BigFix® Security Configuration Management (SCM) Deployment Guide

BigFix, Inc.

Emeryville, CA

Last Modified: 9/18/2008

All inquiries regarding the foregoing should be addressed to:

BigFix, Inc.

1480 64th Street, Suite 200

Emeryville, CA 94608

Contents

Preface

Audience

This document describes a portfolio of security configuration content from BigFix called Security Configuration Management (SCM). This content comes in the form of SCM Checklists and will provide a means for organizations to assess and manage the configurations of their desktops, laptops, and servers.

The audience for this guide includes those people in IT operations responsible for managing and enforcing corporate system configuration policies on endpoints. This includes administrators at all levels who must maintain compliance with Federal and Industry Regulations or are generally interested in maintaining a centralized configuration management security policy across hundreds to hundreds of thousands of systems using the BigFix real-time visibility and control solution.

Security teams in the enterprise will use the SCM checklists to define the security parameters and configurations that are required by corporate policy. IT managers will use the SCM checklists to enforce security policy and document the current state of compliance against corporate policy. BigFix Console Operators will focus on the detailed day-to-day configuration management of all systems within their purview and will take advantage of both detailed and summary information for each endpoint. Auditors will use SCM checklists to determine at any given point in time what the current state of compliance is for any given set of systems within the entire organization.

Organization of this Manual

This guide is divided into six main parts:

- Versions, Platforms, Conventions and Product Requirements
- Introduction
- Quick Start
- Using the SCM checklists
- Using the SCM Dashboard
- Appendix and Index

Conventions Used in this Manual

This document makes use of the following conventions:

Bold Sans	Bold sans-serif font is used for headings.
Bold	Bold font indicates labels and field names in the user interface.
Italics	Italics are used for BigFix document titles.
`Mono-space`	Mono-space font is used for sample code.

Product Requirements

The following list of requirements is relevant to this site and the BigFix deployment must be configured according to these requirements.

Minimum supported browser versions:

- IE 6.0
- Firefox 2.0

Minimum Adobe Flash player version:

- Flash Player 9.0

Minimum BigFix component versions:

- Console 7.0.9
- Web Reports 7.0.9
- Windows Client 7.0.9.164
- Unix Client 7.0.2

Introduction

Security compliance requirements loom ever larger for companies as computing power – and its attendant need for protection – grows exponentially. Solutions for effective security management are becoming more formalized as industry best practices, federal government requirements, and industry-specific regulation have come into play. At the same time, companies are dealing with far-flung global networks that can tax even the most robust infrastructure. Automated solutions are desperately needed to bring stability to this sprawling growth, but legacy solutions do not allow for the kind of visibility, control and flexibility demanded by modern enterprises.

BigFix Security Configuration Management (SCM) combines automation, in the form of timely and easily distributed compliance libraries, with the flexibility of customized parameterization. For the administrator, it provides instant visibility into the configurations of systems within a globally distributed infrastructure. With analysis performed locally on the endpoints and an intelligent relay system to collect the data, BigFix SCM is a fast and highly scalable solution for enterprises with hundreds to hundreds of thousands of clients. BigFix SCM includes a comprehensive Dashboard to summarize and analyze this huge data stream providing real-time visualization of the health of your IT assets.

Although all of the SCM checklists are designed to assess a system against a defined set of configuration policies, much of it can also be leveraged to remediate a system and bring that system back into compliance with the security configuration policies. Fixlet messages include the necessary Actions that enable an operator or system administrator to target one or more assets within the enterprise and remediate the configuration settings that are found to be non-compliant to your security policies.

SCM Product Features:

- Out-of-the-box library of standard security-configuration controls, with each control mapped to a specific industry standard and its associative reference Id.
- Content can be customized and control parameters can be modified to suit your specific enterprise requirements
- Ability to assess and evaluate systems against the standard control baseline
- Ability to remediate select configuration controls against defined standards
- Real-time Dashboard to identify compliance with defined security policies
- Scalable up to hundreds of thousands of endpoints

Quick-Start

Installing SCM

As with all BigFix offerings, installation of SCM is as easy as subscribing to the desired content site. Each SCM checklist will be provided as a single site and will represent a single standard and platform. Once added to a BigFix deployment, the content is continuously updated and delivered automatically.

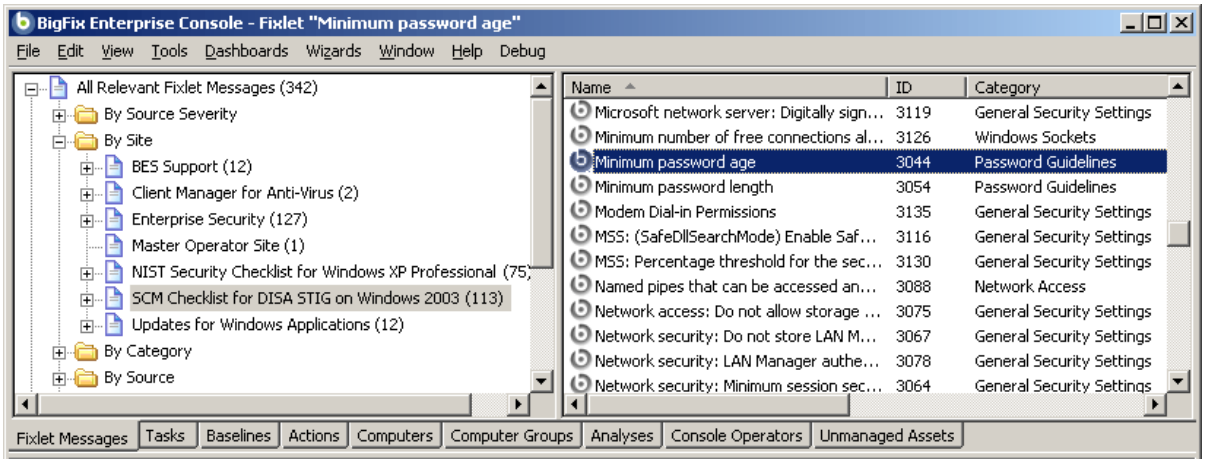
To add an SCM site or checklist, simply double-click the Fixlet site masthead on a computer where the BigFix Console is installed. The BigFix Console will then gather the content for the SCM site. You must be a master operator to subscribe to the site successfully. Typically your BigFix Server will make a connection to the Internet on port 80, however it can also be set up to use a proxy, which is a common configuration. Alternatively, an 'air-gap' can be used to physically separate the BigFix Server from the Internet Fixlet Server (for more information, visit http://support.bigfix.com/bes/install/airgapnetwork.html)

The Fixlet messages in this site will help you implement the security standards as-is or allow you to customize them to meet your own security policies. Because the relevance is evaluated locally on each endpoint, the SCM solution scales gracefully and can accommodate up to hundreds of thousands of clients.

The following Quick-start section will provide you with a high-level overview of SCM solution, the checklists and the basics of how to use them. Immediately following this section is a detailed look at how to operate the default content as well as how to customize the content to suit your own corporate policy.

Using the Default SCM Checklists

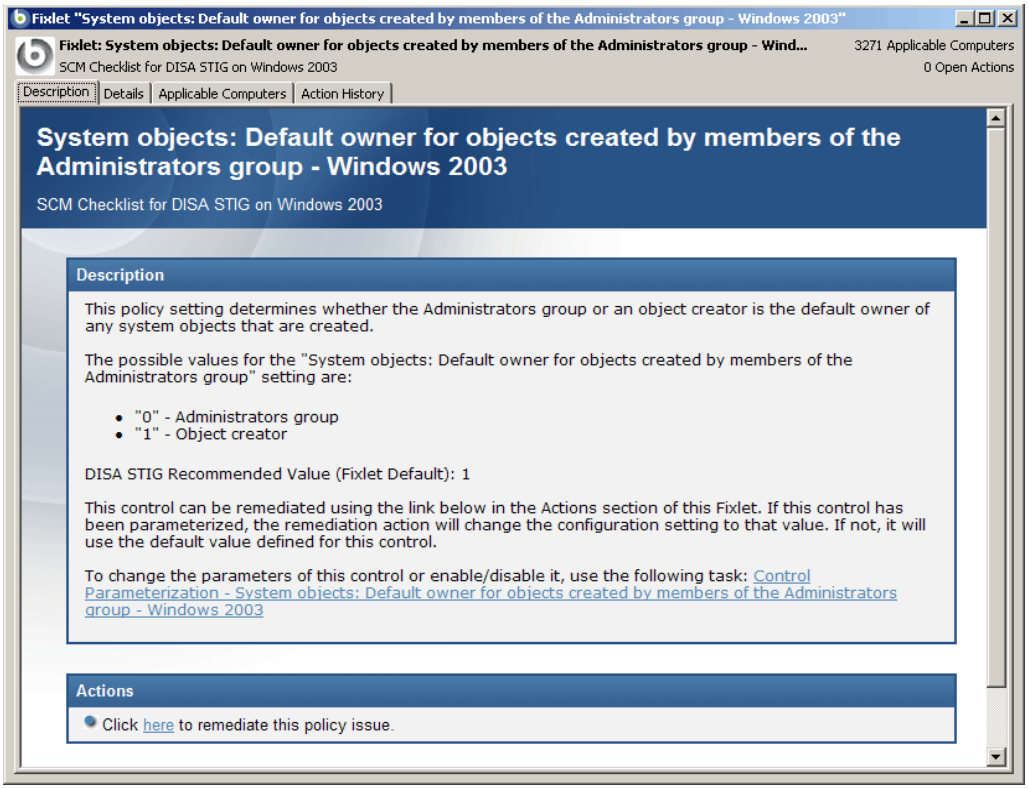
After subscribing to the SCM site(s) you can view the content by clicking on the **Fixlet Messages** tab, opening **All Relevant Fixlet Messages** from the left panel and looking in the **By Site** folder. There you will see the Fixlet site containing the SCM checklists. Click on it to view the associated Fixlet messages in the right-hand panel.



The Fixlet messages in the list represent security controls with which at least one BigFix-managed computer on your network is out of compliance. Fixlet messages use Relevance expressions to

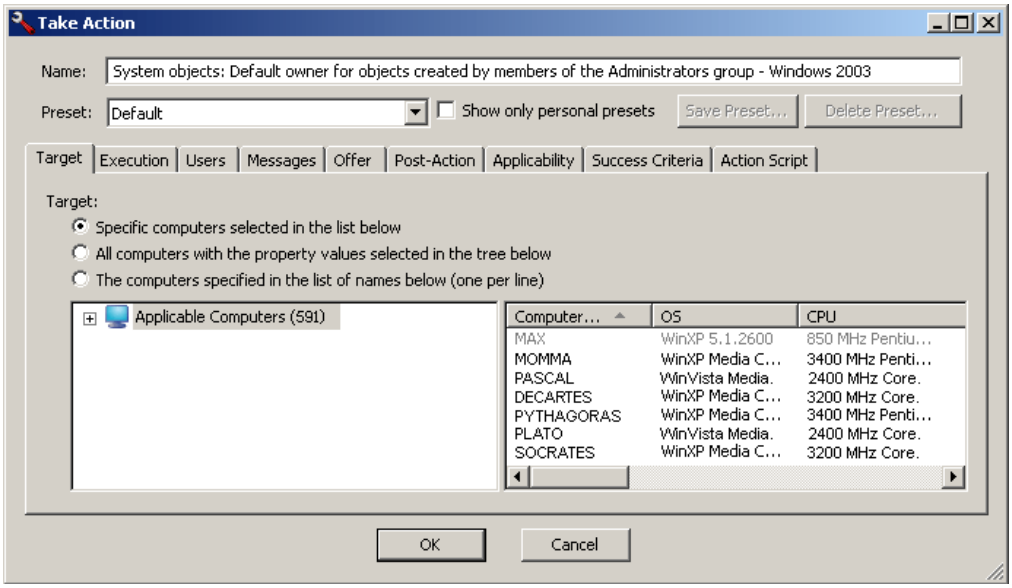
evaluate a security control locally, on each endpoint. An endpoint that is out of compliance will then report back to the BigFix Console, which will list the Fixlet message as relevant. All of this happens in minutes, guaranteeing that you are always viewing a real-time evaluation of your security status.

Double-click a Fixlet message from the list to view it. A document opens in the bottom window with tabs allowing you to view the **Description**, **Details**, **Applicable Computers** and any **Action History** that might be associated with this message. Click the Description tab to look at the text describing this Fixlet message.



Typically, you will find a short report on the security issue, allowing you to evaluate the importance of this compliance issue before you take action. Sometimes the issue is simply informative, providing you with a procedure you can follow to maintain compliance. However, most controls have active remediations associated with them. These are found by scrolling to the bottom of the message to the **Actions** section. There you will see a link that you can click to deploy the remediation.

When you select a Fixlet Action, the **Take Action** dialog opens and lets you fine-tune the deployment. In particular, you can easily select specific computers or groups of computers be remediated.



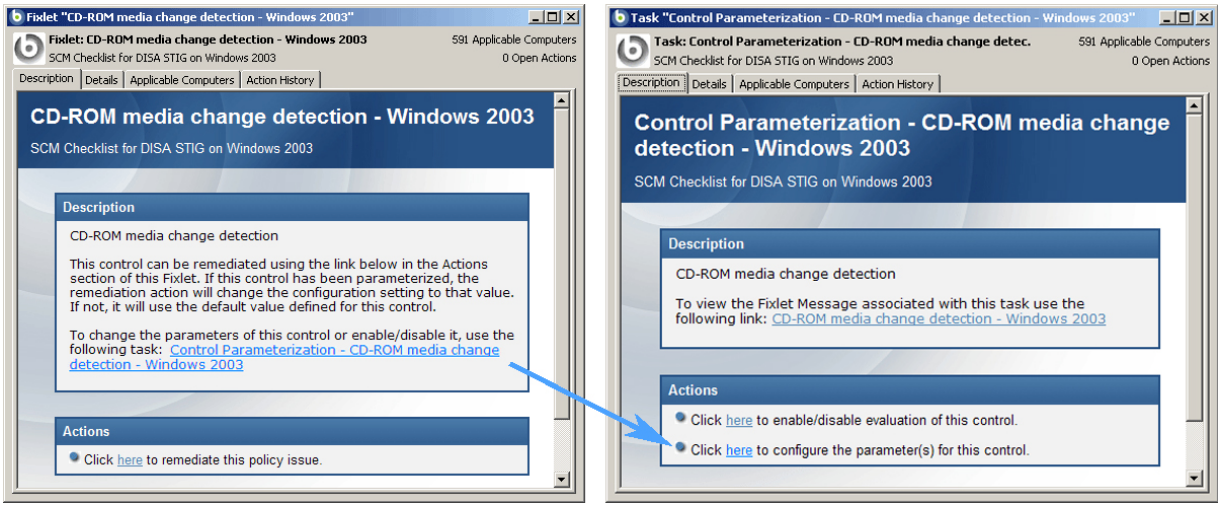
Once you have targeted your desired set, click the **OK** button and supply your password. This sets the Action in motion, and it will be sent to the appropriate endpoints immediately. As the computers are remediated, you can watch the progress using any of the reporting tools contained in the BigFix Console, including the Fixlet list, Visualization Tools, Web Reports and Dashboards. When every endpoint in your enterprise is remediated, this particular control will no longer be relevant, and it will disappear from the list of relevant Fixlet messages. As you bring your network into compliance, the list will grow ever shorter. Although the Fixlet messages will no longer be listed, they will always remain vigilant, constantly checking for any computer that deviates from the specified level of compliance.

Modifying the Controls

As well as monitoring and remediating, you can modify certain parameters to adjust the sensitivity of the controls. For instance, you might want to observe a stringent policy of using 14-character passwords, or you might be comfortable with just 8 characters. Either way, you can customize the password-length parameter to match your specific policy. Although parameters can be modified on both UNIX and Windows content, there are some differences in how this is implemented. UNIX content is aimed at users who want maximum command-line control (discussed at length later in this document).

The SCM checklists for Windows systems use BigFix Tasks to enable alteration of the parameters for each configuration setting. For each Fixlet control parameter, there is an associated Task that sets the parameter. To invoke the Task, scroll to the bottom of the Fixlet description and click on the **Control Parameterization** link. The associated Task opens with a description of what the parameter does, what the possible range is and what the recommended values are.

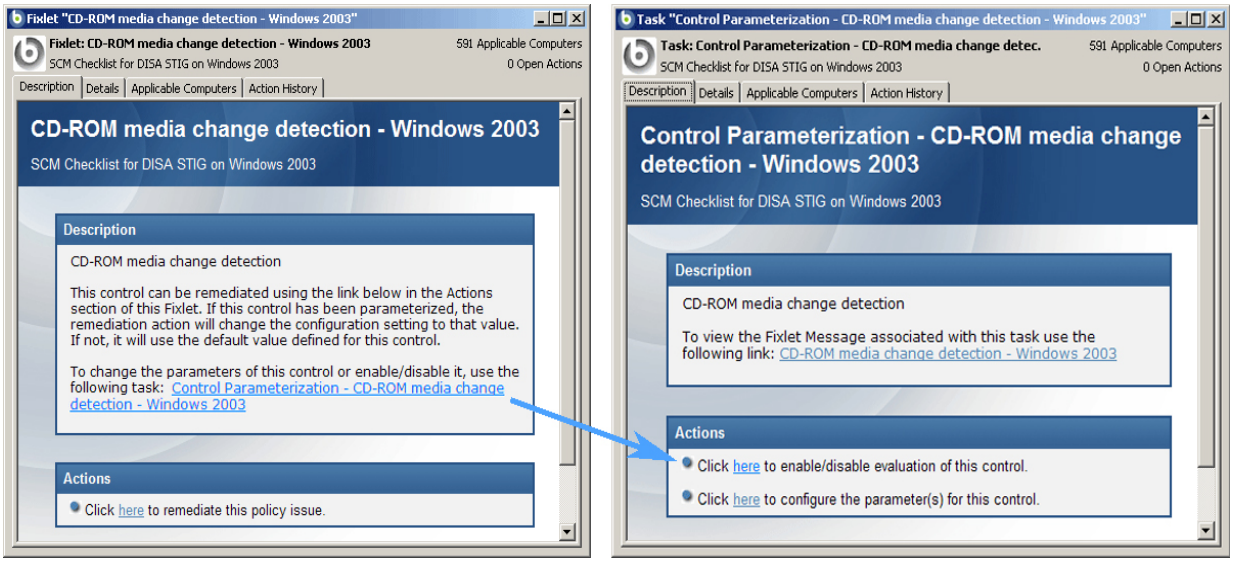
At the bottom of the Task is an Action section. You will see a link allowing you to configure the parameter(s).



When you click on this link, an Action Parameter dialog opens, where you can enter the desired value. Click OK and enter your password to deploy the new setting that will now guide the associated Fixlet control. Once set, the Fixlet message will only become relevant on those computers and devices that do not meet this new threshold. Thus, you can easily modify the Windows content to suit your exact level of comfort for each detail of your security policy.

Disabling Controls

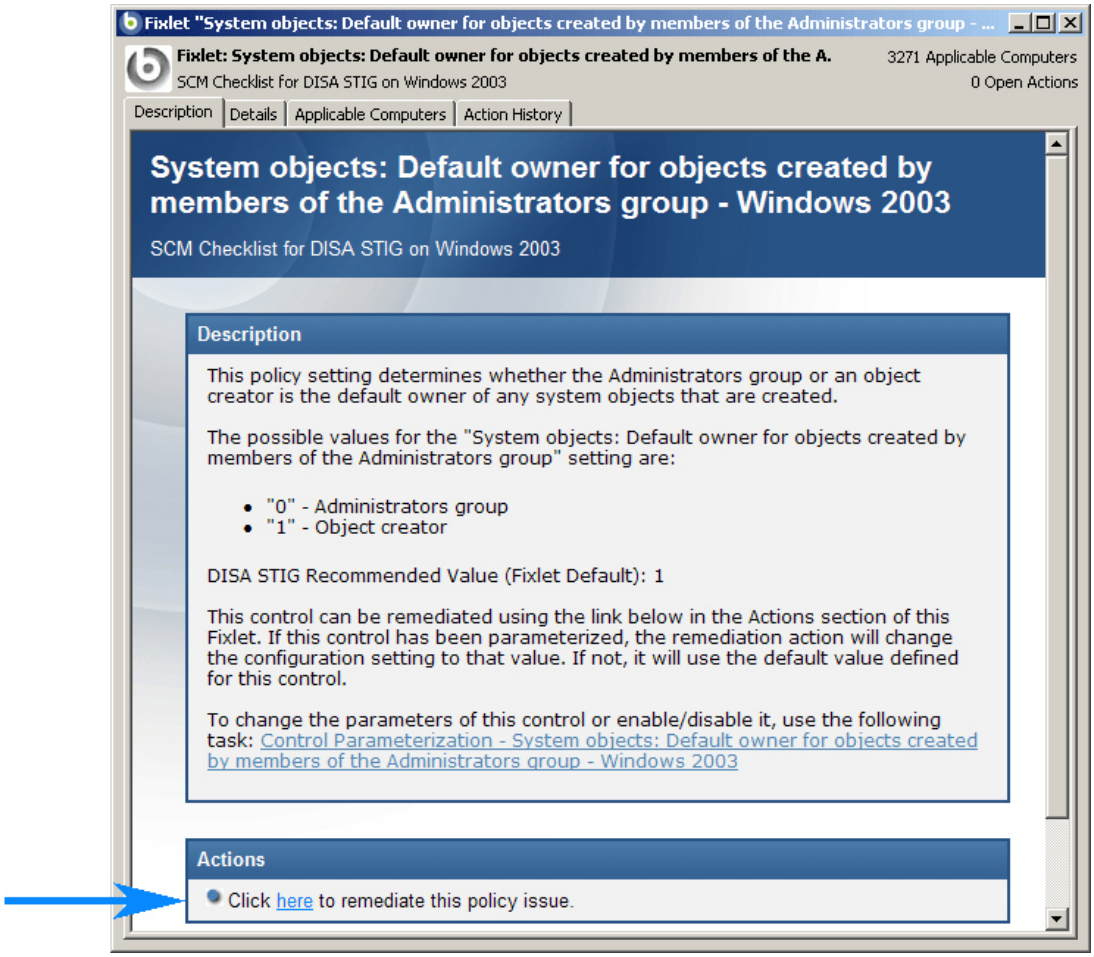
You can, on a computer-by-computer basis, disable certain controls. For instance, you may have some special legacy computers or development workstations that have their own custom security policies. To remove them from the security scan, you can disable the control for those specific devices. Again, this procedure is different on UNIX and Windows systems, and the UNIX procedure is discussed later in this guide. To disable a Windows control, follow the procedure outlined in the previous section to bring up the Task associated with the Fixlet control. In the Task you will see an action to enable/disable the control.



Click this link to bring up the **Take Action** dialog and target the set of computers that you want to exclude from evaluation. Click OK and then supply your password to deploy this exclusionary action. The selected computers will henceforth be excluded from Dashboards and Reports that are generated for the specified controls.

Remediating Out-of-Compliance Controls

If an endpoint is out of compliance with policy, it will appear in the BigFix Console as a relevant Fixlet message. Based on the nature of that issue, it may offer to remediate the problem, typically by modifying or updating a file or (on Windows) a registry entry. Click on the Fixlet message to read about the specific issue and then scroll down to the bottom of the description. If the Fixlet message offers remediation, it will appear as a link in the **Action** section.

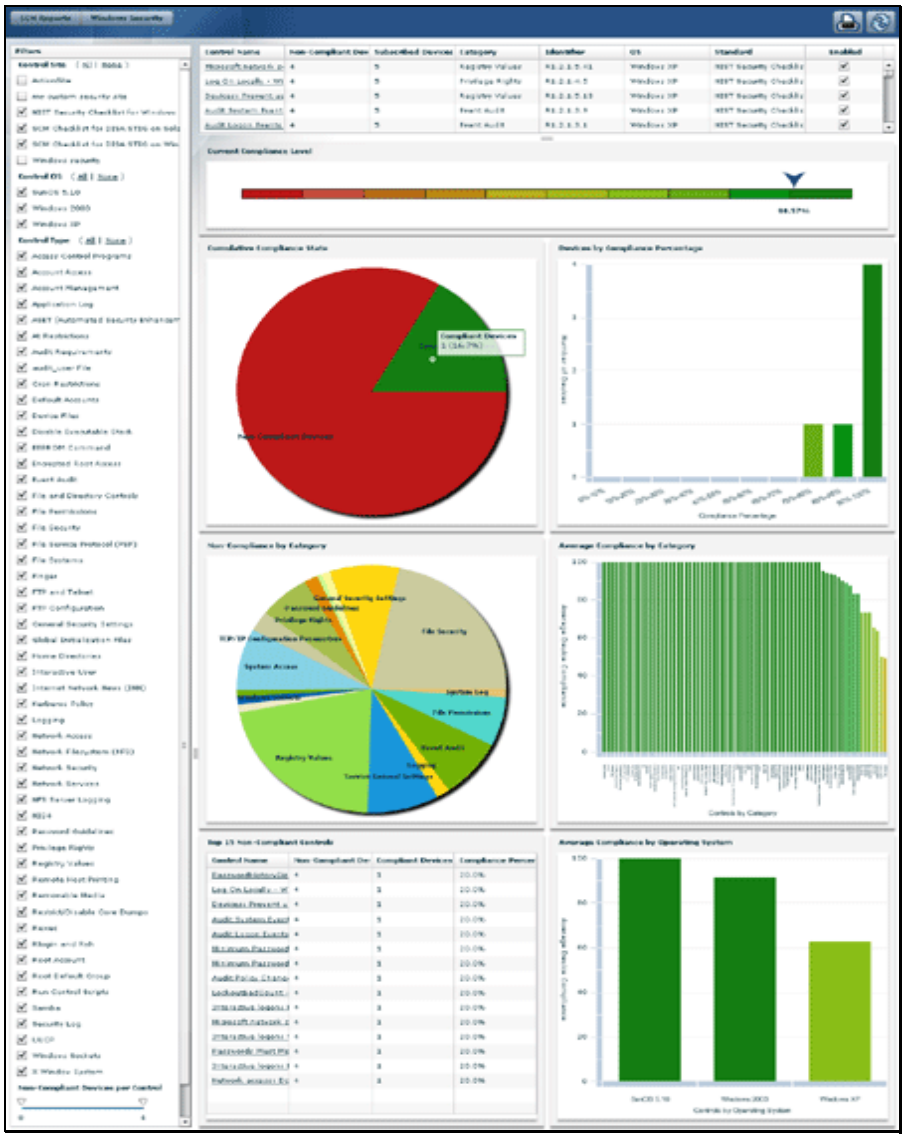


Click on this link to initiate the remediation process. The **Take Action** dialog opens, allowing you to target the Action to just the subset of computers you desire. You can also set other parameters for the Action as described in the ***BigFix Console Guide***.

Using the Console Dashboard

The SCM solution includes a graphical dashboard that provides an overview of your security posture and allows you to drill down into the details. The charts can be precisely tuned and customized to help you concentrate on any desired slice of your company that is currently of importance to you. These custom reports can be saved, so that you can quickly revisit any subset of your enterprise in minutes. Since the information for the dashboard is generated at the endpoints and sent back through an intelligent relay system, you can visualize the most far-flung enterprise in real time.

To see it in action, select **Security Configuration Management** from the **Dashboard** menu. Click **Create New Report** and supply a name. After it gathers the information from your endpoints, the Dashboard will create its display. Experiment with the controls and watch how the associated graphs change. Move your mouse over the graphs to see specific information on each segment. Click on a graph to drill down into the constituent information. To save your report, click on the disk icon in the upper right.

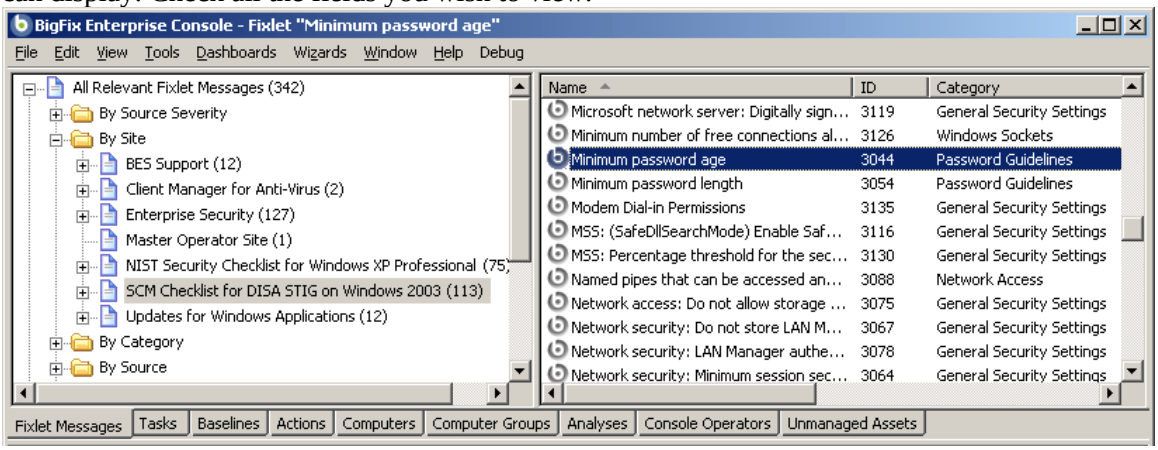


SCM Fixlet Controls

All of the Fixlet controls in the 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 one of the configuration standards. By viewing the SCM Fixlet messages within the BigFix Console, you can quickly identify which security standards are being violated and which computers are out of compliance.

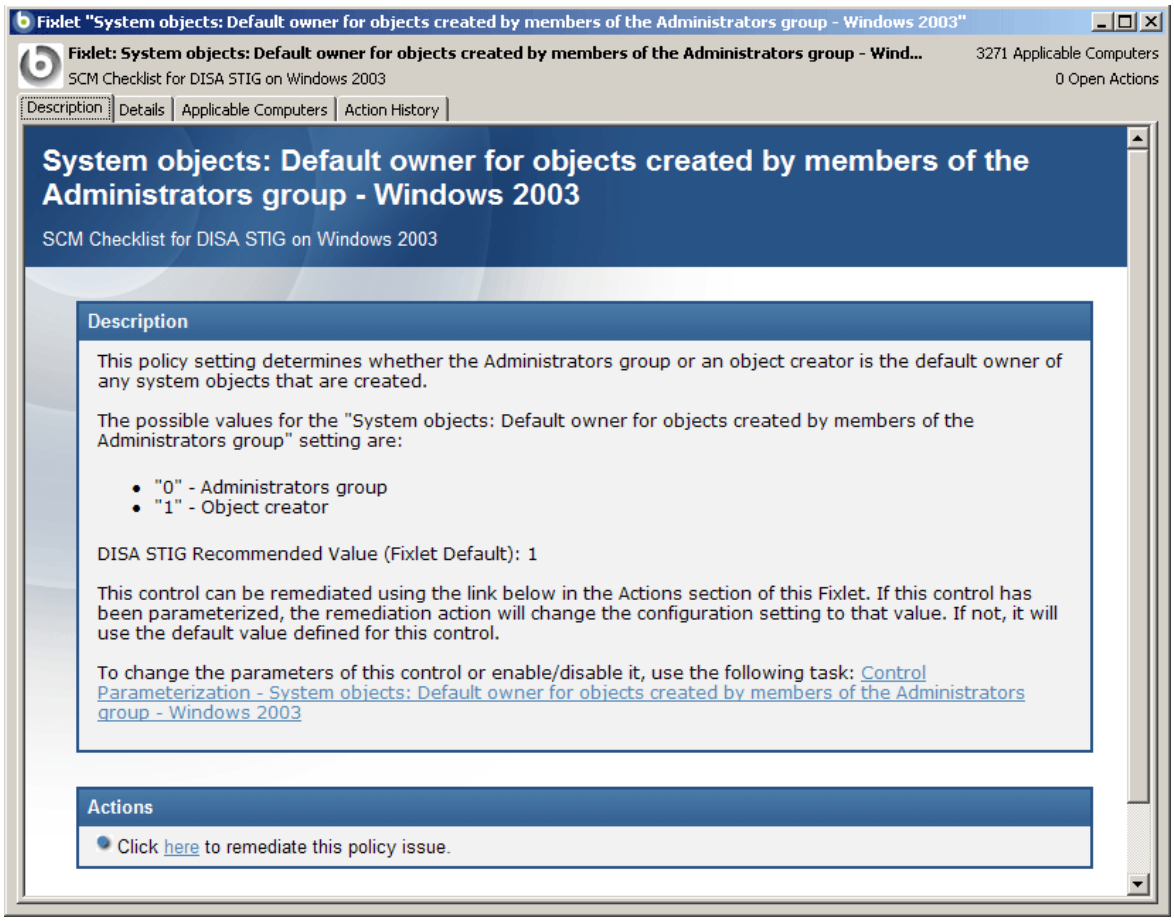
To start using the SCM checklists and other controls, you need to contact your BigFix representative and get a masthead for the appropriate SCM site. When you receive the masthead, simply double-click it to open it within the BigFix Console, which will immediately start to download the latest content. Once you have gathered the entire Fixlet library, follow these steps to view the controls:

1. Click the **Fixlet Messages** tab.
2. From the filter panel on the left, choose **All Relevant Fixlet messages** and then select **By Site**. The sites you have subscribed to are listed, along with the number of relevant Fixlet messages (in parentheses) next to each. You can also select **All Fixlet Messages** to view the entire list of Fixlet messages, including those that are not currently relevant.
3. From the site list, choose the SCM site you want to explore. When you do, the Fixlet list in the right panel displays the currently relevant Fixlet controls from that site that are applicable to your BigFix network. You can sort the list of Fixlet controls by any field by clicking on the desired header. Right-click the header to bring up a context menu with a list of the available fields you can display. Check all the fields you wish to view.



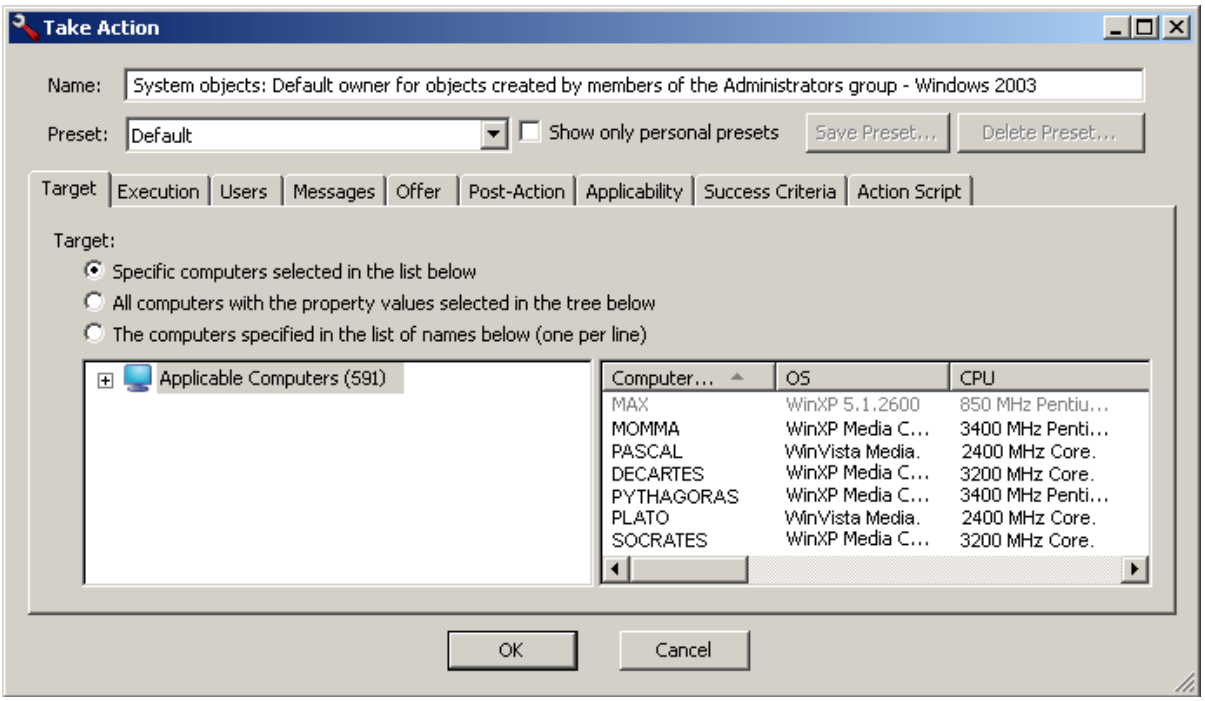
4. Double click to select a Fixlet control from the list to view it in detail. The corresponding document opens in the work area below the list. It contains information about the control and may also have links to customize the evaluated value of the configuration setting and may also include an Action 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 given as the number of applicable computers in the upper right of the panel. Read the description to understand more about this particular control.



5. Windows Fixlet messages may have a link at the bottom of the description allowing you to customize the parameters of the control. If you want more stringent or more flexible values than the recommendation, you can change the parameter that determines whether or not a device is in compliance. This is a fast and simple way to customize an SCM control to suit your own security policy. UNIX controls also provide custom parameterization, but through a different mechanism, as discussed later in this guide. To modify the value, click the **Control Parameterization** link to bring up a parameter-setting Task. For more information on this feature, see the section titled .

6. Many Fixlet controls have built-in Actions to quickly remediate the issue. To start the remediation process, click the Action link. This opens the **Take Action** dialog, which allows you to target the computers you wish to remediate.



7. The **Take Action** dialog enables you to select computers manually or by retrieved properties, such as the operating system. Click **OK** and provide your password to propagate the Action.

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 the remediation value brings the given client computer into compliance with the 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 it will re-appear in the relevant Fixlet list.

The SCM Dashboard collects statistics based on the status of these Fixlet messages, letting you quickly visualize which computers are compliant for any given control across your entire network.

Subscribing Clients to SCM Sites

When deploying an SCM checklist, special consideration should be given to what baseline of configuration settings should be implemented on a given system. In many cases, organizations define a single baseline for a single class of systems or type of systems and apply that baseline for both assessment and remediation when needed. The SCM checklists should be carefully 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 the systems. Not subscribing the sites may lead to a distortion in the reporting dashboard.

Generally, when you subscribe to a Fixlet site, the Console does all the work and distributes the sites to all BigFix Clients by default. To properly target your Clients, follow these steps:

1. From the **Tools** Menu, select **Manage Sites**.
2. The Manage Sites dialog opens. From the list of sites, select a security site that is targeted to a specific OS, such as the **SCM Checklist for DISA STIG on Windows 2003**.
3. Click the **Properties** button.
4. From the Site Properties dialog, click the **Subscription** tab.
5. Click the button labeled **Subscribe only the following group of clients to this site**.
6. Click the **Edit subscription group definition** at the bottom of the dialog box.
7. From the Edit subscription group dialog, enter a property setting that will 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 subscribe only those computers where the OS contains “Win2003” 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. Here are the group definitions for other operating systems:

- For Sun
  - OS contains "SunOS 5.10"
  - OS contains “SunOS 5.9”
  - OS contains “SunOS 5.8”
- For Windows:
  - OS contains "Win2003"

This is the basic procedure for viewing and using a SCM checklist on all supported platforms. However, there are differences between the Windows and UNIX platforms and how you set parameters, as the subsequent sections demonstrate.

Using Windows SCM checklists

The SCM checklists for Windows systems are delivered as a set of Fixlet messages and Tasks. Both the Fixlet messages and the Tasks have several key attributes that can help you find the information you want.

- **Name** – A descriptive title for the Fixlet message.
- **Description** – A plain-text discussion of the control explaining the source of the problem and various remedies.
- **Source ID** – The Source ID for each Fixlet message, based on the standard addressed by the particular Fixlet site.
- **Category** – Fixlet messages are grouped into easy-to-understand categories that allow you to sort, group and find them by function.
- **Source** – The Source field will indicate the originating standard and version from which the configuration setting was drawn.

Understanding Windows-based SCM

The SCM checklists for Windows-based platforms will exist within a specific out-of-the-box Fixlet site. Each Fixlet message corresponds to a specific configuration setting and uses the standard BigFix Relevance language to define how that particular setting will be evaluated on the Windows-based endpoints. Each control is assigned a category (such as **File Permissions** or **Password Guidelines**), which can be used for sorting or reporting.

Controls have associated Actions and Tasks that may provide one or more of the following features:

- **Enable/Disable Fixlet evaluation** – allows you to exclude the given Fixlet message from evaluation on one or more endpoints. This is a toggle that you can turn back on to include the Fixlet message again.
- **Parameterize Fixlet message** – allows you to change the parameter value of a Fixlet message on one or more endpoints.
- **Remediate Issue** – allows you to enforce and reset the actual value of the configuration setting on one or more endpoints.

Disabling Windows Controls

You may want to stop the Relevance evaluation of a Fixlet message for a certain segment of your endpoints. There are two ways to do this: you can create a custom site and simply leave this Fixlet message out, or you can disable the Fixlet message for specific computers. Custom sites are discussed later in this guide. To disable a Fixlet message for a given set of computers, follow these steps:

1. After opening a Fixlet message for viewing (see the previous section), click the **Description** tab to see the message associated with this particular control.
2. If the selected Fixlet message can be disabled, you will see a link at the bottom of the description, typically with language talking about **Control Parameterization**. Click this link to bring up the related settings Task that will allow you to disable the Fixlet control.

3. The associated Task appears in the work window, typically with a title starting with “Control Parameterization”. Make sure the Description tab is selected.
4. At the bottom of the description, you will see an **Action** section. Click on the link to **enable/disable** the evaluation of the control.
5. An **Action Parameter** dialog will open. Enter a “1” to disable the Fixlet control.
6. The **Take Action** dialog will appear and from there you can target the set of machines on which you would like to disable the control. Click **OK** and supply your password to deploy the Action. If you disable the control on all applicable computers, this Fixlet message will disappear from the list of relevant Fixlet messages.

Enabling Windows Controls

You can enable a Fixlet message that has been disabled by following the previous procedure and entering a “0” to enable the Fixlet message. However, if the Fixlet message has been disabled on all endpoints, it will no longer appear in the Relevant Fixlet list. It is still stored in the Fixlet site, however, and you can re-enable it if you wish. To do so, follow these instructions:

1. To locate the disabled Fixlet message, use the filter panel in the upper left corner of the BigFix Console and click the item labeled **All Fixlet messages**. This allows you to view all Fixlet messages, regardless of their relevance.
2. Locate the desired Fixlet message from the list to the right of the filter panel. Double-click it to view it in the work window.
3. Click the **Description** tab and scroll down to see the link labeled **Control Parameterization**. Click it to bring up the related settings Task.
4. Click the **enable/disable** link and enter a “0” (zero) in the **Action Parameter** dialog.
5. The **Take Action** dialog opens. As before, target the desired computer(s), click **OK** and supply your password to deploy the Action. If there any computers out of compliance with this issue, in a few minutes the control will re-appear in the Fixlet list.

Setting Windows Fixlet Parameter Values

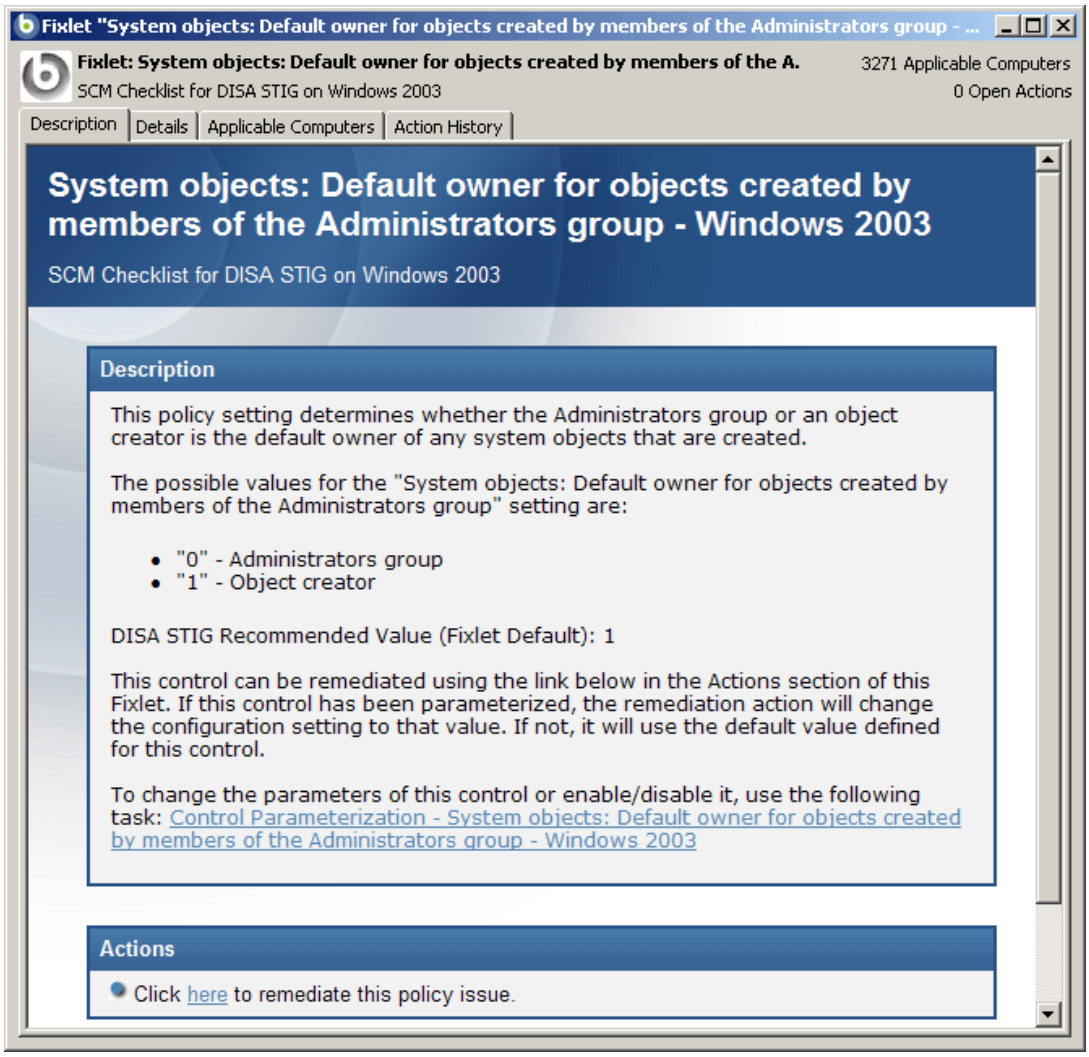
Every organization requires different levels of security. Depending on the system administrators, thresholds for security, the applications that run on each system and myriads of other potential differences, organizations may need to customize their own security policies. Part of this customizing process includes changing the values for defined configuration settings to meet specific corporate policies.

BigFix enables you to customize the content in the default Fixlet site by special targeting, customizing parameters and disabling controls, as discussed in the previous sections. However, with a little more effort, you can achieve far greater flexibility with a custom site. This gives you great latitude in your deployment options, helping you to craft finely targeted security policies and apply those policies to selected endpoints.

To address these variable needs, you can parameterize Fixlet controls to suit each individual situation. These parameters are stored as site settings, which means you can parameterize the same control differently for each site containing a copy of the control. This level of flexibility provides the most important rationale for creating custom sites.

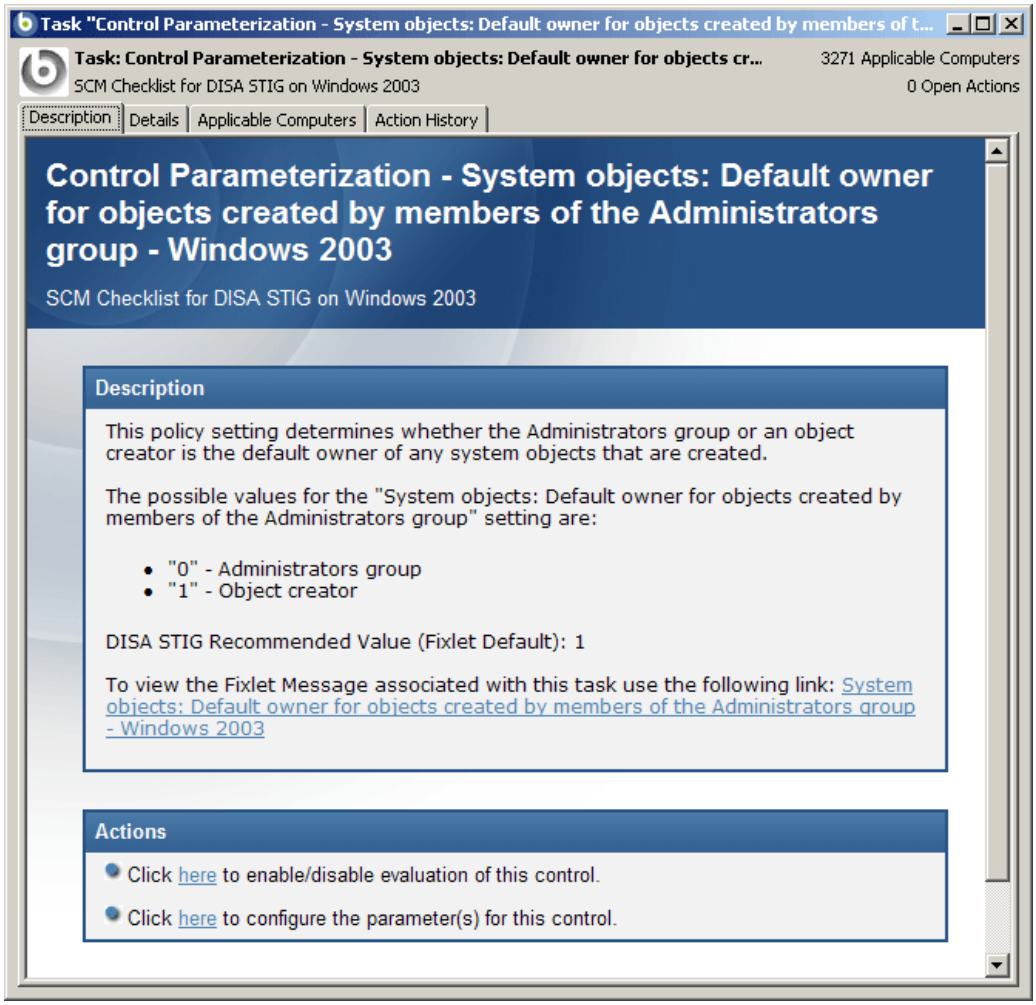
Parameters for Windows content can be modified by using the Task associated with the particular Fixlet message. Follow this example to see how this is done:

1. From the Fixlet site named **SCM Checklist for DISA STIG on Windows 2003**, select a Fixlet message. The Fixlet message opens in the workspace window. Make sure the **Description** tab is selected. You should see a window like the following.



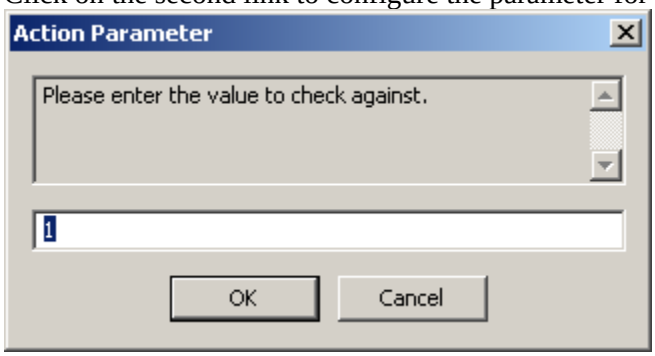
This Fixlet message has a link to **Control Parameterization**. Click the **Details** tab to analyze the Relevance clause attached to this Fixlet message. Click the **Applicable Computers** tab to see which computers in your enterprise are affected.

2. Click on the **Control Parameterization** link. This opens a task like the following in the work window.



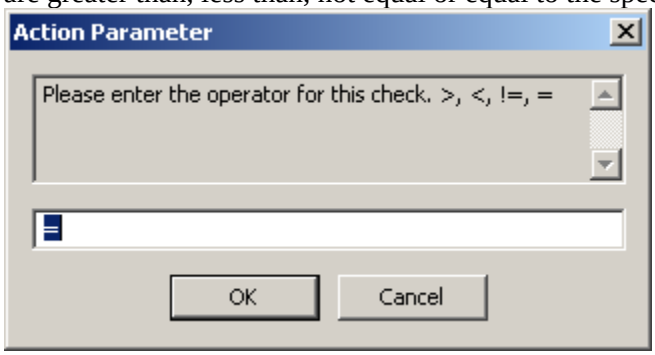
This task is tied to the previous Fixlet message and allows you link back to it if desired. There are typically two actions associated with the Task. The first lets you toggle the evaluation and the second lets you modify the parameter associated with the control.

3. Click on the second link to configure the parameter for this control. This opens a setting dialog.



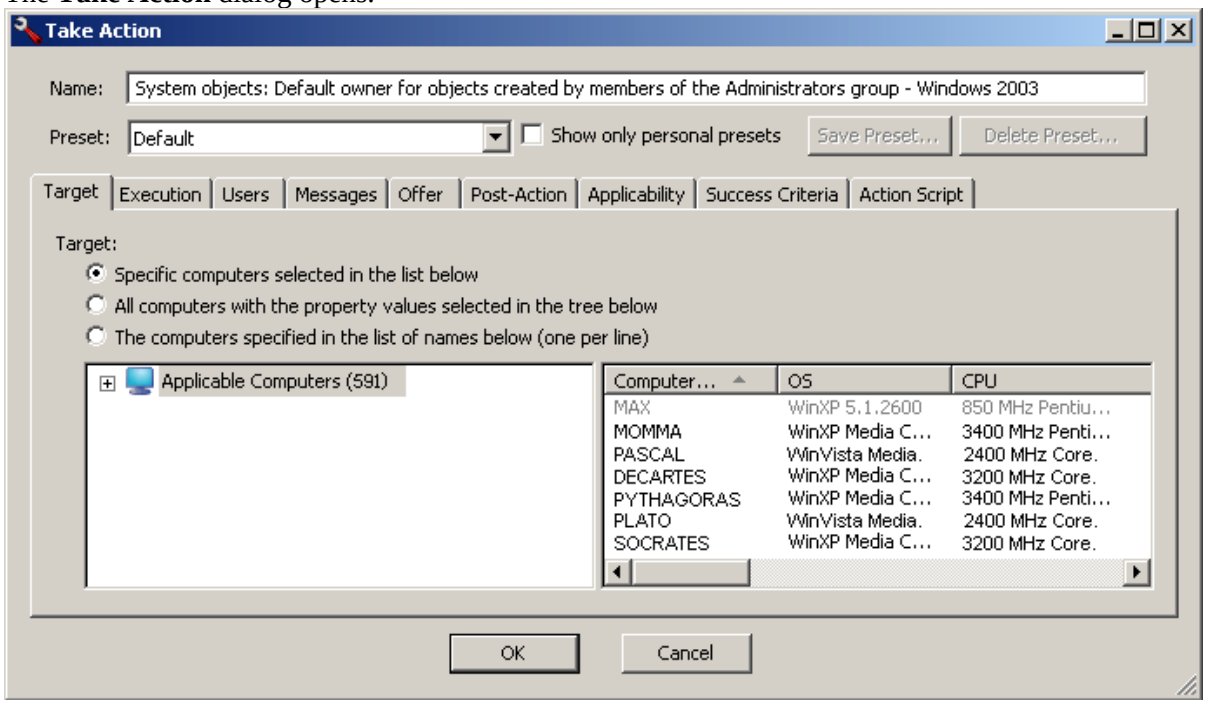
The recommended parameter is the default value (in this case 1), or the last value entered if you have previously customized the parameter. Enter a new value or click **OK** to accept the existing value.

4. The next dialog prompts you for the desired operator. The options here are to allow values that are greater than, less than, not equal or equal to the specified parameter.



In this case, we would accept the equivalence operator, and then click **OK**.

5. The **Take Action** dialog opens.



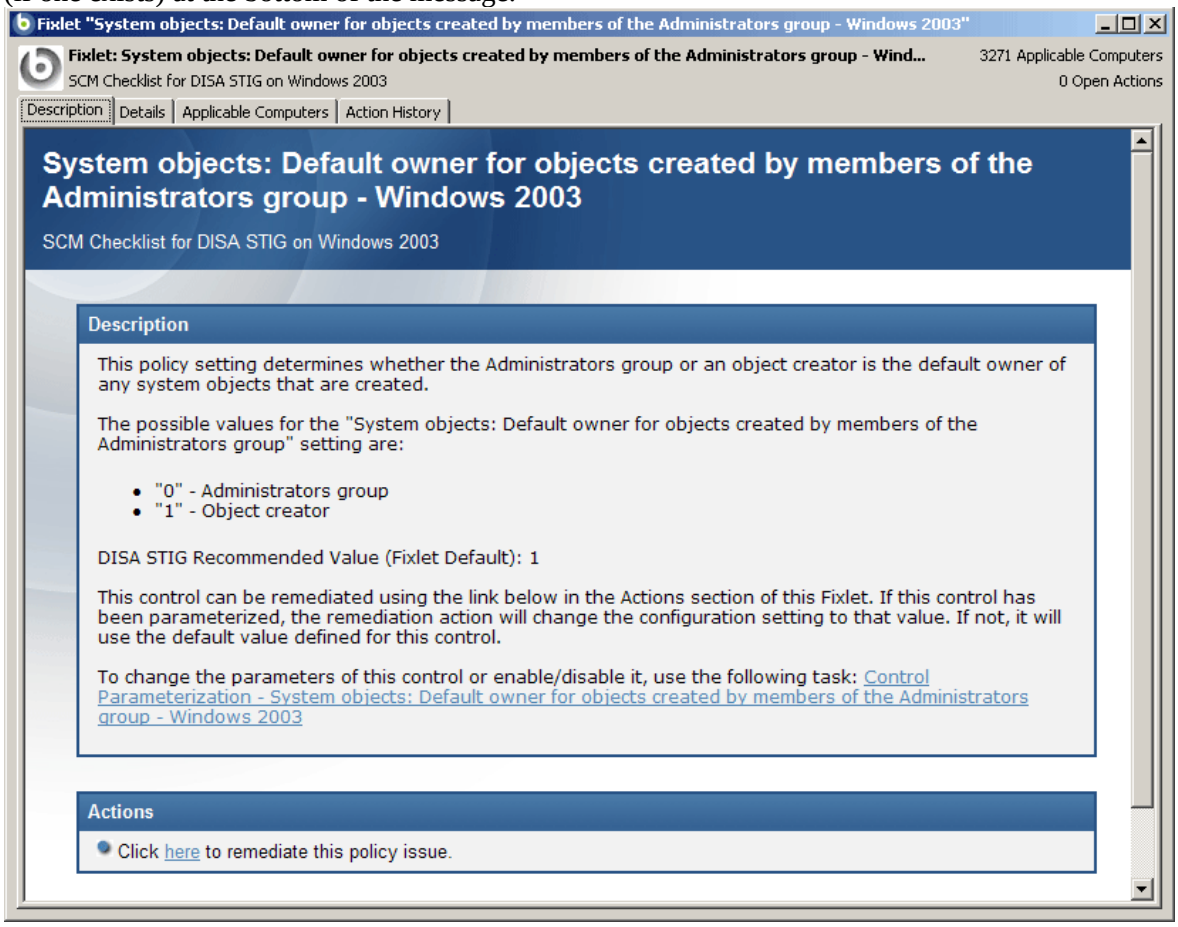
This dialog enables you to target any desired subset of computers. By clicking the other tabs, you can also customize the scheduling, users, message, post-action and more. For further information on the detailed operation of the Take Action dialog, see the ***BigFix Console Guide.***

6. Click **OK** and enter your user password to send the Action. You have now set a parameter for the specified Fixlet message, which will propagate to the targeted computers to align them with your corporate policy.

Remediation of Windows Configuration Settings

The BigFix SCM solution has the ability to audit, assess and remediate configuration settings. For those Fixlet controls that can be automatically remediated, you will see an Action displayed in the relevant Fixlet message. Follow the steps below to remediate a configuration setting:

1. Double-click to open a Fixlet message from the Console list.
2. Make sure to click the **Description** tab, then read the text and scroll down to the Action section (if one exists) at the bottom of the message.



3. Click the **Action** link to remediate the specified policy issue.
4. The **Take Action** dialog appears. There are many choices available to you for deploying Actions. Click on the various tabs to explore your options. For more information on the Take Action dialog, see the ***BigFix Console Users Guide***. Typically, you will accept the listed computers or select a subset of them to receive the action, and then click **OK**.
5. Enter your password, and the remediation Action will then deploy across your network to the specified computers. The Action will typically change the value of a setting in a file or (on Windows) in the registry. That setting can be the value supplied by the default Fixlet control or the value you supplied if you customized the parameter.

Using UNIX SCM checklists

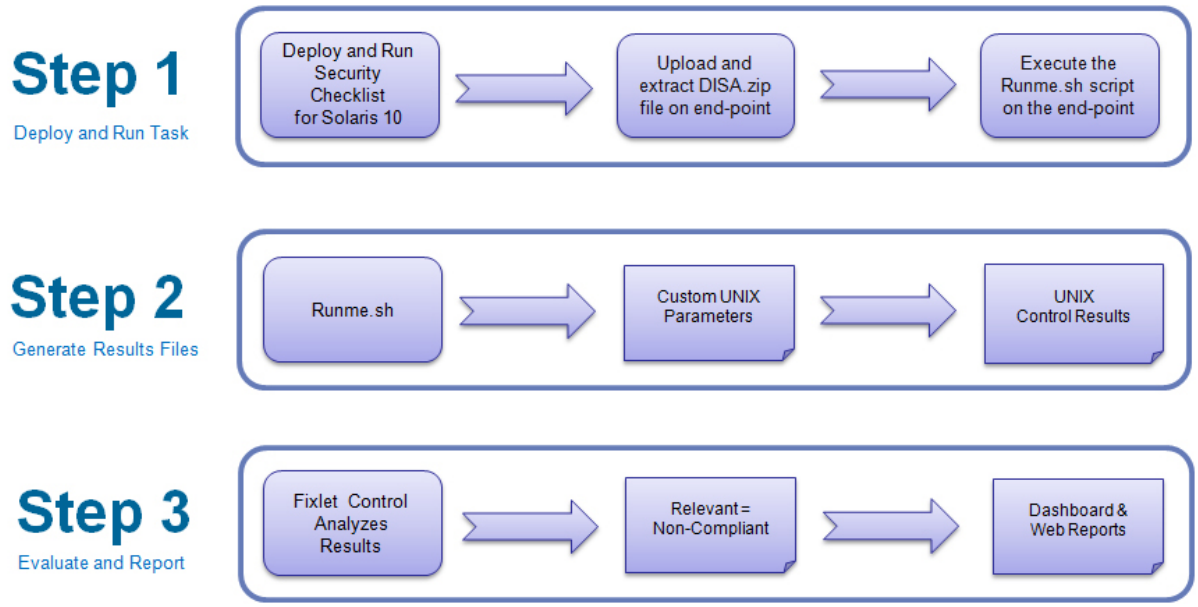
The SCM checklists for UNIX systems are delivered as a set of Fixlet messages and a single Task that is used to scan a UNIX system on demand or periodically via scheduling. Each UNIX SCM Fixlet message includes key attributes that can help you to manage the information:

- **Name** – A descriptive title for the Fixlet message.
- **Description** – A plain-text discussion of the control explaining the source of the problem and various remedies.
- **Source ID** – The Source ID for each Fixlet message, based on the standard addressed by the particular Fixlet site.
- **Category** – Fixlet messages are grouped into easy-to-understand categories that allow you to sort, group and find them by function.
- **Source** – The Source field will indicate the originating standard and version from which the configuration setting was drawn.

These fields stay attached to the Fixlet message even when you copy them to a custom site.

The UNIX content is predicated on the need to execute a Task that runs each of the defined SCM UNIX controls in a batch, as distinct from the real-time assessment employed by the Windows site. When the batch file runs, the results are evaluated on the desired endpoints, and the results are logged and made available to the corresponding Fixlet controls for evaluation. Fixlet messages then use the BigFix Relevance language to examine the log and determine relevance. The results appear in the BigFix Console, where compliance can be determined as with any other BigFix content.

The workflow for managing a UNIX SCM checklist can be represented diagrammatically.



The following sections explain this workflow in greater detail.

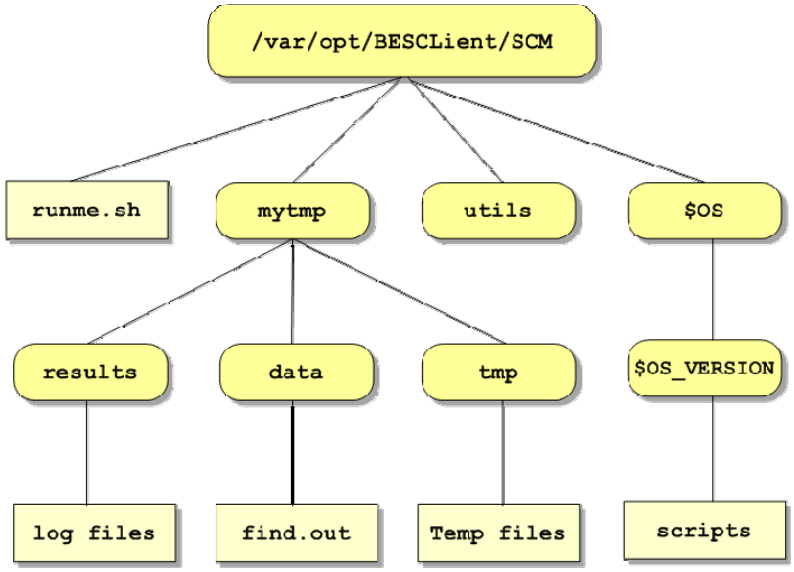
Understanding UNIX SCM

With most BigFix content, Fixlet messages constantly evaluate conditions on each endpoint and show up in the Console when the relevance clause of the Fixlet message evaluates to true.

BigFix UNIX SCM content works differently. Here, a **Task** initiates a scan of the endpoints. This Task can be run on an ad-hoc basis each time a scan is required, or may be run as a recurring policy from the Console.

The endpoint scan is accomplished by a series of UNIX Bourne Shell scripts. As each script runs, it detects a setting or condition and then writes the information to an output file that is made available to the corresponding Fixlet control for evaluation. Once the log files have been written to disk the Fixlet messages read each log file and display the results in the BigFix Console. Although the end result is similar, this method of detection provides greater accessibility to UNIX system administrators.

After running the **Deploy and Run Security Checklist** Task, the scripts reside in a directory under **/var/opt/BESClient/SCM**. Here is an overview of the directory structure:



- **/var/opt/BESClient/SCM** is the base directory of all the scripts and contains the shell script **runme.sh**. This is the master script which, in turn, executes the OS-specific scripts in the appropriate directories.
- The **utils** subdirectory contains utility scripts that are used by the rest of the scripts.
- The **$OS** and **$OS_VERSION** directories contain the control scripts that do the actual detection of settings and conditions. Each control script is named with the corresponding control ID that is referenced elsewhere.
- The **mytmp/results** folder is of particular interest because this is where the OS-specific shell scripts write their log files. These logs are examined by Fixlet messages to ultimately determine relevance. The log file format is covered later in this section.
- **mytmp/data** primarily contains the **find.out** file which contains a directory listing of all locally mounted file systems. This file is used by many of the OS-specific scripts.
- **mytmp/tmp** is used for temporary files created by the shell scripts.

There are several options you can pass to the shell script runme.sh:

- When run from the **Deploy and Run** task, runme.sh defaults to the **-g** option which does a global find. This creates a directory listing of all locally mounted files. The script then executes all scripts.
- When run with no options, runme.sh runs all the detection scripts that are appropriate for the specific endpoint operating system.
- When run with the **–t** option, runme.sh creates a trace file of the commands executed by the OS-specific script(s). This option is used for debugging only.
- When run with the **–f <source id>** option, runme.sh runs only the specified OS-specific control script.
- When run with the **–F <FILE>** option, runme.sh runs only the OS-specific scripts given by <FILE>. This allows you to runs any subset of scripts you desire by simply listing them in a file. When specifying the **–F** option the file format must be a 7-bit ASCII text file with UNIX -style newline characters. The OS-specific scripts must be listed one per line, as in the following example:

```
GEN000020
GEN000400
GEN000440
```

Each OS-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 will write two files GEN000020.detect.log and GEN000020.results.

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

Once created, the files with the **.results** extension are read by a Fixlet message and the result becomes available through the BigFix Console. The Fixlet messages examine the [STATUS] section to determine relevance.

An example of a results file is shown below:

```
[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]
[CONTROL_COVERAGE]
DISA-STIG-GEN000020
[CONTROL_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]
```

Section Name	Description
[RUN_DATE]	Contains the date that the script was run.
[DESCRIPTION] and [FIXLET_DESCRIPTION]	Not applicable to this discussion.
[CONTROL_COVERAGE]	Contains the names of the regulations to which this Fixlet message applies.
[STATUS]	Used by the associated Fixlet message 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 message will become relevant.
[PARAMETERS]	Contains the parameters associated with the script (spaces will display as ‘;’).
[TIMETAKEN]	Contains the number of seconds of wall-clock time that the script took to execute.
[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 BigFix 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**, looks like the following:

```
TOTAL_SCRIPTLETS_RUN:69
TOTAL_SCRIPTLETS_PASS:33
TOTAL_SCRIPTLETS_FAIL:36
TOTAL_SCRIPTLETS_NA:0
TOTAL_SCRIPTLETS_ERR:0
TOTAL_TIME_TAKEN:1367
```

Setting UNIX Fixlet Parameters

The BigFix UNIX SCM **checklist** sites come pre-configured with default values for various operating system settings according to a designated standard. However it is possible to customize your deployment to meet the specific settings required by your organization. This is done by modifying the parameters passed to the UNIX controls. A list of the UNIX Parameters is contained in the OS-specific ***BigFix SCM Parameter*** documents. This section explains how to adjust them.

NOTE: The steps outlined below must be followed *before* executing the **Deploy and Run Security Checklist** task that is included in the respective SCM site. Otherwise, your custom parameters will be ignored.

In order to customize the parameters of a control, you create and maintain a text file on each machine that contains one line for each control you wish to override. The line must contain the name of the control, the parameter(s) to customize and the new value. It will be of the form:

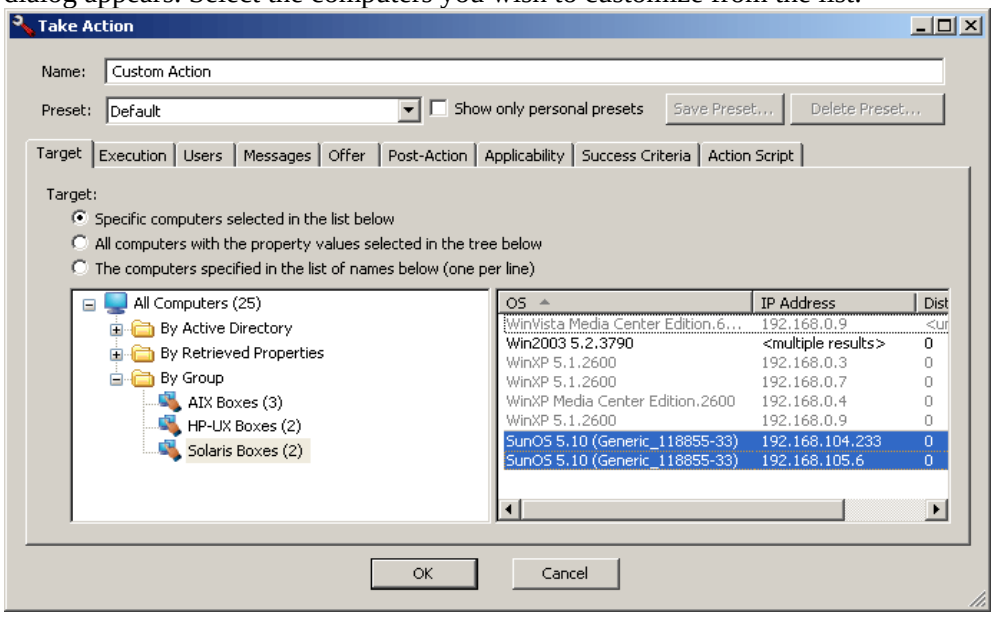
```
CONTROL_ID:PARM_NAME=PARM_VALUE
```

For example, if you wish to specify a minimum length of 6 and one alphabetic character in each password, you will need to customize two controls. The file would therefore have two lines, one per control:

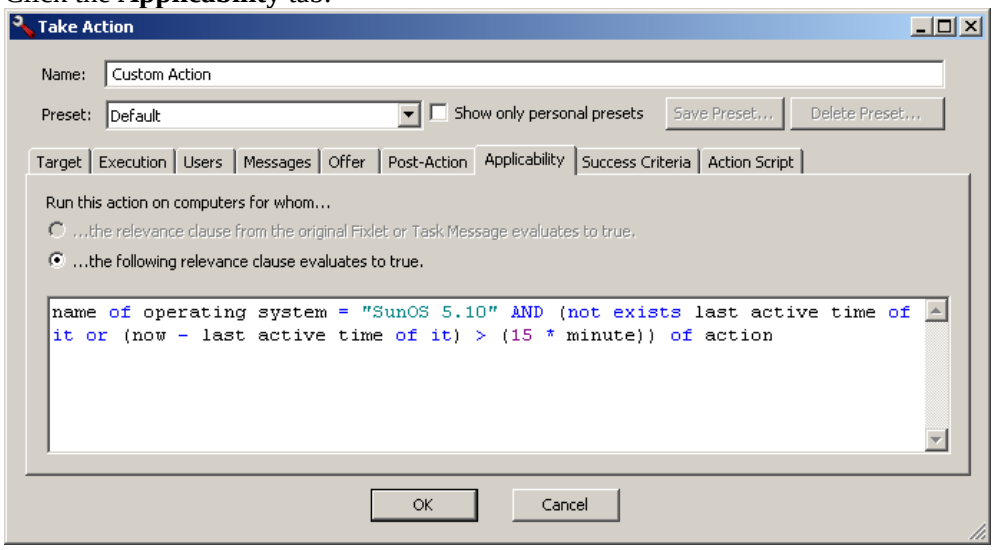
```
GEN000580:VALUE=6
GEN000600a:VALUE=1
```

Here, the name of the parameter is VALUE. The various ***BigFix SCM Parameter*** guides discuss the individual controls, their parameter names and the default values of each. Consult those documents to see which controls can be parameterized and their default values. The basic steps for parameterization are as follows:

1. Begin by creating a custom Action which you will use to create and deploy the override file to the appropriate endpoints. To do this, select **Custom Action** from the **Tools** Menu. The Take Action dialog appears. Select the computers you wish to customize from the list.



2. Click the **Applicability** tab.

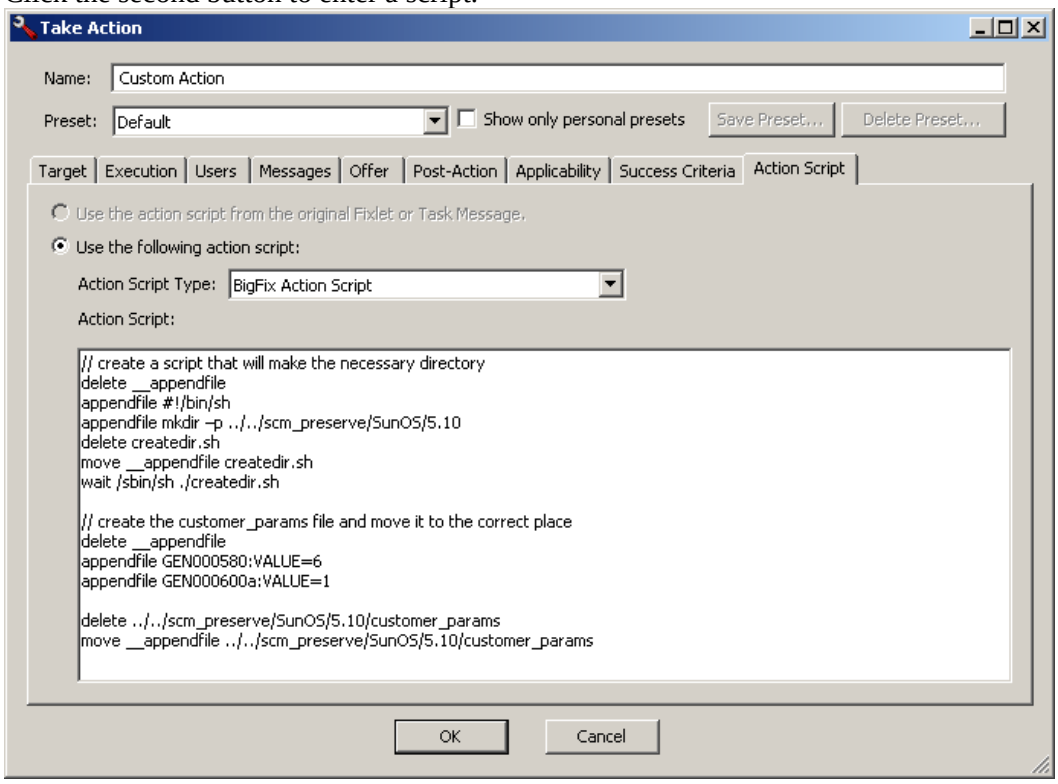


Click the second button to run the action on computers with a custom relevance clause. In the text box, enter following relevance expression:

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

This will restrict the action to Solaris 10 systems and ensure the task reapplies successfully if reapplication behavior is specified on the execution tab.

3. Click the **Action Script** tab to create a script that will copy the file onto the target computers. Click the second button to enter a script.



Insert a script in the text box to create the target directory with the file containing your custom parameters. The script must then move the file into the appropriate directory. Here is a sample script that would customize the password parameters as discussed previously:

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

// create the customer_params file and move it to the correct place
delete __appendfile
appendfile GEN000580:VALUE=6
appendfile GEN000600a:VALUE=1

delete ../../scm_preserve/SunOS/5.10/customer_params
move __appendfile ../../scm_preserve/SunOS/5.10/customer_params
```

Customizing UNIX Deployment

When you run the shell script **runme.sh** from the **Deploy and Run Security Checklist** task (included in the SCM site) it uses the **-g** option by default. This runs a program called **globalfind** that creates a directory listing of files on the system using the find command. The script then saves this list in a file called **find.out**. Many of the individual OS-specific scripts require access to this file.

By default the globalfind program will exclude the following file system types from its search:

```
cdrfs procfs ctfs fd hsfs proc mntfs smbfs iso9660 nfs msdos
```

It will also exclude any directories named lost+found. In order to provide more granular control over the directory listing, you can modify these default parameters:

- **EXCLUDEFS** – This must be a space-separated list of all the file system types to exclude from the search.
- **EXCLUDEMOUNTS** – This must be a space-separated list of all the file system mounts to exclude from the search. 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”
  ```

  This will prevent the shared file system from being scanned from multiple systems.
- **EXCLUDEDIRS** – Any directory names specified in EXCLUDEDIRS will be omitted from the directory listing.

NOTE: When you exclude a directory, you exclude all similarly named directories as well. For instance, if you specify EXCLUDEDIRS=”foo/”, you also exclude /foo/usr/foo and /usr/local/foo.

The default parameters are:

```
globalfind:EXCLUDEFS="cdrfs procfs ctfs fd hsfs proc mntfs smbfs
iso9660 nfs msdos";EXCLUDEMOUNTS="";EXCLUDEDIRS="lost+found"
```

To take advantage of these exclusions, include a line like the one above in your parameter file, as discussed previously.

Scheduling Specific Controls

The default behavior for UNIX SCM deployment is to run the scripts as a single batch, as described previously. However, you can also run any subset of the controls on your own defined schedule. Each time you do, the batch you deploy will overwrite any previous batch commands. As described previously in , the runme.sh master script provides a '-F' option which takes a file name as its argument. It has the following form:

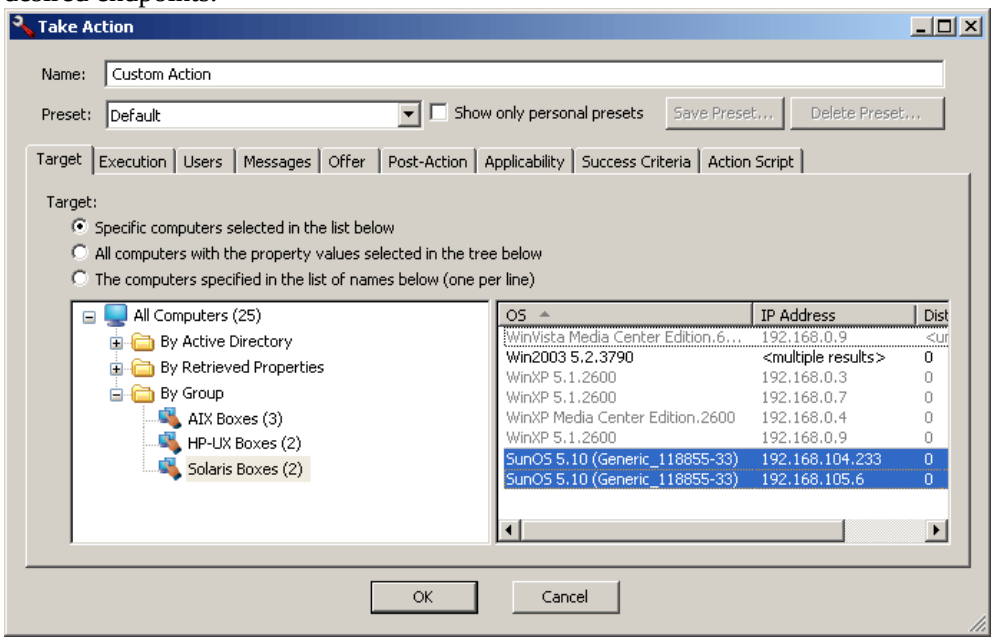
```
./runme.sh -F <FILE>
```

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

```
GEN000020
GEN000480
GEN000560
…
```

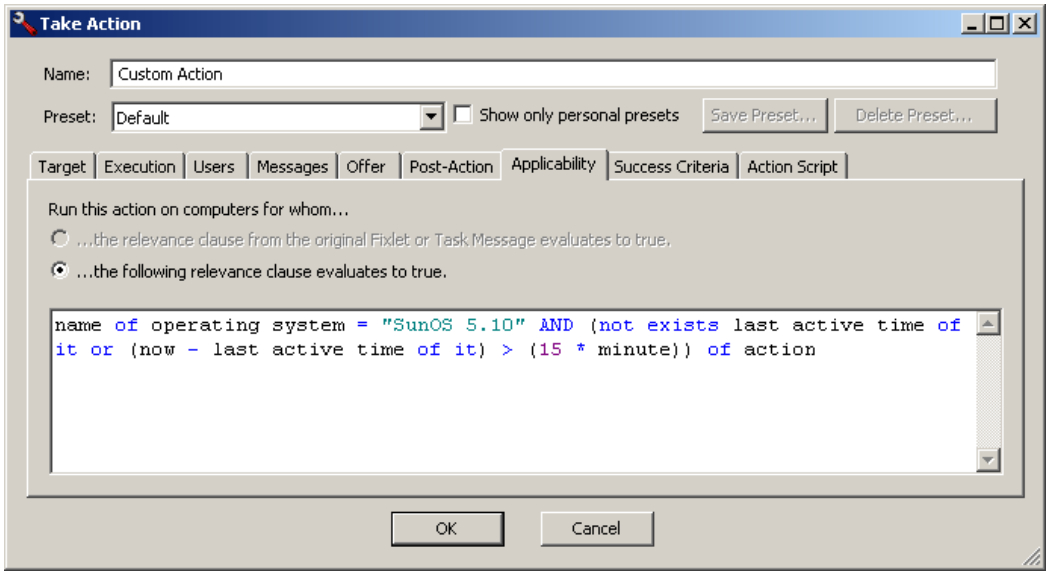
This allows you to run just the scripts you desire, when you desire. To enable this functionality, you need to create a Custom Action. This Action will create the file containing the list of controls and then deploy it to the desired BigFix Clients. This action is similar to the creation of a custom parameter file. To create your own custom set of controls, follow these steps:

1. Select **Custom Action** from the **Tools** Menu to bring up the **Take Action** dialog. Choose your desired endpoints.

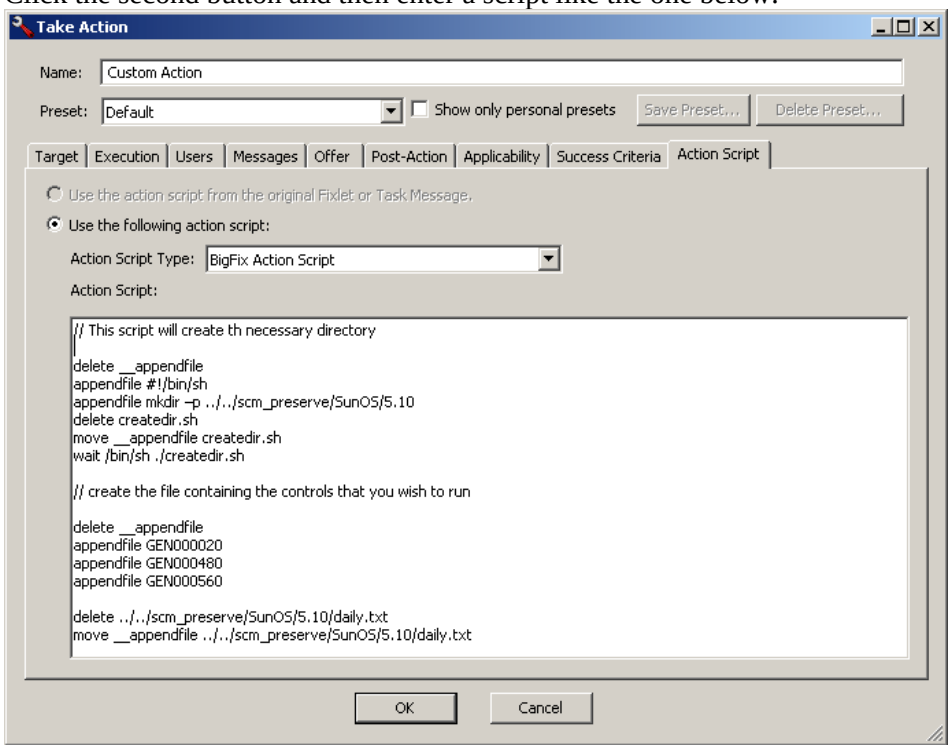


2. Click the **Applicability** tab and then click the second button to run this Action on computers with a custom Relevance clause. In the text box, enter a Relevance clause to identify the desired subset of computers you wish to target. For instance, to restrict the action to Solaris 10 systems, you would 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
```



3. Click the **Action Script** tab to create a script that will copy your file onto the target computers. Click the second button and then enter a script like the one below.

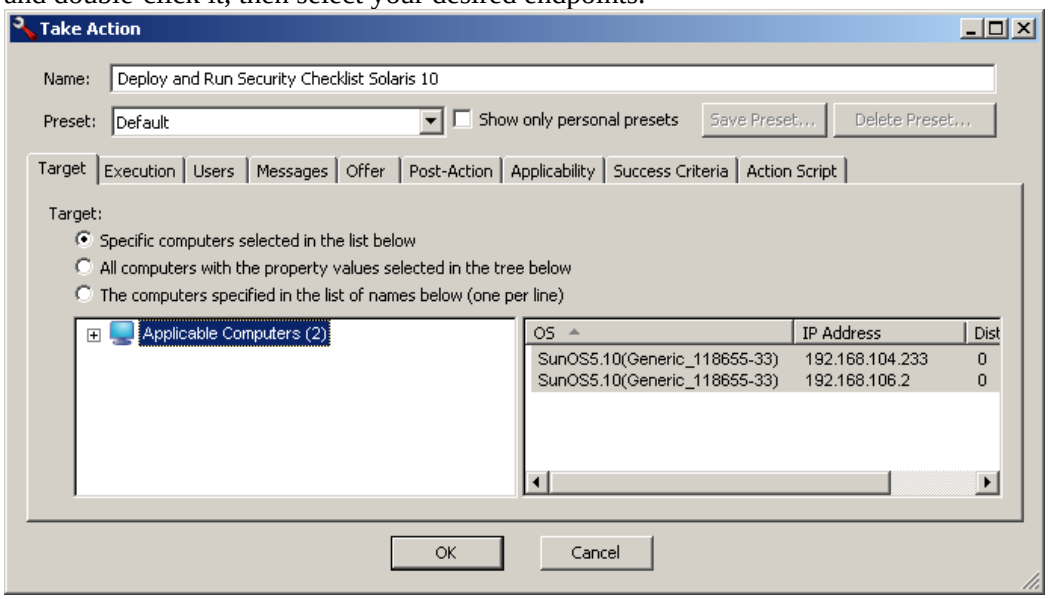


This script creates the target directory with the file containing the controls you wish to run and then moves the file into the appropriate directory. Here is a sample script (that you can copy and paste) that specifies three controls, GEN000020, GEN000480 and GEN000560:

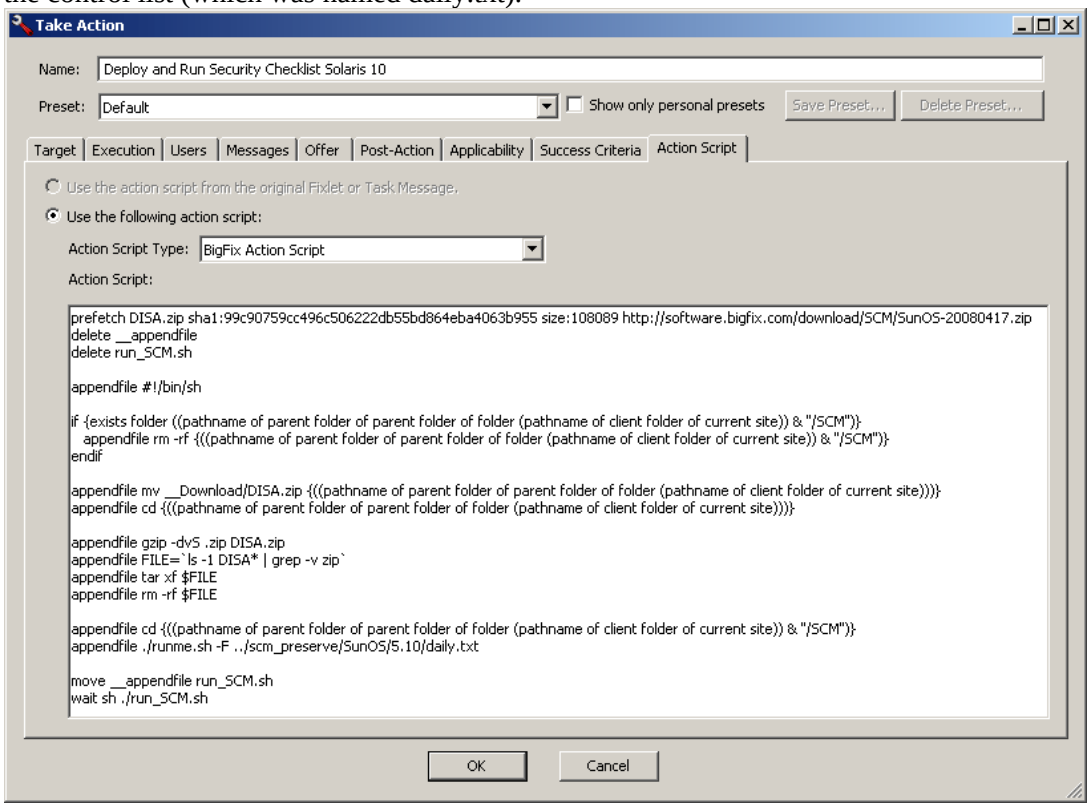
```
// create a script that will create the necessary directory
delete __appendfile
appendfile #!/bin/sh
appendfile mkdir -p ../../scm_preserve/SunOS/5.10
delete createdir.sh
move __appendfile createdir.sh
wait /bin/sh ./createdir.sh

// create the file containing the 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
```

4. Execute the runme.sh script with the –F option. The easiest way to do this is to modify the **Deploy and Run Security Checklist Solaris 10** task that comes with the content. Find this task and double-click it, then select your desired endpoints.



5. Modify the Action Script to make runme.sh use the –F option and point to the file that contains the control list (which was named daily.txt).



Here is a sample script that you can copy, paste and modify:

```
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
```

6. Click OK and enter your Private Key Password to execute the Action.

NOTE: Several controls make use of the globalfind utility and require a fresh find.out file to work correctly. If you are running one or more of the following controls you *must* supply the '-g' option to runme.sh.

The following controls require the global option, and may be included with the '-F' option only if the '–g' is also supplied.

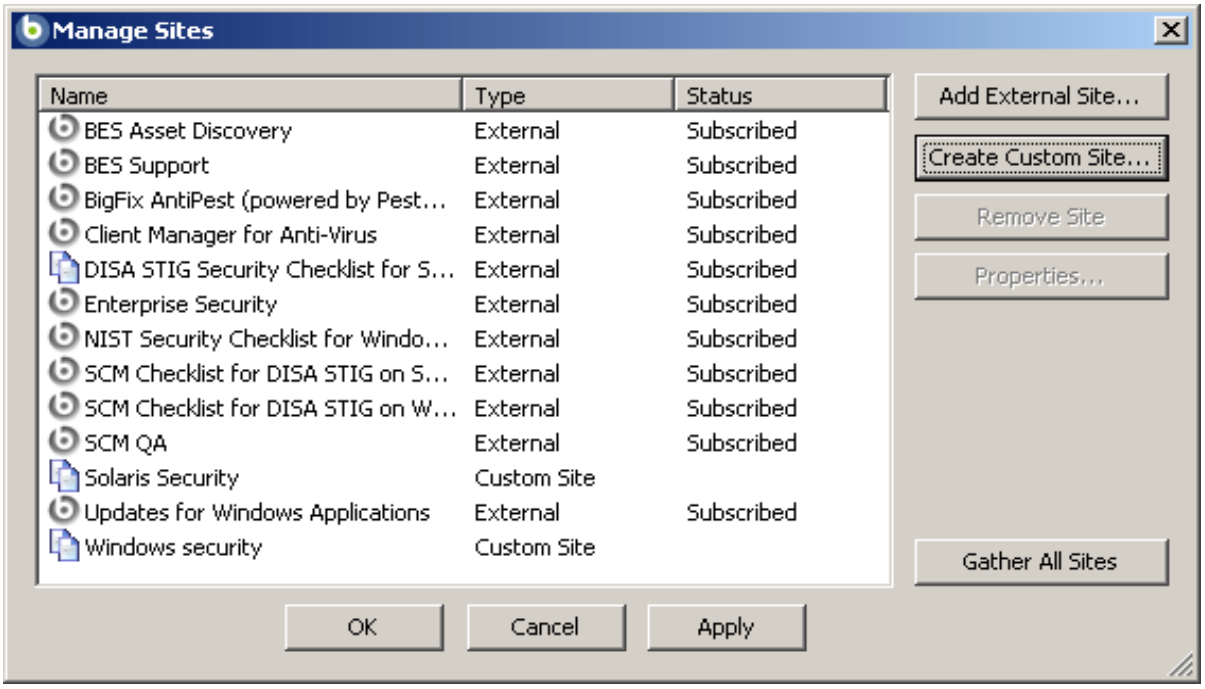
GEN001160	GEN001200	GEN001220	GEN001240
GEN001260	GEN001280	GEN001300	GEN001360
GEN001540	GEN001560	GEN002160	GEN002180
GEN002200	GEN002220	GEN002240	GEN002280
GEN002480	GEN002500	GEN002520	GEN002540
GEN006340	GEN006360		

Leveraging SCM Sites

The ability to customize SCM parameters and exclude specific computers from analysis gives you a great deal of control over your security posture. However, you can go even farther by creating custom sites and repurposing the SCM checklists 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 craft your own policy with custom sites, follow the four-step process summarized here. You will find a more detailed explanation immediately following this section.

Step 1: Create a Custom Site

To create a custom site, select **Manage Sites** from the **Tools** menu.



Click the **Create Custom Site** button and provide a name for your site. From the **Site Properties** dialog, provide a description and assign permissions that enable other console operators to work with the site. Once your custom site is created, subscribe the desired BigFix Clients to the site in order to assess them against your configuration policy. If they are not in compliance, you can then opt to remediate them.

NOTE: Although there is a built-in Baseline feature in the BigFix Console, BigFix SCM is best managed using custom sites. Custom sites let you subscribe precisely defined sets of computers and devices to just the content you desire. That allows your statistics to be properly evaluated against the selected group, properly excluding those computers where the policies are not relevant.

Step 2: Copy the Desired Fixlet Messages into the Custom site

Once you have created your custom site and assigned ownership/writing/reading permissions and subscribed endpoints, you can begin to populate it with Fixlet messages. Create custom copies of Fixlet messages from the sites that you received from BigFix, and place them into your custom site. There are two ways to copy Fixlet messages into your custom site:

- **One-by-one**: Simply right-click a Fixlet message and select **Create Custom Copy** from the context menu. In the dialog that appears, select the name of your custom site from the pull-down menu and click OK.
- **In Bulk**: This method is described in detail in the next section (), and is the recommended technique when you have many Fixlet messages to copy.

The Fixlet messages you copy into this custom site will define the security policies you wish to deploy to just those systems that require them.

Step 3: Customize Fixlet Messages using Parameters and Exceptions

Although you can use the SCM checklist sites straight out of the box, many companies will want to customize the content to suit their own corporate security policies. You can implement these changes to permit greater flexibility or to enforce tighter control. Either way, you can adjust the parameters of many of the Fixlet messages to accommodate your own level of comfort. Each site can have uniquely customized parameters, offering you a great amount of control over the deployment of your security policies. The method of setting a parameter varies between platforms:

- **Windows**: The Windows Fixlet messages have parameters available directly from a corresponding Task. Simply click the link to open the parameter Task and then select the appropriate link to provide a new value for the specified parameter.
- **UNIX**: On the UNIX side, control parameters can be supplied line-by-line in a straightforward text file. In addition, UNIX controls can be limited to specific file types and directories, helping you to fine-tune the actions and potentially improve performance. Once submitted, this file is evaluated at the endpoints and the results are quickly made available to the BigFix Console where Fixlet controls check the results for relevance and potential remediation.

Step 4: Subscribe the proper clients to the custom site

In order to get an accurate picture of the health of your network, you must ensure that you have subscribed your clients to the appropriate sites. Make sure your Windows clients are not subscribed to UNIX content and vice-versa. The goal is to subscribe a BigFix Client *only* to those sites that you wish to evaluate and no others. There are two ways to do this. One is to select individual computers from the **Computer** tab and from the right-click context menu, select **Modify Custom Site Subscriptions**. From the dialog that opens, click the first button to subscribe and choose your custom site from the pull-down menu. After you provide your password, an Action is deployed to manage the subscription.

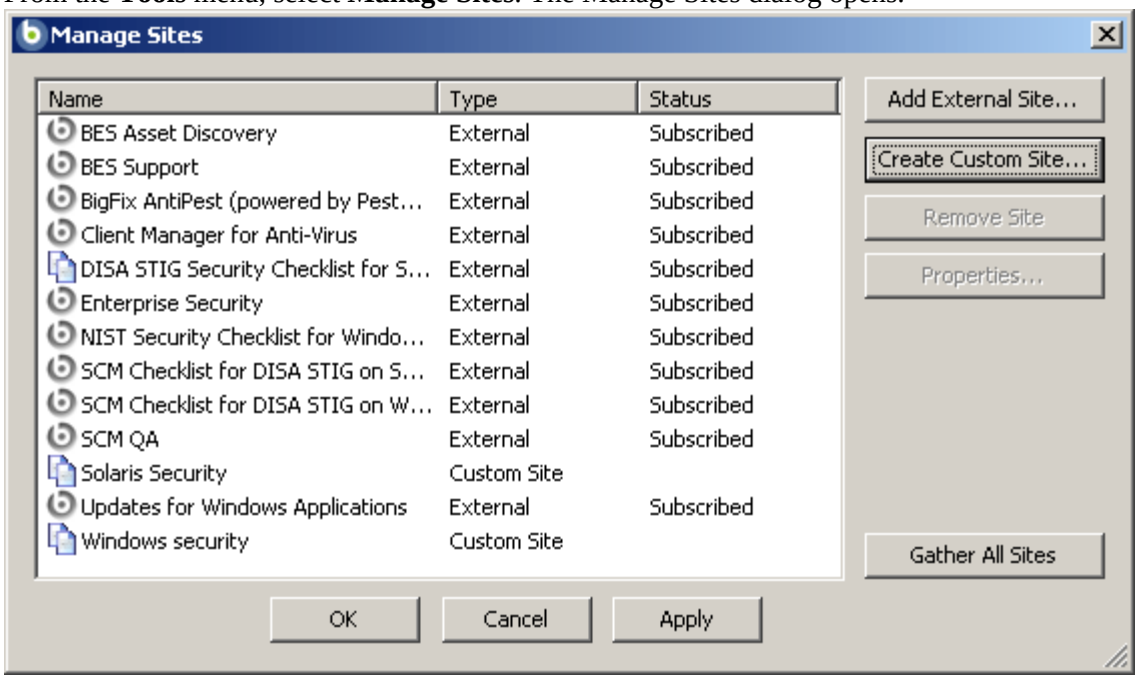
The second method is more flexible. Go the Action tab and select the subscription Action you made using the first technique. Right-click to **Export** it and then double-click to import it back into the Console. From the **Take Action** dialog, select the second button to target the subscription Action by **Retrieved Properties**. Select the desired property (typically the OS) and click OK to propagate the Action. This technique is preferred, because it will automatically recruit any new computers you add to the proper site. Both of these techniques are described in greater detail later in this guide.

If you do not properly target your endpoints, you will get spurious compliance metrics. The next few sections go into greater detail on creating and managing custom sites.

Creating Custom Sites

As you have seen, you can derive a great deal of power and convenience by grouping Fixlet content into custom sites. Once you have defined a custom site, you might also want to incorporate security-based Fixlet controls from other sites. For instance, BigFix AntiPest or 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:

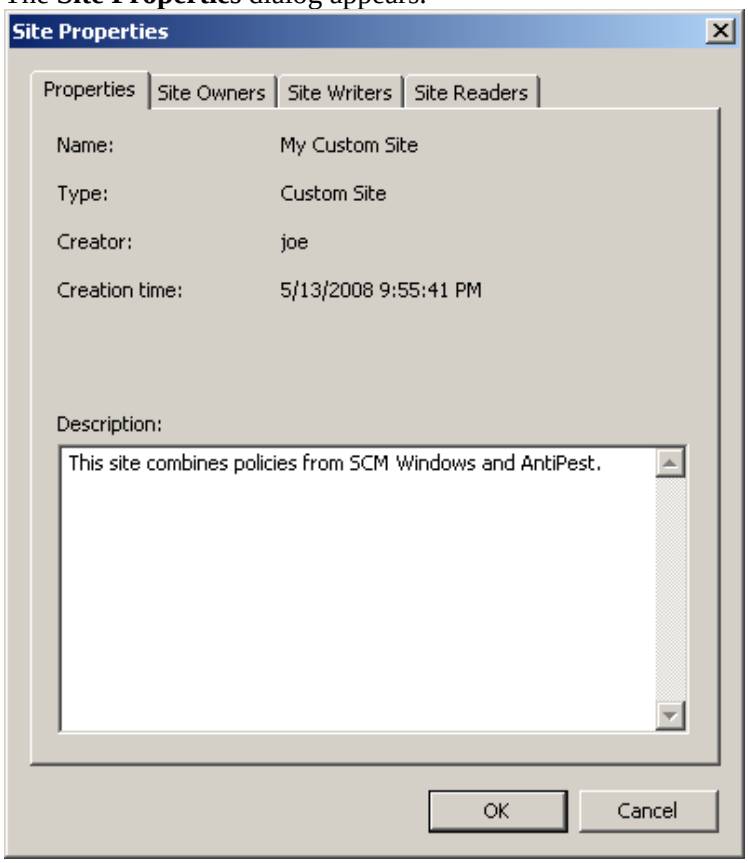
1. From the **Tools** menu, select **Manage Sites**. The Manage Sites dialog opens.



2. Click the button labeled **Create Custom Site**. The Create Custom Site dialog opens.

3. In the dialog box that appears, enter the name of your site. Do not check the box to **Create a policy action that will subscribe all computers to this Custom Site by default**.

4. The **Site Properties** dialog appears.



Enter a description of your site in the text box.

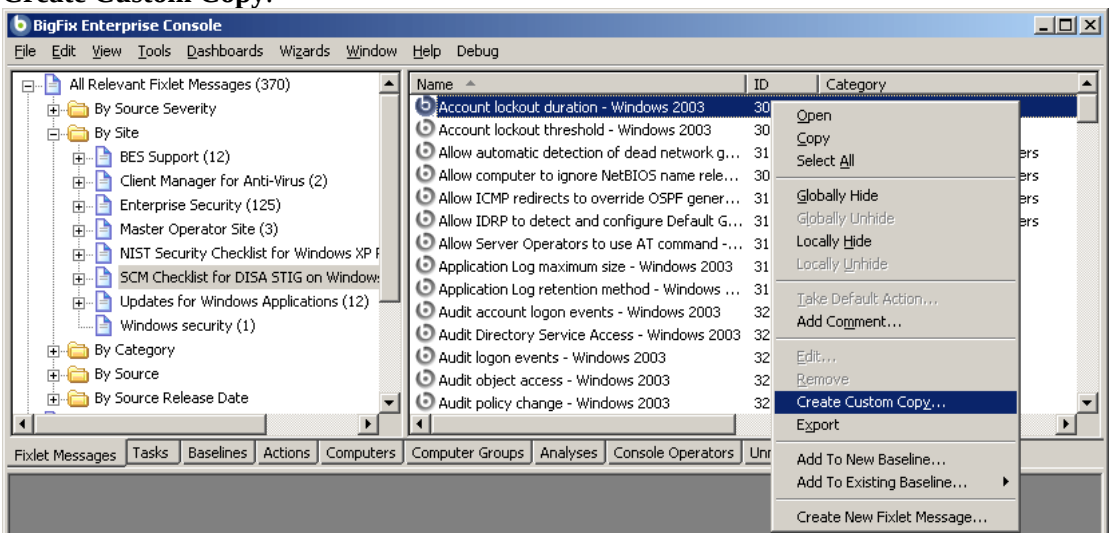
5. Click on the other tabs to set **owner**, **writer** and **reader** permissions for this site, then click **OK**.

6. From the **Manage Sites** dialog, click **OK** to propagate your new site. You will need to provide your user password.

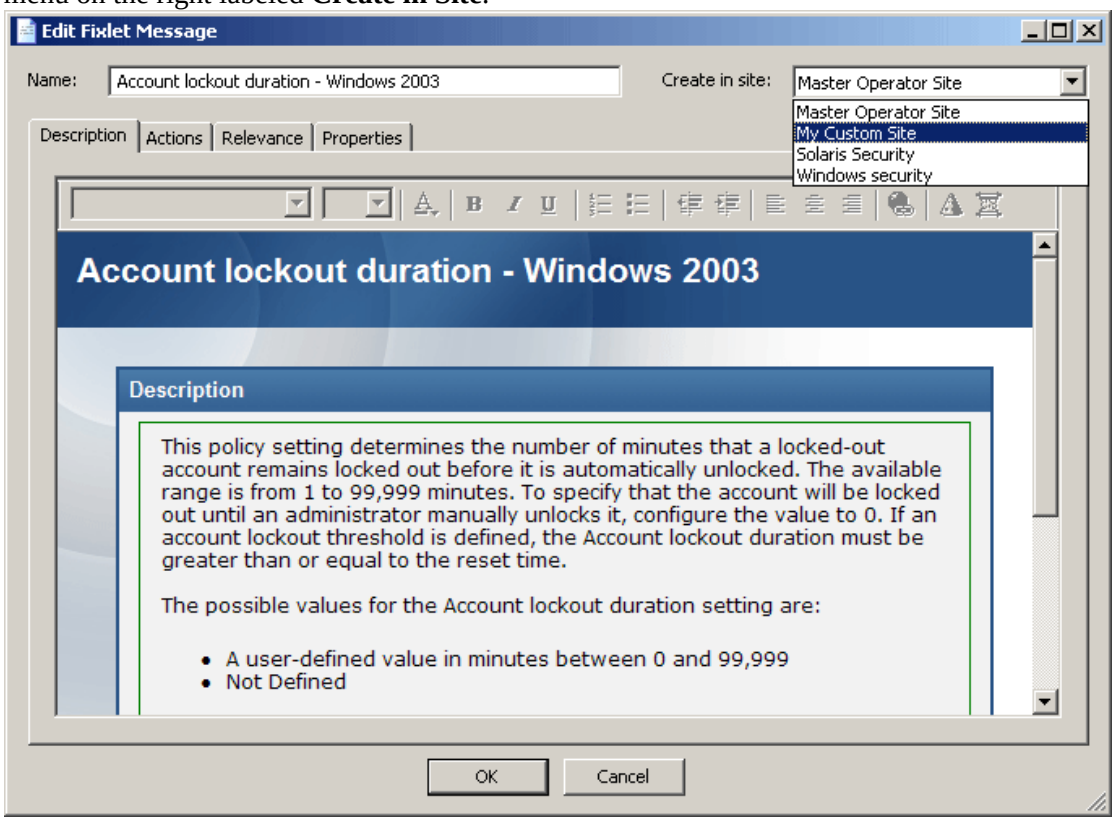
Copying and Customizing Content for Custom Sites

Now that you have a custom site, you need to populate it with Fixlet messages and Tasks. To add content from SCM sites published by BigFix one at a time:

1. Simply click on any item in the Fixlet list, right-click it to bring up the context menu, and select **Create Custom Copy**.



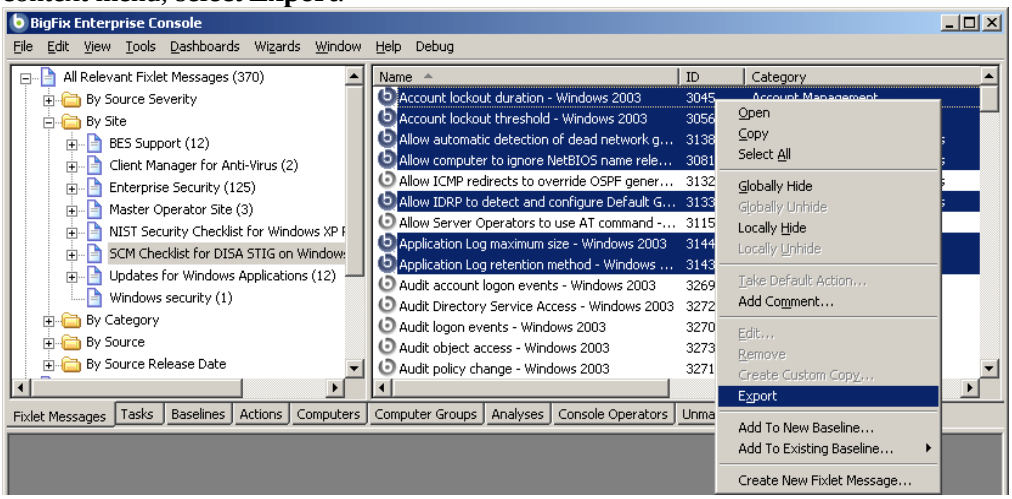
2. From the **Edit Fixlet** message dialog that appears, select your custom site from the pull-down menu on the right labeled **Create in Site**.



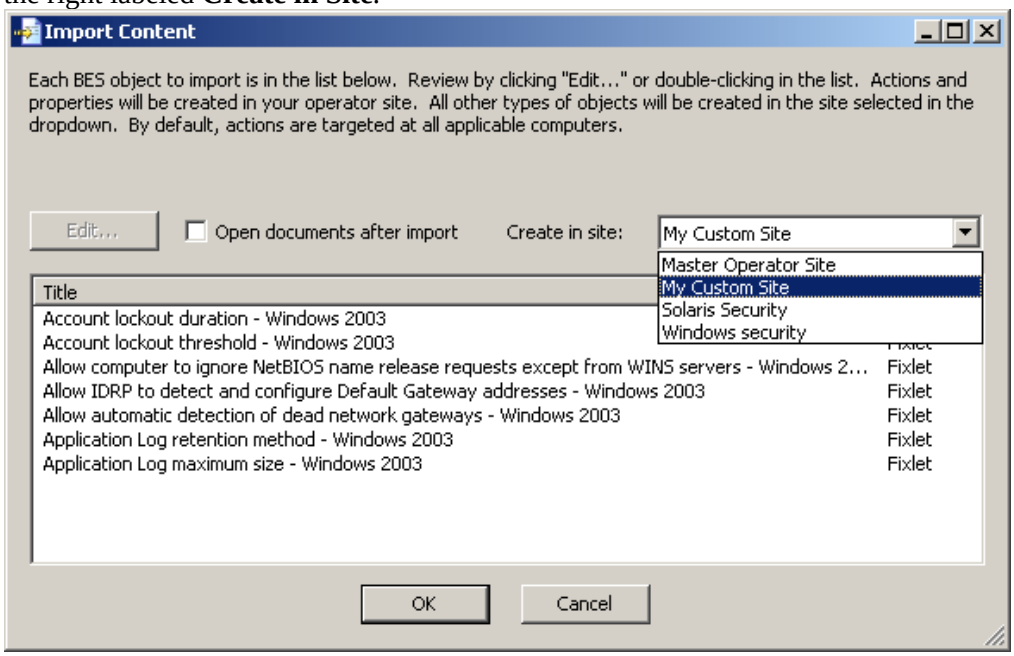
3. Customize the Fixlet message, if desired, by changing its parameters, as described in the previous sections.
4. Click **OK** and enter your password.
5. Repeat this process for each Fixlet message you wish to place in your custom site.

To add content from BigFix SCM sites as a batch:

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



2. The **Save As** dialog opens. Select a pathname for the file and save it.
3. In the Windows file system, locate the saved **.bes** file and double click to import it.
4. From the Import Content dialog that appears, select your custom site from the pull-down menu on the right labeled **Create in Site**.



Click **OK** and enter your password to complete the process.

To add content that is not part of a BigFix SCM site:

1. Select the Fixlet messages or Tasks you would like to move and then right-click the set. From the context menu, select **Export**.
2. The **Save As** dialog opens. Select a pathname for the file and save it.
3. Open the exported **.bes** file using a text editor. Note that it is an XML document.
4. On the line below every <SourceSeverity></SourceSeverity> tag, add a section like this:

```
<MIMEField>
      <Name>x-fixlet-scm-category</Name>
      <Value>Application Log</Value>
</MIMEField>
<MIMEField>
      <Name>x-fixlet-scm-control</Name>
      <Value>NIST</Value>
</MIMEField>
<MIMEField>
      <Name>x-fixlet-scm-id</Name>
      <Value>NISTSecurityChecklistforWindowsXPProfessional_3100</Value>
</MIMEField>
<MIMEField>
      <Name>x-fixlet-scm-os</Name>
      <Value>Windows XP</Value>
</MIMEField>
```

   These are Name/Value pairs that attach extra information to each Fixlet message. In essence, you are adding category, control, id and OS information to make the Fixlet message conform to SCM rules. Refer to other exported SCM checklists for good examples. The <Value> sections here are examples only. You will want to enter appropriate values for each Fixlet message you add.

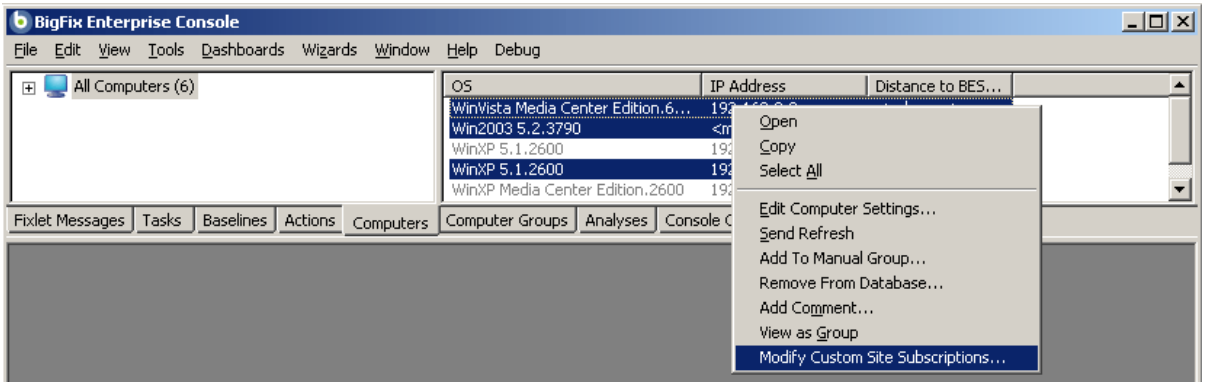
5. After editing the XML to add the tags above, save the **.bes** file and then double click to import it into the BigFix Console.
6. From the **Import Content** dialog that appears, select your custom site from the pull-down menu on the right labeled **Create in Site**. Click **OK** and enter your password.

Subscribing Computers to Your Custom Site

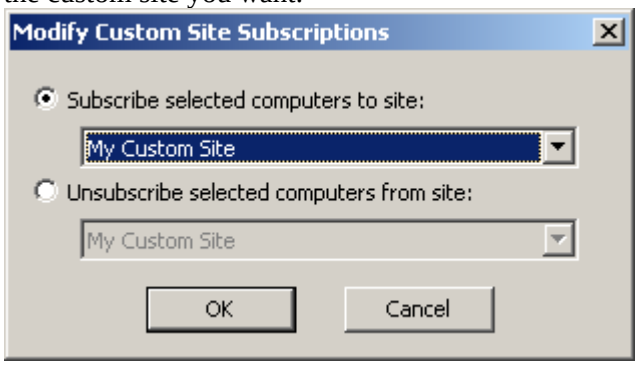
Now that you have created your custom site, you need to subscribe computers to it. Remember that the proper collection of statistics depends on targeting the content to the appropriate computers. Make sure that Windows computers are subscribed to Windows content only, and the same goes for UNIX systems.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

Subscribing Specific Computers

1. Click the **Computer** tab. From the list of computers, select the clients you want to add to the subscription list.
2. Right click on the selected computers and choose **Modify Custom Site Subscriptions** from the context menu.



3. Click the first button to **Subscribe selected computers to site**. From the pull-down menu, select the custom site you want.



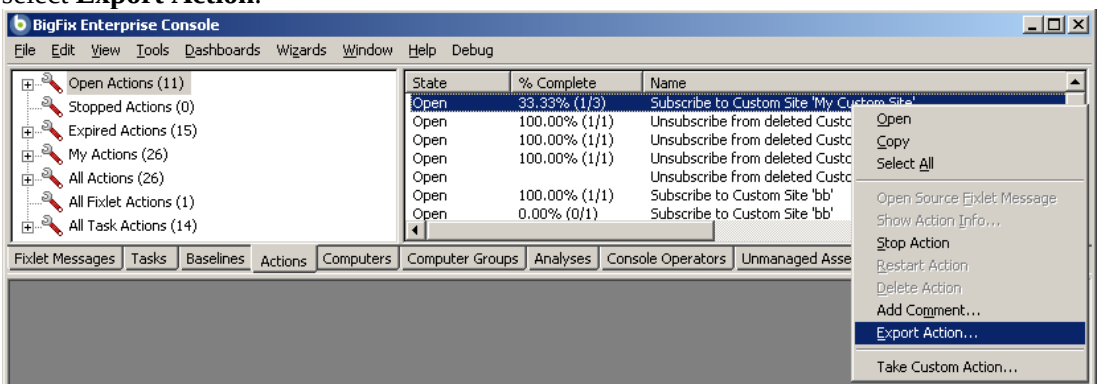
Note that you can also unsubscribe computers from this interface.

4. Click **OK** and then enter your password to complete the subscription process.

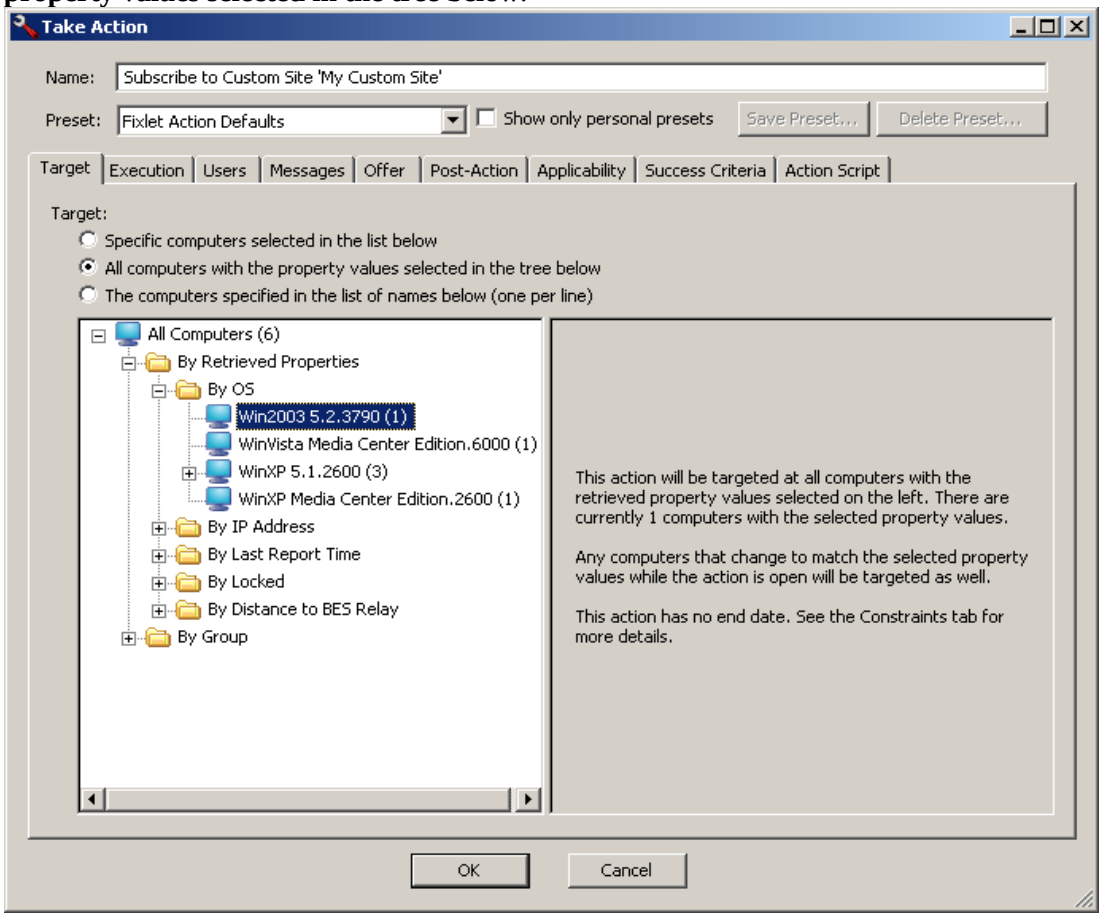
Subscribing by Properties

The previously described method of subscribing specific computers is simple and straightforward, but lacks flexibility. Each time you add a new computer to your network, you need to subscribe it to the appropriate SCM site. Targeting computers by their properties is a much better technique for controlling site subscriptions. This way, whenever a computer is added, its OS (or other characteristic) will be examined and it will automatically be subscribed to the appropriate site. Here is how:

1. Follow the steps described previously to subscribe a computer to the desired site (since we are going to modify the targeting, it does not matter which computer you select). This creates an action that you can find by clicking the **Action** tab.
2. From the Action list, right-click the subscription Action you just created. From the context menu, select **Export Action**.



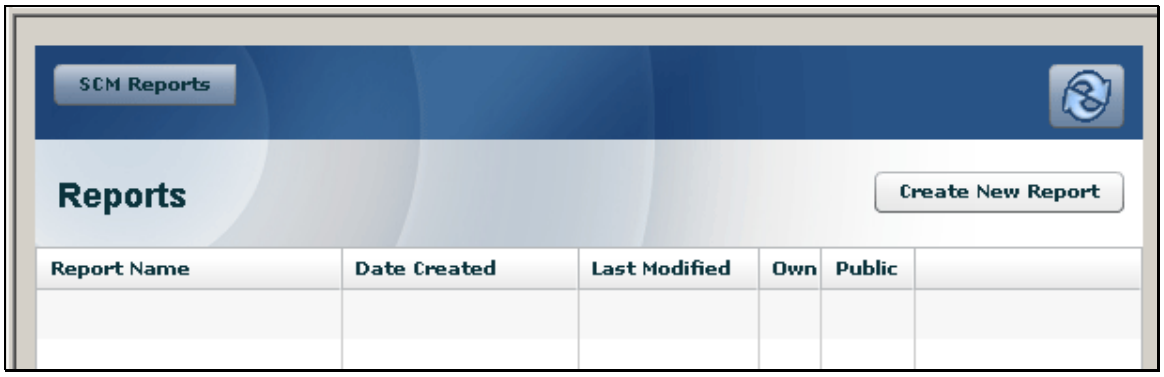
3. From the **Save As** dialog, choose a name and a location to save the exported Action as a **.bes** file.
4. From the Windows file system, locate the exported Action file and double-click it. This opens the **Take Action** dialog in the Console.
5. From the Target tab of this dialog, click the second button labeled **All computers with the property values selected in the tree below**.



6. Open the **All Computers** tree and the **By Retrieved Properties** folder beneath it. From the list of properties, select the ones you want to use to target your computers. Typically, you will find the **By OS** folder most useful, but you may have other criteria that you prefer. Select the desired property (for instance, Win2003) to complete the targeting.
7. Click **OK** to deploy this new subscription Action and then provide your password to propagate it.

Using the SCM Dashboard

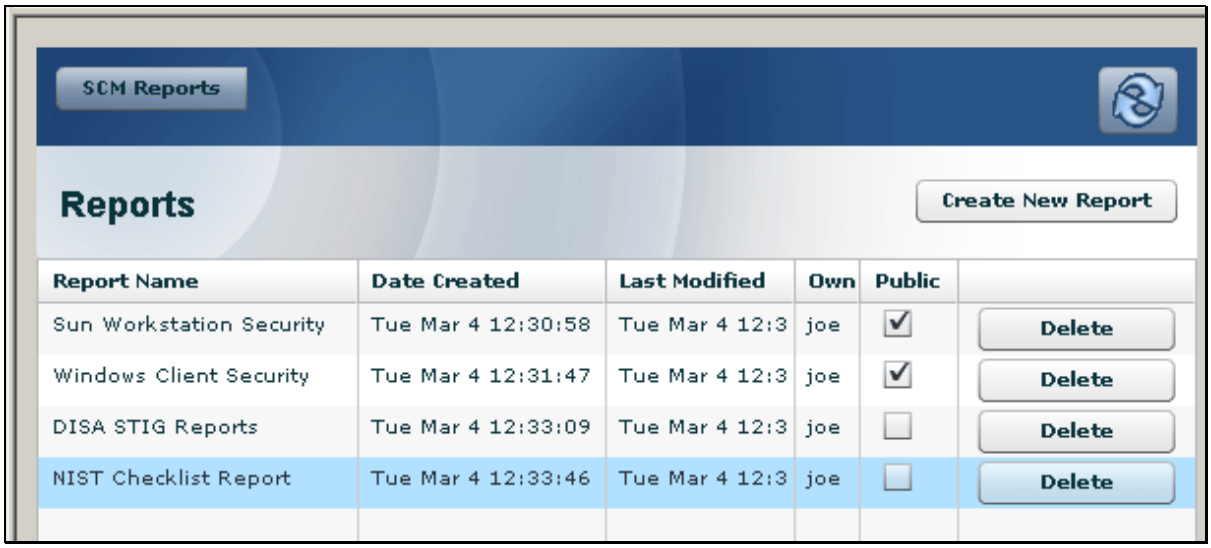
When you subscribe to the SCM Reporting site, a Dashboard is installed that lets you view graphic representations of your current security configuration. Under the **Dashboard** menu, select **Security Configuration Management**. If this is the first time you have viewed the SCM Dashboard, there will be an empty list:



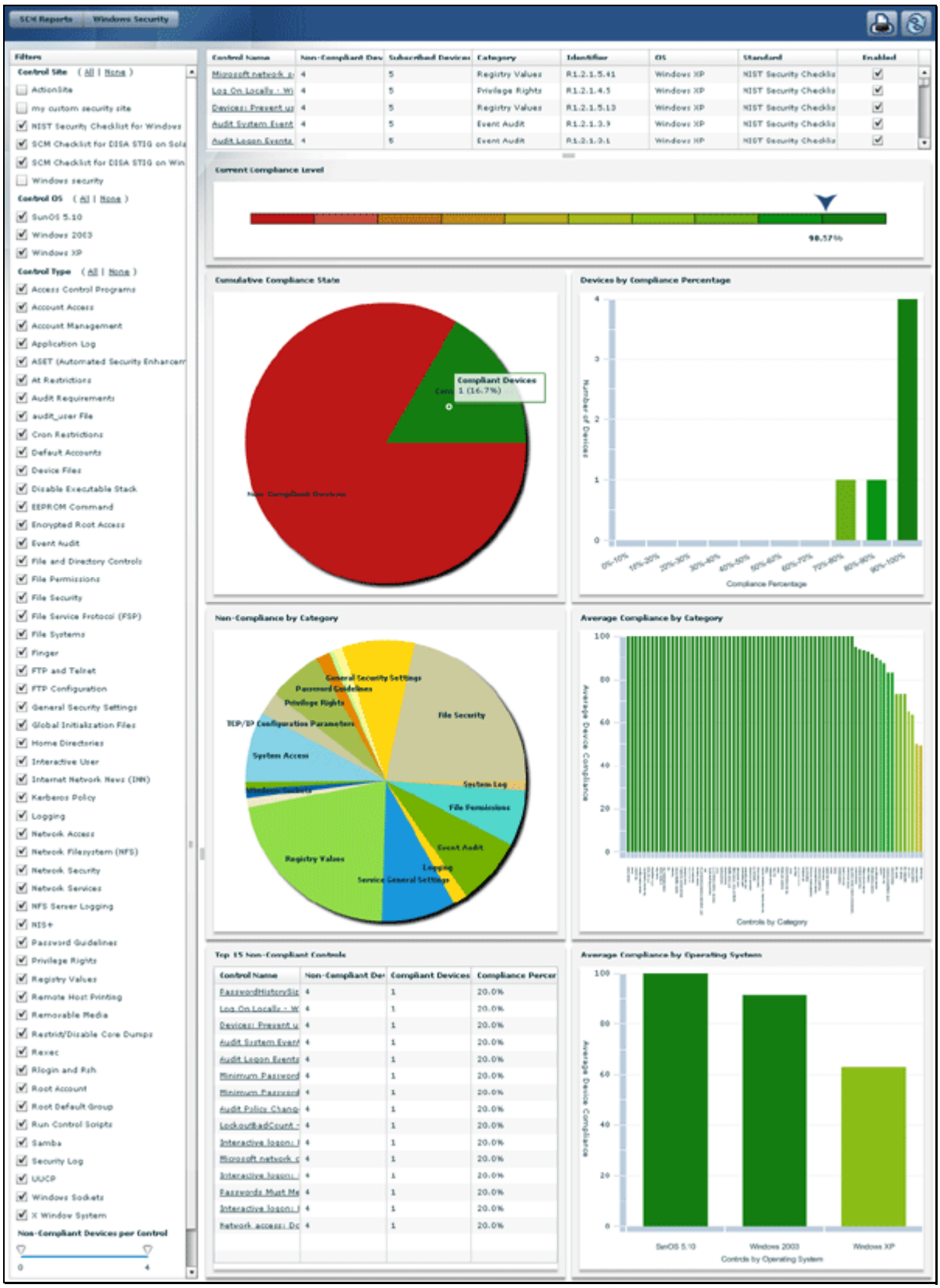
Click on the **Create New Report** button in the upper-right corner of the Dashboard to name and then view a default report. The Dashboard provides the tools you need to easily customize your report and narrow the scope to a more manageable set of issues. You might, for instance, create separate reports that correspond to different standards, or target subsets of machines that have unique compliance requirements.

At any point, you can click on the refresh button at the top right of the screen to ensure that you are viewing the most recent data.

If you have already saved some reports, they will be listed here. This opening screen also allows you to define them as public or private (with the same meaning as Web Reports), delete them or load them for viewing or further modification.



Simply click a report to view it. Select a saved report or create a new one. When you open a new report, a default SCM Dashboard appears in the work area.



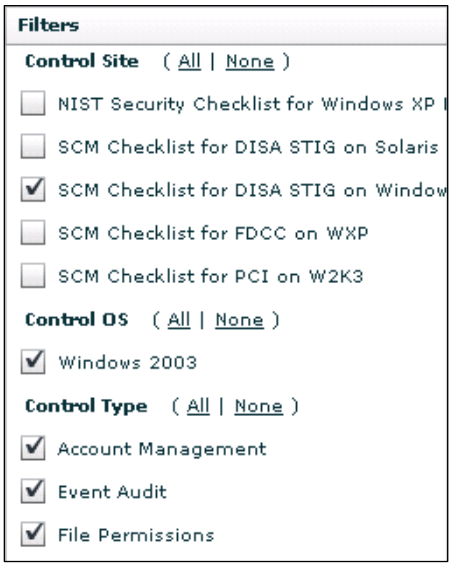
The SCM Dashboard

The Dashboard provides a detailed up-to-date overview of your entire network. You can configure and filter the Dashboard to fine-tune the view. The Dashboard can then be saved as a custom report or printed. The typical workflow will take you through these basic steps:

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 following sections of this guide will expand on each panel.

Filter Panel



On the left side of the Dashboard is a filter panel that lets you select or deselect specific Control **Sites**, **OS**es and **Types**. You can click in the checkboxes next to each item or click on the **All** or **None** links to effect mass changes.

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. The Dashboard examines all your site subscriptions for inclusion in this security report.

The OS check boxes let you filter the content by operating system, so you can monitor controls targeting each individual operating system independently or view them in aggregate.

The Type filter lets you winnow down the control list by the type of control. These types correlate to the Category column in the corresponding control Fixlet list.

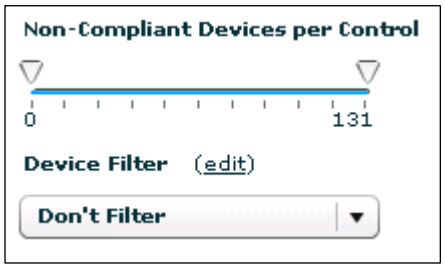
Control List

The SCM Dashboard lets you visualize your corporate compliance with the hundreds of security controls that are selected based on the filter criteria. These are shown at the top of the window:

Control Name	Non-Compli	Subscribe	Category	Identifier	OS	Standard	Enabled
Remote consoles	0	1	Root Account	GEN001000	SunOS 5.10	SCM Checklist for DISA STIG	☑
Root home directory	0	1	Root Account	GEN000900	SunOS 5.10	SCM Checklist for DISA STIG	☑
Home directory Ownership	0	1	Home Directories	GEN001500	SunOS 5.10	SCM Checklist for DISA STIG	☑
at.allow Group Ownership	0	1	At Restrictions	GEN003460b	SunOS 5.10	SCM Checklist for DISA STIG	☑
Root shell location	0	1	Root Account	GEN001080	SunOS 5.10	SCM Checklist for DISA STIG	☑
Dedicated Hardware for Routing	0	1	Unix Routing Vulne	GEN005580	SunOS 5.10	SCM Checklist for DISA STIG	☑
Sendmail DECODE Command	0	1	Sendmail or Equiva	GEN004640	SunOS 5.10	SCM Checklist for DISA STIG	☑
Printer configuration file permissions	0	1	Remote Host Printir	GEN003940	SunOS 5.10	SCM Checklist for DISA STIG	☑
Sendmail Help Command	0	1	Sendmail or Equiva	GEN004540	SunOS 5.10	SCM Checklist for DISA STIG	☑
NFS server logging	0	1	NFS Server Logging	SOL00400	SunOS 5.10	SCM Checklist for DISA STIG	☑
Run Control Scripts Group Ownership	0	1	Run Control Scripts	GEN001680	SunOS 5.10	SCM Checklist for DISA STIG	☑
Encrypted Communications IP Filtering and	0	1	SSH and Equivalent	GEN005540	SunOS 5.10	SCM Checklist for DISA STIG	☑

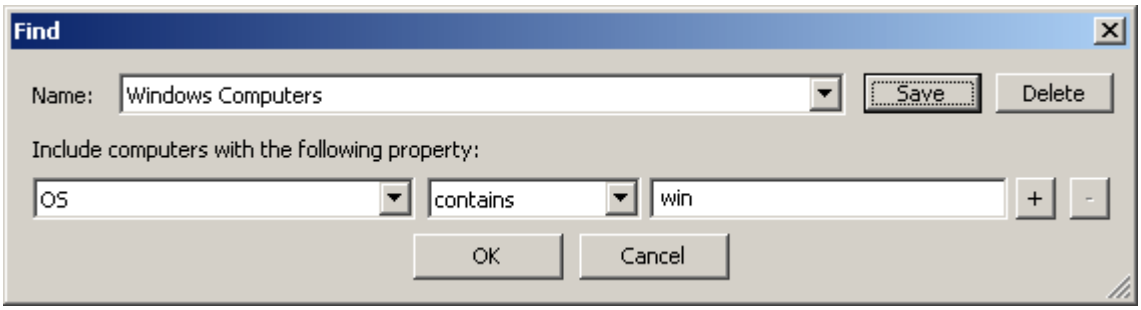
Each entry in this table refers to a security control. Click on the control name to bring up details about its intent and how it works. Click on the column header to sort the table by that field. Note that you can use the check boxes to enable or disable any of these controls to configure a custom security report. By default, all controls are enabled, but if you do not want to view compliance data on, say, password length, then you can disable those controls. Directly beneath this window is a grab icon that allows you to resize it.

Non-Compliant Devices



Below the Filter panel is a slider labeled **Non-Compliant Devices per Control**. It allows you to filter out controls based on the number of endpoints that are non-compliant to the control. For example, you may not care about controls that have less than 5 systems that are non-compliant, so you would set the left slider to 5. Conversely, you may have controls that are relevant on a very large number (or all) endpoints. In this scenario, you may know why these controls are non-compliant, and you wish to exclude them from the analysis. In this case you could set the right slider to filter out all controls that have more than X systems reporting non-compliant. In a case like this, you might also want to leave the control out of your custom content.

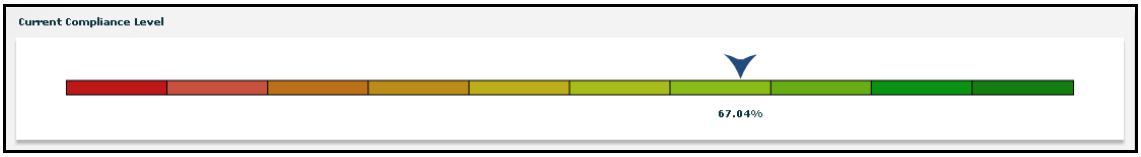
Below that is a pull-down list of specific computer filters. To define such a custom filter, click on the **edit** link next to **Computer Filters**. This brings up the standard computer **Find** dialog:



You can define a new computer filter here and click the Save button to add it to your list. These filters are available from the pull-down menu at the bottom of the Filter panel and give you extra control over the scope of the Dashboard view.

Current Compliance Level

Immediately below the Control List is an important summary graphic showing the overall compliance level for the specified set of controls and computers. It distills all the compliance information about the slice of the network you have chosen into a single number.



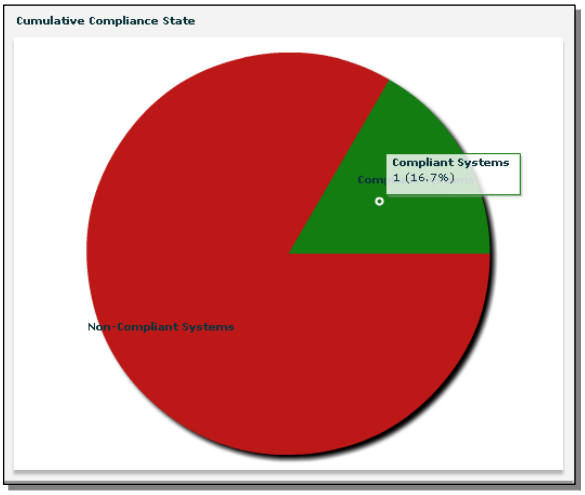
This composite number is an average of the individual scores from all the contributing computers.

NOTE: If a computer is subscribed to a non-relevant site (such as a Windows machine subscribed to a Solaris site) it will report spurious compliance. This can give you a much higher score on all measures, so make sure each computer is properly subscribed. This applies to all of the compliance graphs in the SCM Dashboard.

The Graphs

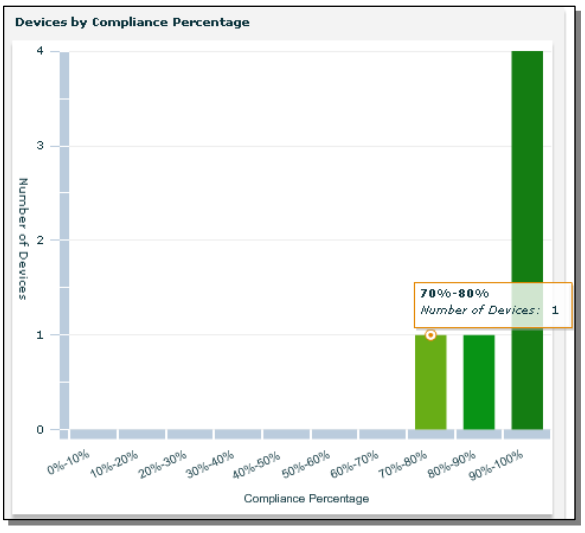
Below the overall compliance bar are several graphic displays. In each of these, when you roll your mouse over the constituent elements, a small window pops up to provide numeric detail. To drill down into the constituent data, simply click on the element. A table replaces the graphic with a detailed breakdown of that particular element. To view the graph again, click the button labeled **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. Here is a breakdown of each chart.

Cumulative Compliance State



This is a pie chart displaying the relative numbers of compliant and non-compliant computers. 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. Thus, this graph provides an instant view of the security of your enterprise, and the bigger the green section, the better. Click on either of the two pie sections to see the individual computers. The green section shows all the secured machines, while the red section provides a detailed look at each computer, showing the number of outstanding compliance issues for each. To view the computers in the standard computer group window, click the **View as Group** button (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.

Devices by Compliance Percentage

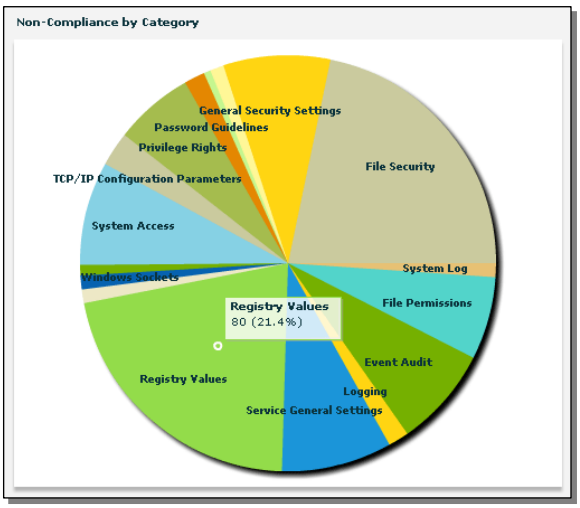


This bar chart groups computers and devices into 10% slots, showing the number of computers in each slot. For instance, all computers that have satisfied 60% to 69% of their compliance issues will be added together and assigned to that group.

Move your 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 the **View as Group** button. To return to the Dashboard, select **Security Configuration Management** from the **Window** menu.

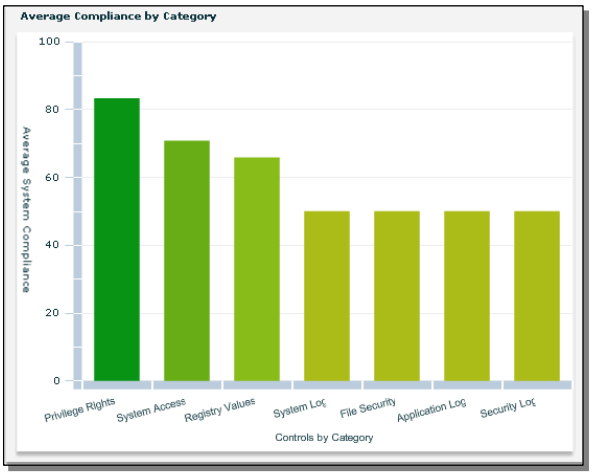
Non-compliance by Category



This is a pie chart displaying the break-down by category of non-compliant controls. This allows you to see at a glance which issues are looming largest for your enterprise.

Roll the 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 those computers that are non-compliant or applicable to that selection. 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

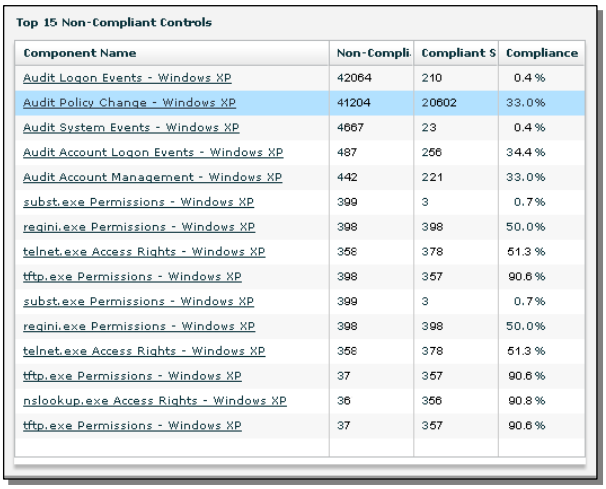


This bar graph displays the average percentage of managed computers that are compliant within each security category. There may be many categories in the graph; to limit their number, uncheck some of them in the Filter list. Roll the mouse over any bar to see the actual numeric percentage for each category. 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 determined by adding all the non-compliant computers in the category by the total number of affected computers.

There are two buttons at the bottom of the panel that allow you to view a list of the affected as well as non-compliant computers for any given selection of controls. As usual, you can click on a specific control to view the Fixlet message in its own window.

NOTE: As mentioned before, if a computer is subscribed to an non-relevant site (such as a Windows machine subscribed to a Solaris site) it will report spurious compliance. This can give you a much higher compliance score than is warranted, so make sure each computer is properly subscribed.

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 %

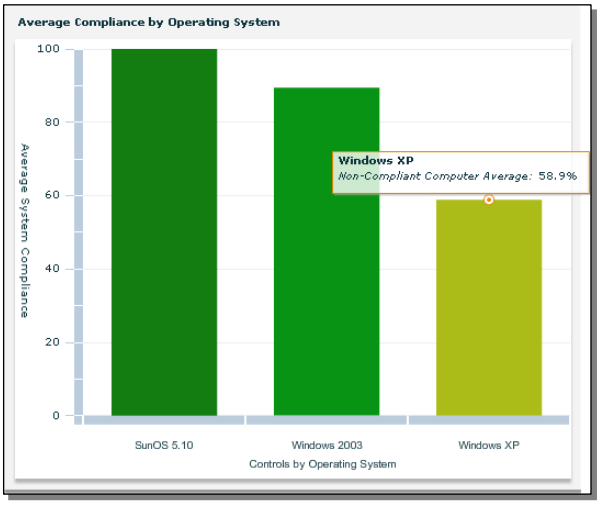
This is an abbreviated list of just the top 15 security controls. This list is ranked by the absolute number of non-compliant computers, not by percentage of compliance. As with the other control lists, you can sort these or click on the link to view the associated Fixlet message.

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 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 the controls. As usual, 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

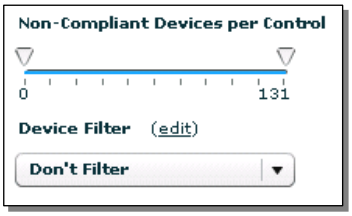
Click on the disk icon to save your report under the existing name. Each new report will become available to you whenever you run the Dashboard. Simply click SCM Reports from the button in the upper left of the window to bring up a list of saved reports.

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 (possibly large) tables will be printed last.

Report Filters

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. There are three primary types of filters:

- **Category filters** include those items that appear in the filter panel on the left side of the Dashboard report (with the exception of device filters, described next).
- **Device filters** are saved search filters. Click the **edit** link next to **Device Filter** at the bottom of the left filter panel. This lets you define a filter using **properties** to define any given subset of your networked devices. After defining this filter, you can save it and then select it at any time from the pull-down menu at the bottom of the panel.



- **Individual control filters** include or exclude specific controls from the report. These are visible in the data grid at the top of the report that lists each of the individual controls matching the criteria selected in the overall filter panel. Click the **Enabled** check box next to a control to toggle it in or out of the report.

SCM Web Reports

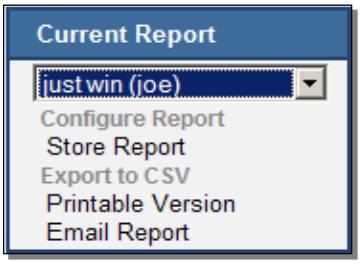
To view SCM Reports from a browser, follow these steps:

1. Select **Web Reports** from the BigFix Console **Tools** Menu. Enter your username and password, and then click **Login**.
2. Click **Reports** from the tabs 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.

SCM Reports are comparable to ordinary Web Reports, but due to their enhanced graphics capabilities, they cannot be emailed. However, as with other Web Reports, 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 public and private reports. These rules are the same as for all other Web Reports. For more information see the ***BigFix Console Operators Guide***.

Current Report Filters



Current Report filters are saved search filters. These are available in Web Reports in the pull-down menu located in the upper left part of the screen. You can create a filter to look only at Windows machines, for instance, and this can be applied to the SCM Web Report. You can also Manage Filters (edit, delete or rename) them by selecting this item from the menu. These filters are similar to the device filters noted in the Dashboard section.

SCM Report Options

Storing

Click on the link labeled **Store Report** in the upper left corner of the Web Reports screen to save the currently displayed report. Enter a name, description and category, and set the visibility to either public or private. Then click the Store Report button. The report will be saved in your list of reports under the private or public section for you to choose at any time. From this list (under the Reports tab), you can edit the report or select it as a favorite. You can also delete a saved report here.

SCM Dashboard Considerations

Dashboard users will share a similar user experience between the BigFix Console and Web Reports, but they DO NOT share the same report data store. Therefore, if you create a report in the Console, it will not be available in Web Reports and vice-versa.

As discussed previously, it is extremely important to limit SCM site subscription to the proper endpoints. The dashboard collects data from every subscribed client for its analysis. For instance, if Windows clients are subscribed to a UNIX site (or vice-versa), the Dashboard analysis will collect this information and will determine that the Windows boxes are out of compliance with the UNIX controls. To avoid this, always subscribe the computers to appropriate sites.

Appendices

Frequently Asked Questions

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.

Troubleshooting

Microsoft Policies

Troubleshooting Group Policy / Local Policy to identify effective settings can be difficult. Microsoft has supplied the following tools to help you manage them, available from the **Start>Run** option.

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

The “Home directory file Ownership” UNIX Fixlet contol (GEN001540) is taking a long time to complete.

On a system for which the home directory has many files, such as root, 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”.

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.

Index

T

U

V

W