right-click on it. Select *Export Action* from the right-click list.



3. At the Save As dialog, select a name and location to save the exported Action as a .bes file.
4. From the Windows file system, locate the exported Action file that you just saved, and double-click it. This opens the Take Action dialog.

Set your desired parameters for this export action in the Take Action dialog, then click *OK* and enter your Private Key Password.

Part 3

Dashboards

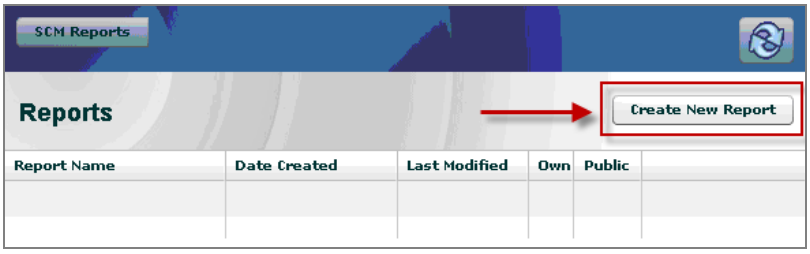
SCM offers two dashboards, which provide a convenient way to view and manage the information in your deployment. The sections below will outline how to use the SCM Dashboard and the Exceptions Management dashboard.

SCM Dashboard

The SCM Dashboard provides a detailed, up-to-date, graphic overview of the current security configuration of your entire network. It allows you to filter and customize the information you want to view and set parameters for how it displays. The Dashboard can then be saved as a custom report or printed.

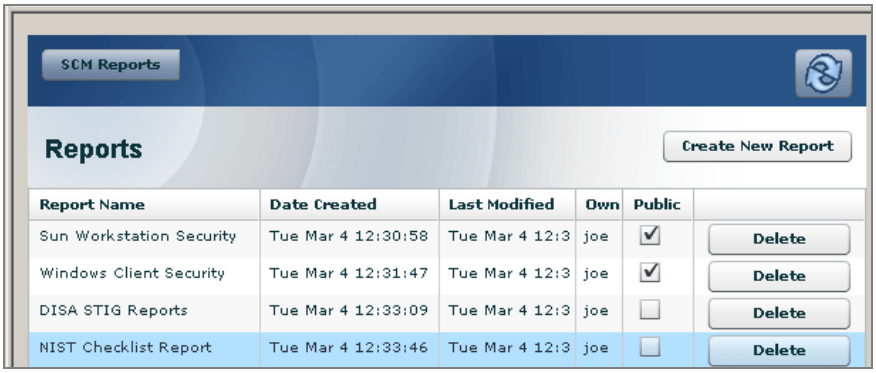
How it Works

Under the Dashboards pull-down menu, select Security Configuration Management. The SCM Reports window will open, which will display any of your saved reports. If this is the first time you have viewed the SCM Dashboard, the window will be empty. Click *Create New Report*.

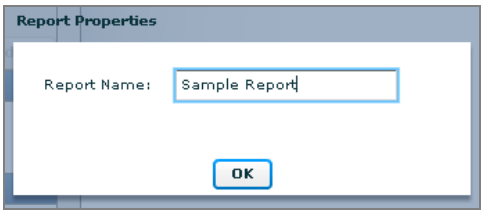


You can create separate reports that correspond to different standards, or target subsets of machines that have unique compliance requirements. At any point, you can click the refresh button at the top right of the screen to ensure that you are viewing the most recent data.

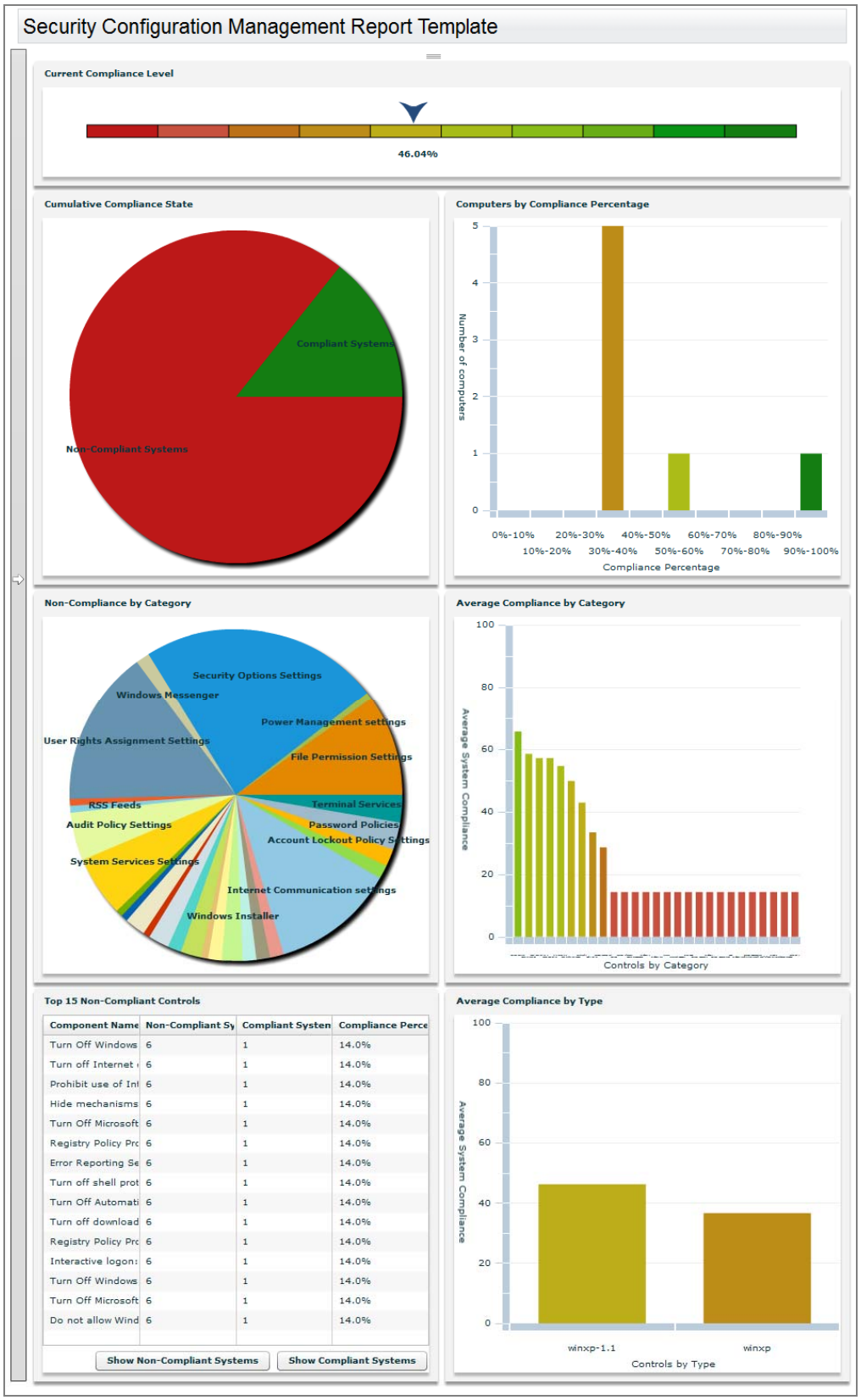
This Report listing screen allows you to create a new report, load existing reports, designate reports as public or private, or delete reports.



Simply click a report to view it. When you create a new report, you will be prompted to provide a name.



Once the name is provided, the report and filter bar opens. (No data has been defined yet.)



The SCM Dashboard

The typical workflow will take you through these basic steps:

> **Note:** There are several required filters that need to be defined before data is available. See the Filter Panel section below for more information.

1. Select the desired SCM site from the Control Site section of the Filter Panel.
2. Choose the desired set of controls from the Control List.
3. Select the operating systems you want to evaluate from the Control OS section of the Filter Panel.
4. Select the desired Control Types to monitor.
5. View the resultant charts.
6. Drill down into the charts for detailed information.

The sections below will describe each individual panel.

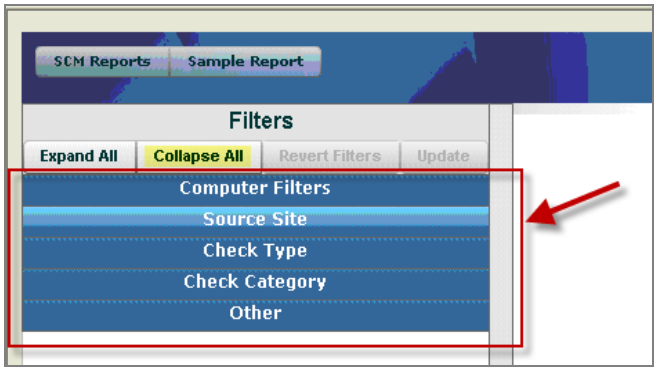
Filter Panel

An individual SCM report can be considered as a collection of saved filters. By carefully crafting your filters, you can design tightly targeted reports on hundreds of aspects of your network. The left side of the Dashboard contains a filter panel that lets you select or deselect specific Control Sites, operating systems, and types. You can click the checkboxes next to each item or click the *All* or *None* links to create comprehensive changes. The filter panel can be expanded or collapsed. When expanded, it displays each component. When collapsed, a small bar is available to re-open the panel.

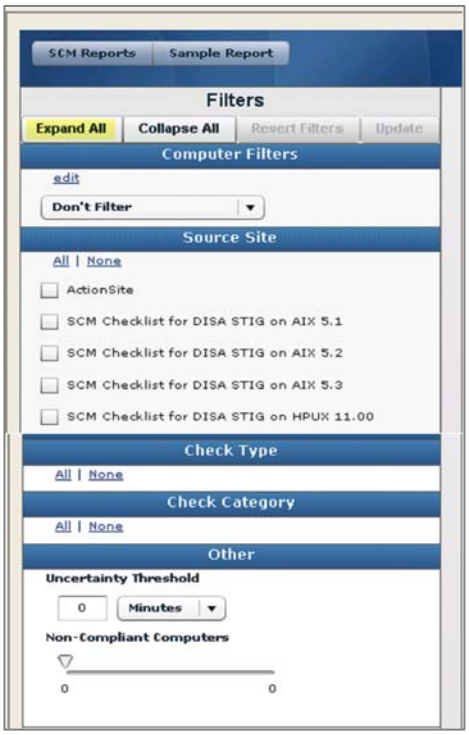
Filter sets are positioned in the Dashboard as follows:

- Computer Filters – specifies a group of computers to report against
- Source site – specifies the benchmark (checklist)
- Check type – specifies the operating systems
- Check category – specifies the control categories
- Other – specifies additional filter options

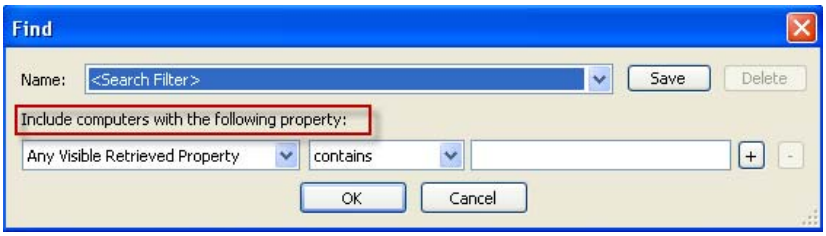
Collapsed View



Expanded View

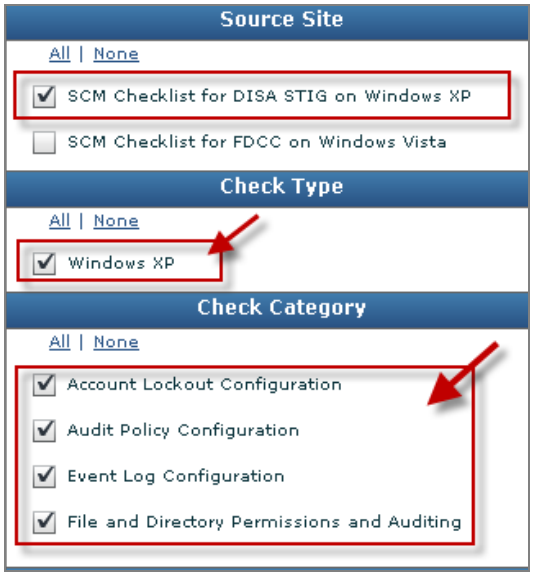


The **Computer Filters** option allows you to specify systems to include based on designated computer properties. Click the *Edit* link to display the box below, which allows you to set parameters for the filter. When finished, click *Save* and then click *OK.*



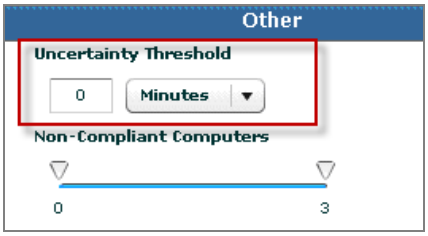
The **Source Site** filter lets you select the specific SCM sites to include in the report. This list includes any custom sites you may have created that contain content tagged as an SCM control. This means that any site with at least one SCM control will be available for reporting. Similarly, any content not tagged as an SCM control will not be displayed, even if the site is selected.

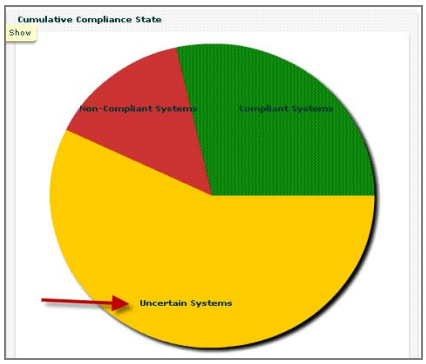
By clicking an available checkbox in the **Source Site** filter, the accompanying **Check Type** and **Check Category** filter boxes will automatically expand below it, allowing you to filter content by operating system and by types of controls.



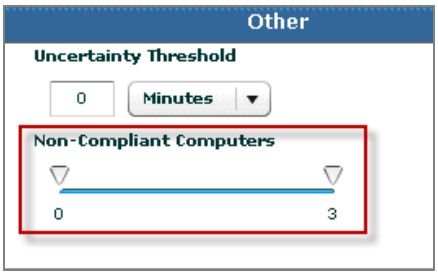
The **Other Filters** box provides two additional ways to filter content: *Uncertainty Threshold* and *Non-Compliant Computers.*

The **Uncertainty Threshold** filter is used to define a threshold based on time, where the user may not have confidence in the results that are returned for a given benchmark. The value specified indicates the period of time allowed before the Dashboard considers the control to be "uncertain" versus compliant or non-compliant. Any system that has not "checked in" with BigFix will register in the Dashboard as an "uncertain" system.

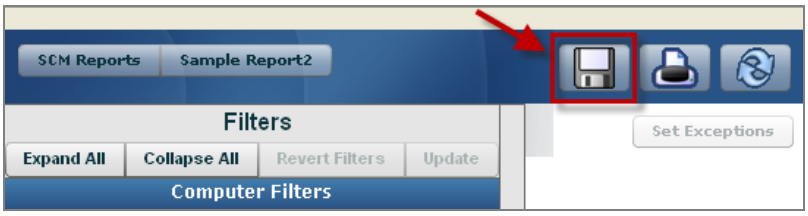




Non-Compliant Computers allows you to filter out controls based on the number of endpoints that are non-compliant to the control.

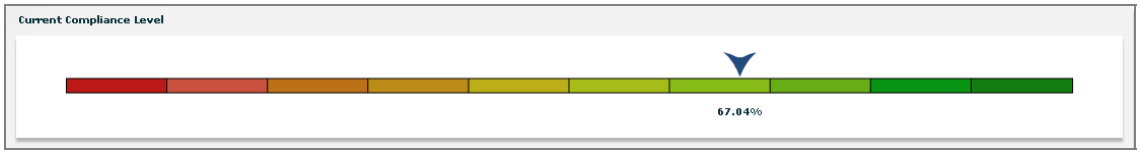


Once you have created a filter, click the *Save* icon located in the top right of the SCM Dashboard. This will allow you to open that saved report again with any saved viewing preferences that you set while creating the filter.



Current Compliance Level

Immediately below the Control List is a summary graphic showing the overall compliance level for the specified set of controls and computers. It distills all of the compliance information about the designated subset of your deployment into a single number.



This composite number is an average of the individual scores from all contributing computers.

> **Note:** Take special care in subscribing sites properly. If a computer is subscribed to a non-relevant site (such as a Windows machine subscribed to a Solaris site), this can skew the results by giving you a much higher score on all measures. This applies to all of the compliance graphs in the SCM Dashboard.

Graphs

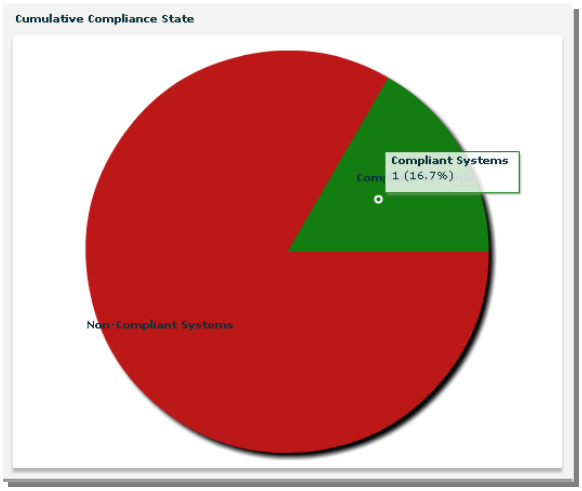
Below the overall compliance bar are several graphic displays. In each of these, roll your mouse over the constituent elements to display a window with numeric detail. To drill down into the constituent data, click on the element. A table replaces the graphic with a detailed breakdown of that particular element. To view the graph again, click *Return to Chart*. Each graph can summarize an enormous amount of data, allowing you to gauge the compliance of your entire global enterprise at a glance.

Graphs enable you to do the following:

- View the results of the assessment
- Drill into a specific subset of information (e.g. non-compliant systems)
- View actual details of each computer making up the result (this is achieved by drilling into the tabular details, then drilling one layer deeper into the console)

Below is a description of each chart.

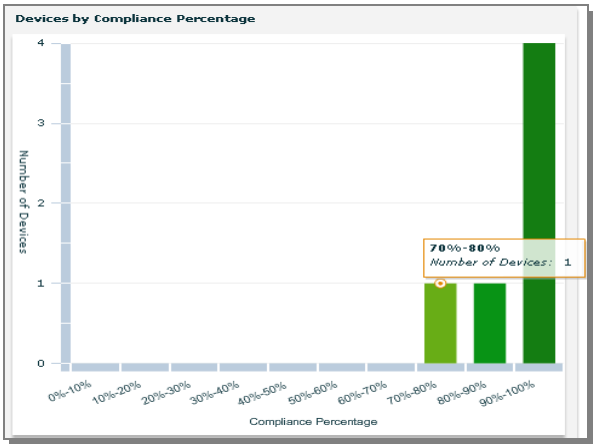
Cumulative Compliance State



This chart displays the relative numbers of compliant and non-compliant computers, providing an instant view of the security of your enterprise. A compliant computer is defined as a machine that is 100% compliant. If even one security issue is unaddressed, the machine falls into the non-compliant category. Click either of the two pie sections to see the individual computers. The green section shows secured machines, while the red section provides a detailed look at each computer, identifying the outstanding compliance issues for each.

To view the computers in the standard computer group window, click *View as Group*. To return to the Dashboard, select *Security Configuration Management* from the Window menu.

Devices by Compliance Percentage

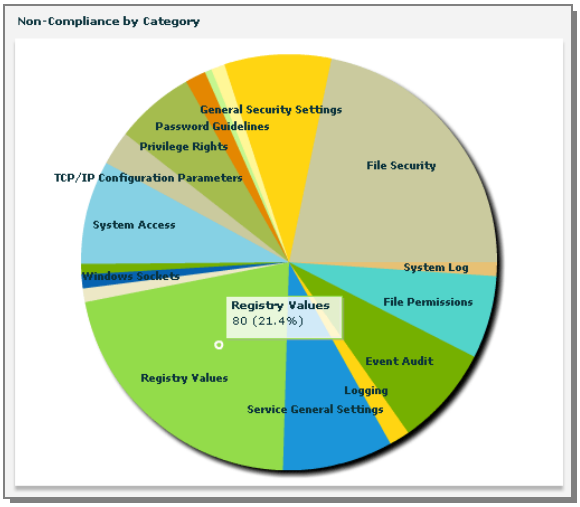


This bar chart groups computers and devices into 10% slots, showing the number of computers in each slot. For example, all computers that have satisfied 60-69% of their compliance issues will be added together and assigned to that group.

Mouse-over any bar to see the actual number of devices in each slot. Click on the bar to bring up a detailed table of the contributing devices. For each device, you can see the number of security controls that have been successfully applied and those that are still outstanding.

To list the devices in a typical group view, click *View as Group*. To return to the Dashboard, select *Security Configuration Management* from the Window menu.

Non-compliance by Category

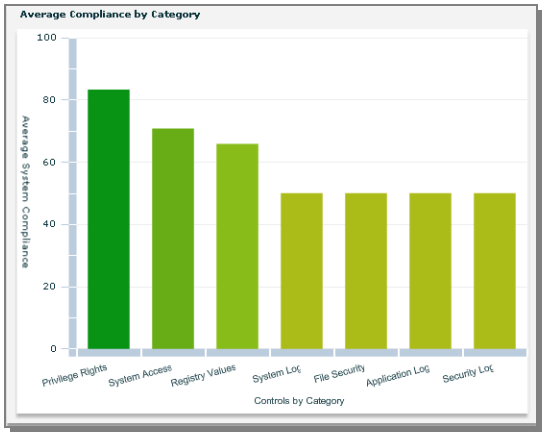


This Pie Chart displays categories of non-compliant controls, allowing you visibility into the most critical issues in your enterprise.

Mouse-over any slice of the pie to see a count of the controls in each category. Click on any category slice to bring up a list of all the controls in that particular category. You can sort this list by clicking on a header, or click on any of the links to view the associated control. Select a control

or a group of controls, and then click one of the two buttons at the bottom of the list to view the applicable non-compliant computers. This produces a standard computer group list (you can also select a subset of the listed computers by Ctrl and Shift-clicking). To return to the Dashboard, select *Security Configuration Management* from the Window menu.

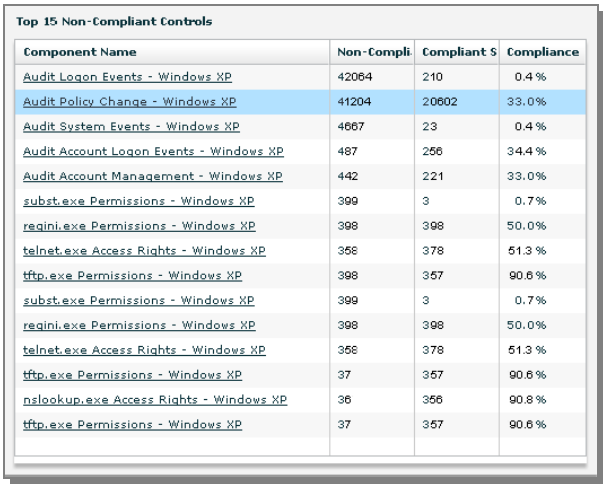
Average Compliance by Category



This graph displays the average percentage of managed computers that are compliant within each security category. Categories that are “checked” in the filter list will be displayed in the graph. To limit the number of categories, uncheck some of them in the Filter list. Mouse-over any bar to see the actual numeric percentage for each category. Click on a specific bar to bring up a detailed list of the controls in the selected category, along with the total number of subscribed computers and the subset of non-compliant computers. The percentage is calculated through the non-compliant computers in the category and the total number of affected computers.

Two buttons at the bottom of the panel allow you to view a list of affected and non-compliant computers for any given selection of controls. Click on a specific control to view the Fixlet message in its own window.

Top 15 Non-Compliant Controls



Top 15 Non-Compliant Controls

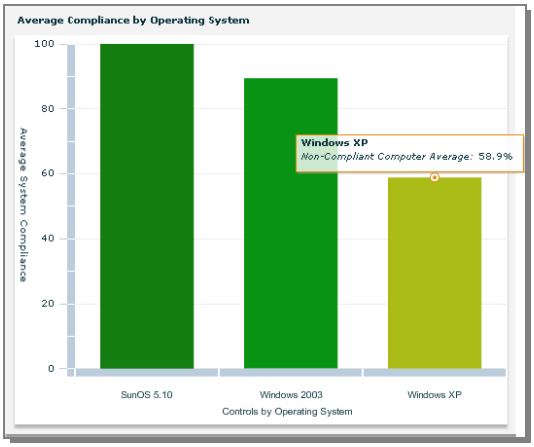
Component Name	Non-Compli	Compliant S	Compliance
Audit Logon Events - Windows XP	42064	210	0.4 %
Audit Policy Change - Windows XP	41204	20602	33.0%
Audit System Events - Windows XP	4667	23	0.4 %
Audit Account Logon Events - Windows XP	487	256	34.4 %
Audit Account Management - Windows XP	442	221	33.0%
subst.exe Permissions - Windows XP	399	3	0.7%
regini.exe Permissions - Windows XP	398	398	50.0%
telnet.exe Access Rights - Windows XP	358	378	51.3 %
tftp.exe Permissions - Windows XP	398	357	90.6 %
subst.exe Permissions - Windows XP	399	3	0.7%
regini.exe Permissions - Windows XP	398	398	50.0%
telnet.exe Access Rights - Windows XP	358	378	51.3 %
tftp.exe Permissions - Windows XP	37	357	90.6 %
nslookup.exe Access Rights - Windows XP	36	356	90.8 %
tftp.exe Permissions - Windows XP	37	357	90.6 %

The **Top 15 Non-Compliant Controls** is an abbreviated list of only the top 15 security controls. This list is ranked by the absolute number of non-compliant computers, not by percentage of compliance. As with the other control lists, you may sort this list or click the link to view the associated Fixlet message.

At the bottom of the list are two buttons. As with the other panels, you can click them to view the compliant and non-compliant computers in the standard computer group window.

A computer must be compliant with every control in your selection to be considered compliant. If it is out of compliance with any control in your selection, it is considered non-compliant. If no controls have been specifically selected, all 15 controls are included in the consideration. To return to the Dashboard, select *Security Configuration Management* from the Window menu.

Average Compliance by Operating System



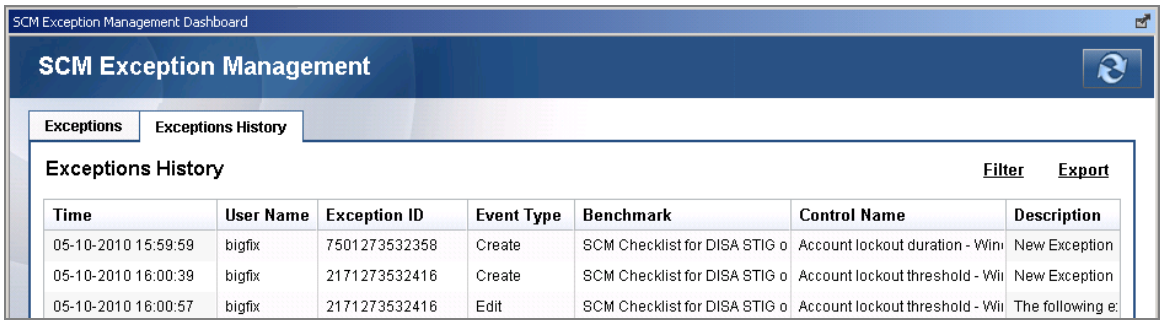
This panel displays the percentage compliance figures for all of the operating systems you are currently monitoring. Mouse-over the bar associated with a particular OS to get an accurate numerical figure. Click on one to bring up a detailed list of controls. This list can be sorted by clicking on the relevant header and individual items can be selected to view the associated control. The buttons at the bottom can be used to view the compliant and non-compliant computers in the standard computer group window. To return to the Dashboard, select Security Configuration Management from the Window menu.

Saving and Printing Dashboard Reports

Click the disk icon in the top right to save your report under the existing name. Each new report will become available to you whenever you run the Dashboard. Simply click SCM Reports from the button in the upper left of the window to bring up a list of saved reports.

Click on the printer symbol to print a copy of the report for your files. The printing routines will print out all graphics first. If you have “drilled down” to the data that underlies a chart, those tables will be printed last.

Exception Management Dashboard



Overview

The purpose of an “exception” is to select a rule that will designate a set of computers as “compliant” based on some common details. Exceptions provide a way for you to define criteria by which BigFix evaluates the compliance of your endpoints. Specifically, the Exception Management Dashboard allows you to define reporting level exclusions for specific controls for specific endpoints. Excluded controls are still evaluated for compliance on the endpoint, but SCM reports can be customized to display exceptions as their true value, or as always “compliant”.

Exceptions have 3 parts:

- **Setting** it in the dashboard
- **Viewing** how it appears in your reports
- **Monitoring** how it relates to all your other reports

The Exception Management dashboard allows you three primary actions for dealing with exceptions:

You can also filter exceptions to define specific parameters, and export exceptions to a CSV or HTML table.

How Do Exceptions Work?

Computer Rules

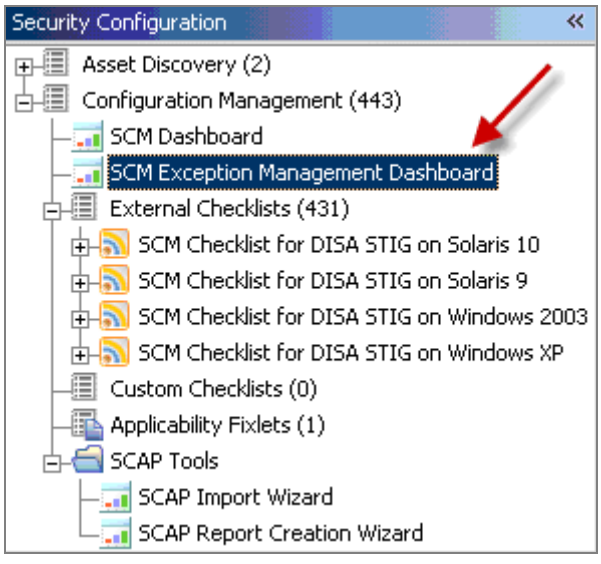
When you apply an exception to a set of computers, you are creating a computer "rule". Computer "rules" can be defined in 3 ways:

- *By Property*
- *By Computer Group*
- *By Name*

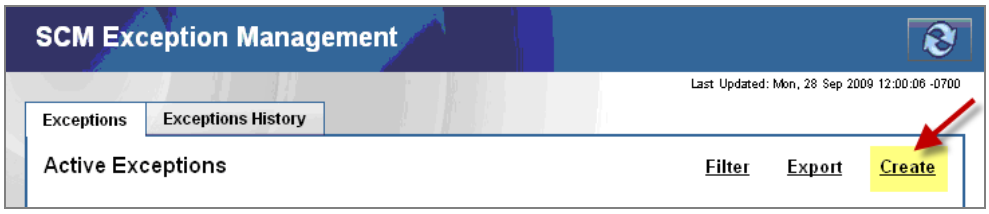
> **Note:** To maintain the most consistent results, only use the *By Name* definition to specify up to a few thousand computer names.

Setting an Exception

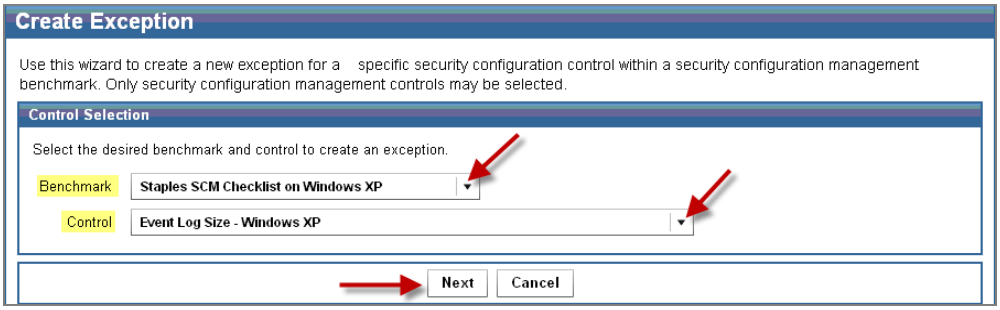
From the Configuration Management navigation tree, click *Exception Management Dashboard.*



Click *Create* in the top right of screen.



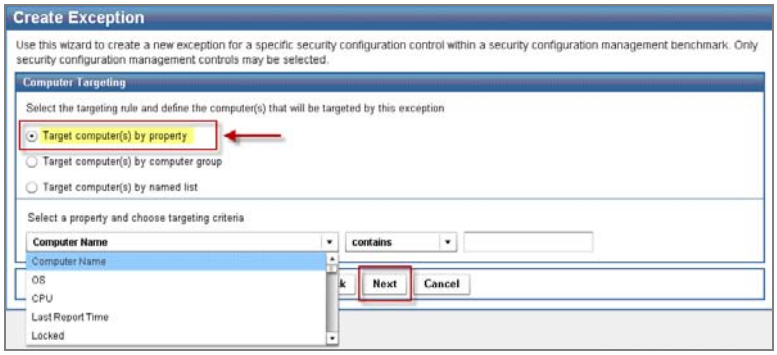
When the Create Exception Wizard opens, select a Benchmark and a Control from the available pull-down lists.



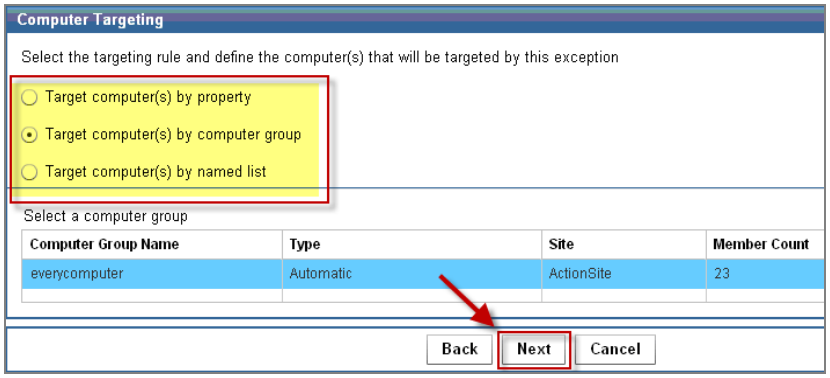
Note: You can only have one exception per Benchmark/Control combination.

Click *Next*. This will open the Computer Targeting window, where you will define the computers to be targeted by this exception. You can target computers in one of three ways:

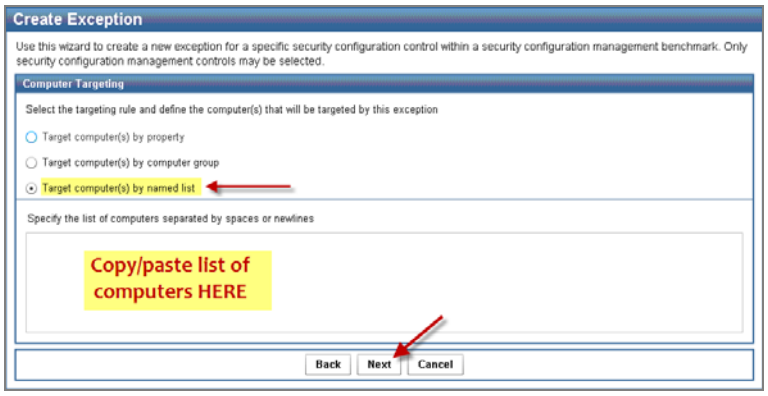
By Property:



By Computer Group:



By Named List:

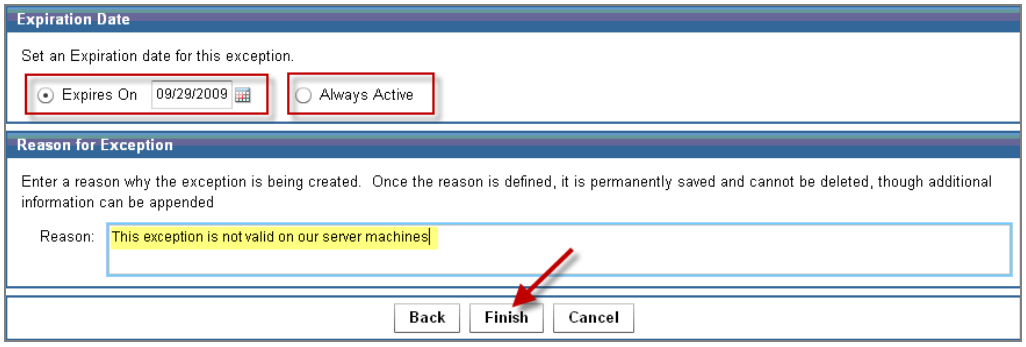


Select the *type* of rule you intend to create: (Property, Computer Group, or Name). Click *Next.*

> **Note:** Pay close attention to correct spelling and naming conventions while manually entering the names of computers. As a best practice, copy and paste a list of computers.

Click *Next*. This will open a new window for defining additional options. This window has two parts:

- **Expiration Date**: Define when you want the exception to expire – never (select *Always Active)* or on a specific date – (select *Expires On* and enter the date).
- **Reason for Exception**: Type a brief description of why you are setting this exception. Example: *I have defined this exception because workstations don't have a minimum password length.*

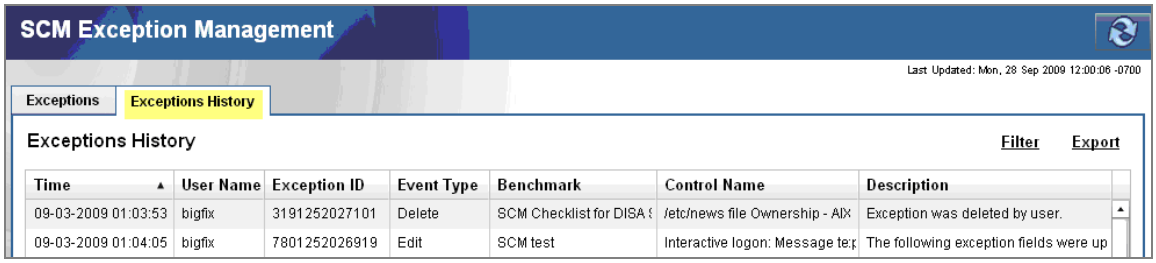


Note: The "reason" field is required in order to track changes to the exception. It must be at least 10 characters in length.

Click *Finish*. This will bring you to the *Active Exceptions Summary* page, where you should see the exception you just added. Click on an exception on the bottom to view details of it.

Exceptions History

The Exceptions History feature allows you to maintain an accurate change history by reconstructing a timeline of activity. Click the Exceptions History tab in the Exception Management dashboard.



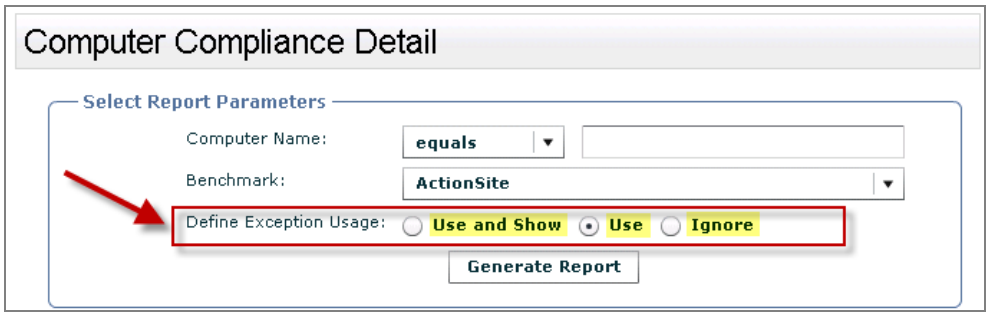
Now you have created an exception, and it has been logged as an exception event. To review your existing exceptions, click the *Active Exceptions* screen and select the desired exception. From the Active Exceptions screen, you can view, edit or delete the exception according to your system needs.

Exception Reports

There are 3 types of Exception reports, which are described in more detail in the Web Reports section of this document:

- Computer Compliance Detail
- Computer Compliance Summary
- Policy Compliance by Computer

In addition, there are 3 ways to use the exceptions you've set in each of the above reports: *Use and Show*, *Use*, and *Ignore*.



- **Use and Show** - Uses existing exceptions to determine compliance, and displays each exception
- **Use –** Uses any exceptions you've set to determine compliance (no display)
- **Ignore** – Ignores all exceptions before generating a report

Exception Dashboard Considerations

- Exception Management is an extension of all reporting. The only place you can set exceptions is in the Exception Management dashboard, but what you set in that dashboard can affect Web Reports and Dashboard reports. As a result, it is recommended to refresh after making any changes to the Exception Management dashboard.

  Note: The Security Configuration Management dashboard and the Security Configuration Management Report Template will not utilize exceptions. Check a future release of this product for this capability.

- Web Reports maintains its own database *refresh* cycles. This means that if you take an action in the Console, Web Reports will not display those changes immediately. By default, there is a 20 minute delay while Web Reports gathers new changes. You can set an option in Web Reports to reduce the delay time to 15 seconds.

Part 4

Web Reports

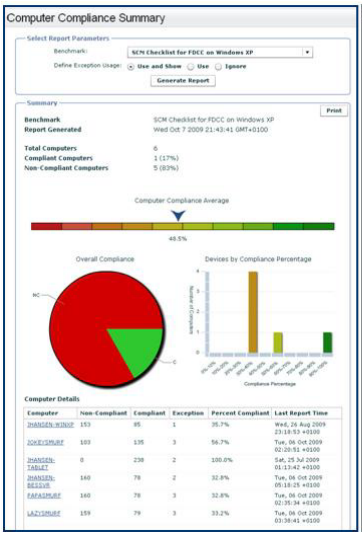
BigFix Web Reports is a web application that connects to one or more BigFix Enterprise databases to analyze the data gathered and provide a visual display in the form of reports. The SCM Reports capability uses the general functionality of the Web Reports application to provide information on the security configuration management of your enterprise. Information on your SCM deployment can be gathered from Web Reports via a left navigation bar, as well as a list of links on the top of the application: *Overview, Reports, Create, Schedule,* and *Email*.

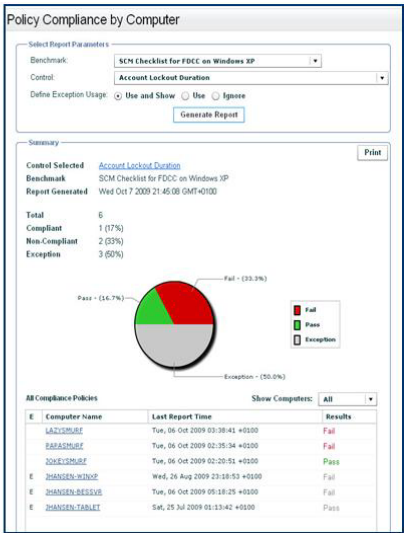
Note: Due to their enhanced graphic capabilities, SCM Reports cannot be emailed.

For more detailed information on how Web Reports works, review the BigFix Web Reports User's Guide on the BigFix support site.

SCM Reports can be made private or public. Public reports allow any authorized operator to conveniently view the information from any browser, anywhere in the world. Depending on your operator status, you have various permissions to alter and view both public and private reports. These rules are the same as for all other Web Reports.

SCM offers three new reports that can identify your compliance with their security baselines.

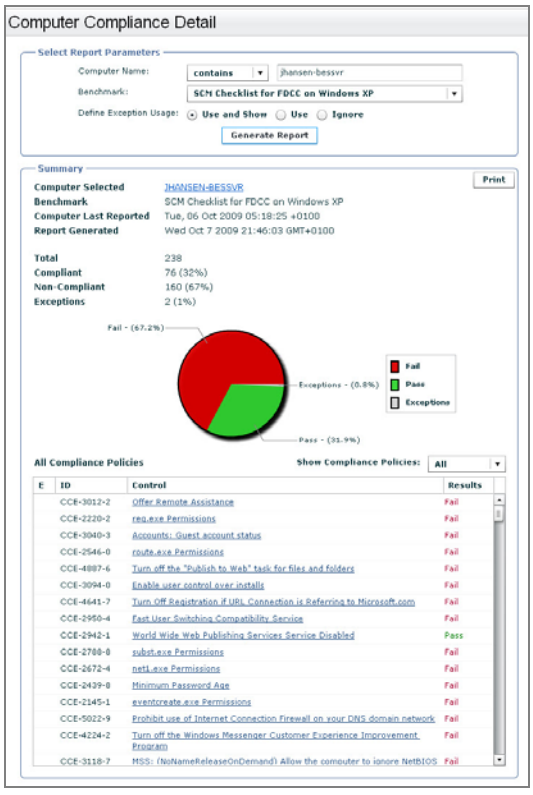




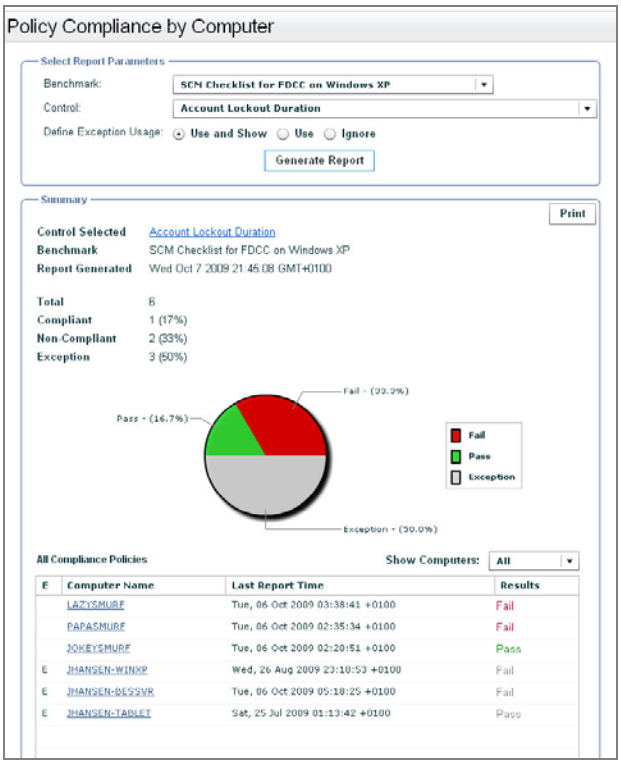
The reports are summarized as follows:

- ***Computer Compliance Summary*** - This report provides a summary view of the infrastructure as compared to a single configuration policy. The report includes a high level summary section that details the overall metrics associated with the configuration policy for all computers selected and provides a detailed break-down for each computer in the report.

- ***Computer Compliance Detail*** - This report provides a detailed compliance view of a single computer against a single standard. It will provide summary information on the overall compliance of that computer to the standard and provide the details for each individual configuration check indicating *pass* or *fail*.

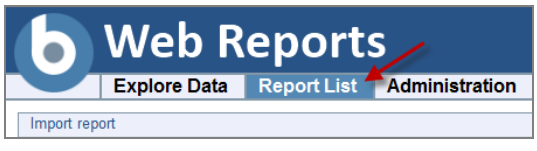


- ***Policy Compliance by Computer*** - This report provides a detailed view of a single policy (i.e. Fixlet) against all systems where that policy is being evaluated. The user can select the standard (i.e. site), choose the specific policy to report on, and generate the report to show systems that are compliant and non-compliant with that policy.



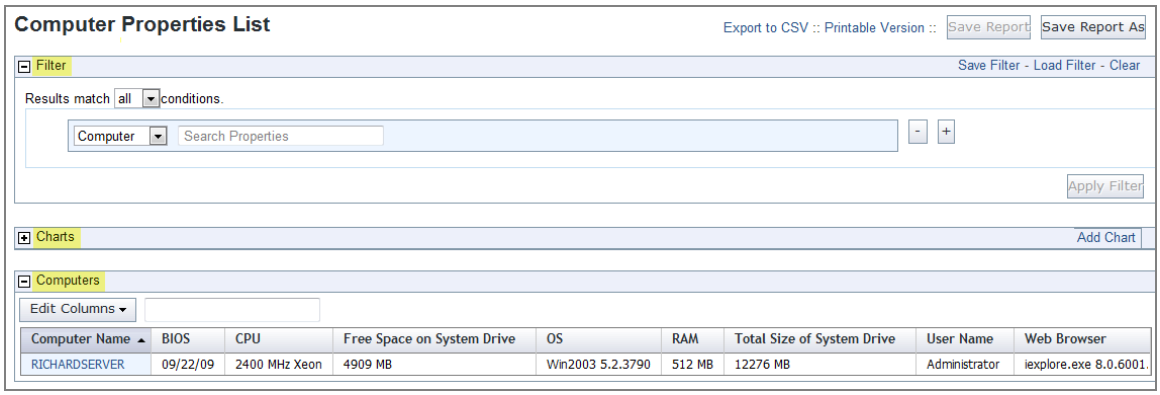
To view SCM Web Reports from a browser, follow the steps below:

1. Select *Launch Web Reports* from the Tools pull-down menu in the Console. Enter your username and password, and then click *Login*.
2. Click *Report List* from the links at the top of the screen.



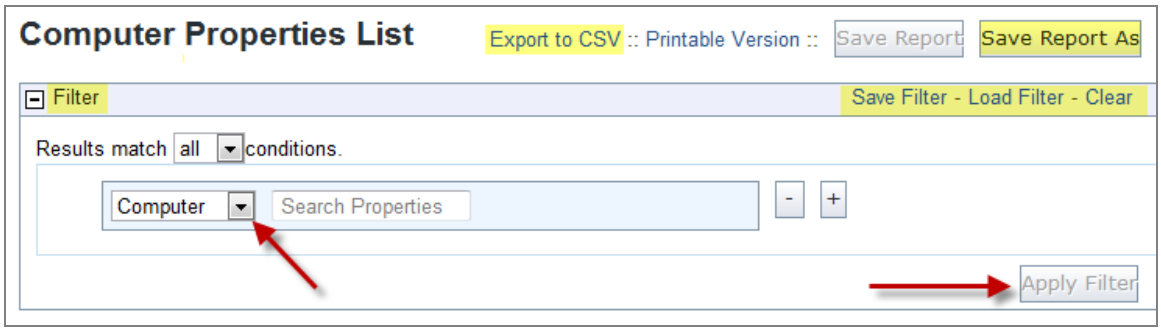
3. From the list of reports, select *Security Configuration Management Report Template* at the top of the page. The browser will display a report similar to the SCM Dashboard.

Web Reports will display content in three sections: Filter, Charts, and Computers.



Customizing Reports with Filters

Report filters for the Web Reports application are way of preserving and re-using the customization settings on a saved search. The *Filter* box will be visible at the top of the report screen, allowing you to customize the content you want displayed in your reports.



You may filter data according to specific computers or groups of computers, or by properties. For example, you can create a filter to look only at Windows machines, and this filter can be applied to SCM Web Reports. These filters are similar to the device filters noted in the SCM Dashboard section of this document.

Use the buttons displayed to save, load, export, and apply filters for future use.

Part 5

Resources

Frequently Asked Questions

Can I parameterize all controls?

No.

Why doesn't remediation work on all Windows controls?

Your security policy is enforced via GPO, or there is no way to remediate this via a local policy.

Where can I find a sample file containing UNIX parameters?

Each task deployment for SCM on Solaris 10 automatically includes a customer_params.sample file under /var/opt/BESClient/scm_preserve/SunOS/5.10, which contains the default parameters for all parameterizable controls.

How do I return UNIX parameters to their default settings?

Make a copy of the customer_params.sample file (as discussed in the previous FAQ) and use this file for new deployment.

Where can I view the current parameter settings on each machine?

There is currently no way to view parameter settings for Windows 2003. For Solaris 10, make sure to keep track of the file containing your customer parameters and use it as a reference. By default, this file is named customer_params and is located in /var/opt/BESClient/scm_preserve/SunOS/5.10. See the section named *Parameterizing UNIX Controls*. To see whether or not your parameter settings have taken effect, take note of the settings as they appear in the find.results files under the results folder mytmp/results, and if necessary compare them with your file containing customer parameters.

Is there support available for Microsoft policies?

Microsoft has supplied the following tools to help you manage policies, available from the Start>Run option:

- Group Policy Object Editor - gpedit.msc
- Group Policy Results - gpresults.msc

Why does the "Home directory file Ownership" UNIX Fixlet control (GEN001540) take so long time to complete?

On a system for which the home directory has many files, this action may take an hour or more to complete. BigFix may provide a more optimized action in a future release.

In the UNIX results folder mytmp/results, I am seeing .detect.log files corresponding to unrecognized controls. These files contain a single line with this format: "./SunOS/5.10/file.detect: ./SunOS/5.10/file.detect: cannot open". What does this mean?

If the runme.sh shell script is run with either the –f or –F options on any control scripts which do not exist in the deployment, a corresponding .detect.log file will nonetheless be created in mytmp/results for those nonexistent controls. This should not affect any existing control scripts, whether for assessment, remediation, or parameterization.

Does BigFix have compliance evaluation reports/mechanisms that compare a machine (laptop/server) against FISMA/NIST/DISA standards?

BigFix Security Configuration Management Compliance Controls (also referred to as "SCM Compliance Controls" or "SCMCC") provide the ability to assess servers, laptops and desktops against a predefined set of configuration standards such as DISA STIG (Standard Technical Implementation Guides) and FDCC (Federal Desktop Core Configuration). BigFix also has the ability to support configuration standards from NIST, NSA and other standards organizations as well. Regulatory compliance regulations such as FISMA, PCI, and others can easily be supported by using the standard configuration controls provided through the BigFix supported product heterogeneously across Windows, UNIX, and Windows environments.

What are some of the things I cannot do using this content?

The BigFix SCM Compliance Controls solution is designed to be very flexible. However, there are some known limitations:

- The remediation functionality on both Windows and UNIX is limited to specific configuration settings. In some cases, there are controls that we are not currently able to remediate.
- The parameter functionality on both Windows and UNIX is also limited to specific configuration settings. Similar to remediation, not everything can or should be parameterized.

What happens if I subscribe sites incorrectly to a system?

It is very important to leverage sites and site subscription functionality as part of your SCM Compliance Controls deployment. The sites will enable you to create a specific template of configuration settings that you want to assess and enforce. The site subscription will enable the BigFix administrator to assign the configuration template (i.e. site) to a single endpoint or group of endpoints. The default behavior of the out-of-the-box SCM Compliance Controls sites will be to subscribe to all computers. If this is not strategically focused on the appropriate endpoints, the reporting dashboard will evaluate all settings for a given system.

> Example: If you load the mastheads for Windows 2003 and Solaris 10 and do nothing else, the reporting dashboard will report on the compliance of the Windows 2003 systems inclusive to both sites. By removing the site subscription for Solaris 10, the system will only evaluate against the Windows 2003 content, which is the desired behavior.

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

When a remediation action is run, the remediation action will rerun the detection script. Once the detection script is run, it should provide the validation of whether or not the remediation was successful. If successful, the Fixlet will turn non-relevant. If unsuccessful, the Fixlet will remain relevant.

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

We utilized 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 will 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 should be root or whichever user is the owner of the BES Client.

Additional Documentation

For information about the BigFix platform, review the BigFix Console Operator's Guide. In addition to this *User's Guide*, this release of SCM also includes an *SCM Setup Guide*, *Guide to Using Windows and UNIX Benchmarks, SCAP QuickStart,* and *SCAP User's Guide*.

For information about parameterization, please refer to the existing Red Hat, AIX, and Solaris Parameter Guides available on the BigFix Support website.

Global Support

BigFix offers a suite of support options to help optimize your user-experience:

- First, check the BigFix website Documentation page
- Next, search the BigFix Knowledge Base for applicable articles on your topic
- Then check the User Forum for discussion threads and community-based support

If you still can't find the answer you need, contact BigFix's support team for technical assistance:

- Phone/US: 866 752-6208 (United States)
- Phone/International: 661 367-2202 (International)
- Email: enterprisesupport@bigfix.com

Index

T

U

V

W

