Security Configuration Management

Guide to Configuring
UNIX and Windows Benchmarks

July, 2010

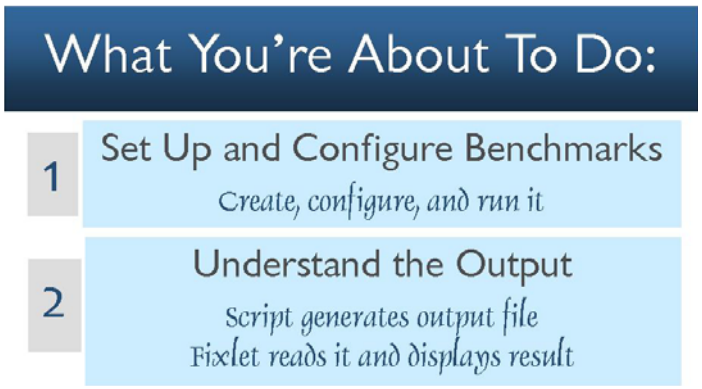
All inquiries regarding the foregoing should be addressed to:

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

Contents

Part 1

Configuring UNIX Benchmarks



Overview

SCM benchmarks (also referred to as 'checklists' or 'baselines') 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 Fixlet message includes key attributes that can help you to manage information:

Name	A descriptive title for the Fixlet message
Description	A plain-text explanation of the source of the problem and various remedies
Source ID	An identifier based on the standard addressed by the particular Fixlet site
Category	Fixlet messages are grouped into categories that allow you to sort, group and locate them by function
Source	Indicates the originating standard and version from which the configuration setting was drawn
Source Severity (DISA sites only)	The DISA-defined severity for each fixlet/check

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

The UNIX content executes 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 these 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.

Setup and Configuration

Setting up your SCM checklists for UNIX involves three basic steps: creating, configuring, and running your benchmark. Each of these steps contains several parts:

Creating a Custom Benchmark

- Create a Custom Site
- Copy Fixlets

Configuring Your Benchmark

- Select Controls via Task
- Parameterize Controls (Console and System)

Running Your Benchmark

- Modify Run Behavior
- Control Global Filescan
- Schedule a Run Task

Creating a Custom Benchmark

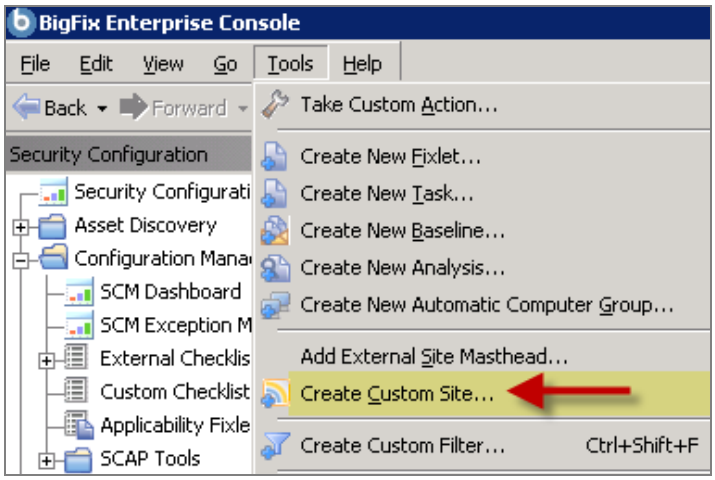
The ability to customize SCM parameters and exclude specific computers from analysis gives you a great deal of control over your security posture. However, you can go even farther by creating custom sites and repurposing the SCM checklists to fine-tune your deployment. Custom sites allow you to target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

Create a Custom Site

The SCM site masthead contains information about BigFix content that performs certain tasks and analyses within your deployment. You must be subscribed to the SCM site in order to collect data from the BigFix Clients. This data will be utilized for reporting and analysis.

The process for site subscription depends on the version of the BigFix Console that you have. Click **here** to get specific site subscription directions from the BigFix Knowledge Base.

Now that you've added a preliminary SCM masthead, you may create a custom site. Click the *Tools* dropdown menu at the top of the BigFix Console and select *Create Custom Site.*



Choose a name for your Custom 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 remediate them.

Note: Although there is a built-in Baseline feature in the BigFix Console, BigFix SCM is best managed using custom sites. The Custom Sites feature allows you to subscribe precisely defined sets of computers and devices to exactly 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.

Copy Fixlets

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.

To copy Fixlet messages individually into your custom site, 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*. You can also select multiple fixlets (or all available fixlets) and copy them into a selected custom site.

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.

Configuring Your Benchmark

Configuring a benchmark is an optional step where you configure the task to be used to run the content itself.

Select Controls via Task

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

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

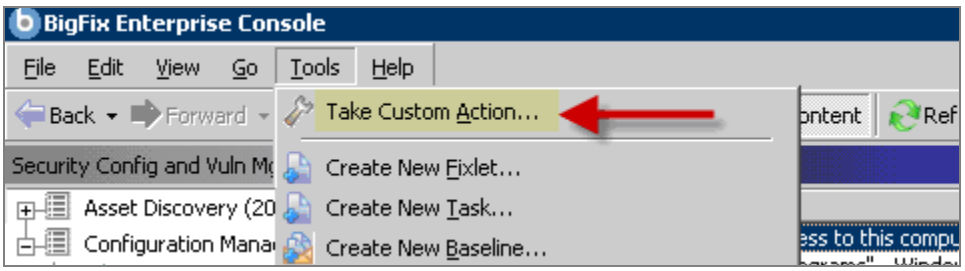
This causes runme.sh to execute *only* the set of controls specified in <FILE>. This is a 7-bit ASCII file with UNIX newlines containing a list of the specific controls you want to run, of the form:

```
GEN000020
GEN000480
GEN000560
```

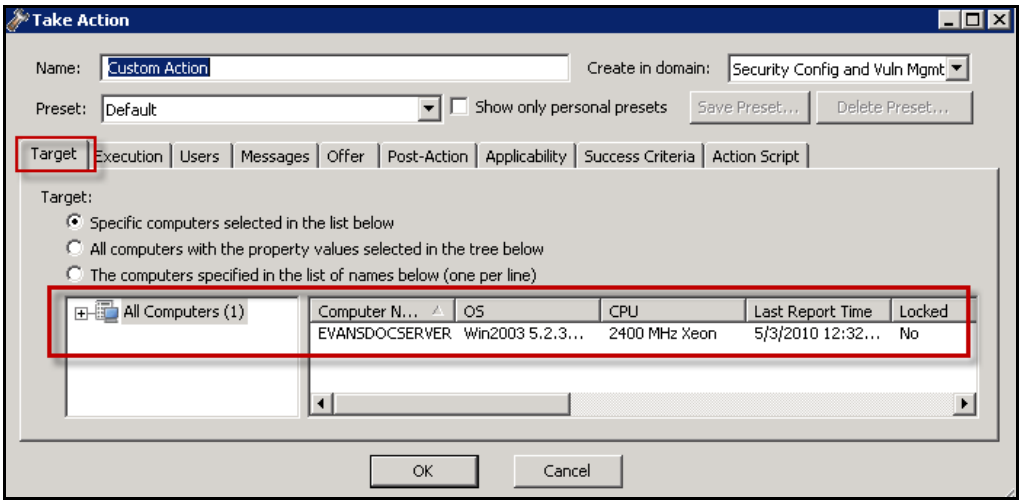
This allows you to run only the scripts you need, when you need them. To enable this functionality, you will create a Custom Action. This Action will create the file containing the list of controls and then deploy it to the desired BigFix Clients. This action is similar to the creation of a custom parameter file.

To create your own custom set of controls, use the following steps:

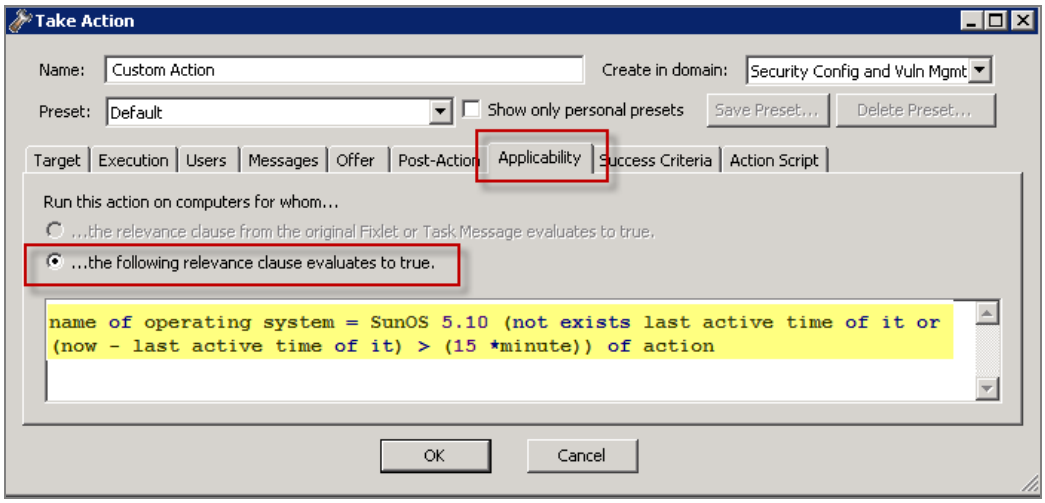
1. Select *Take Custom Action* from the Tools dropdown menu in the Console to bring up the Take Action dialog.



2. On the *Target* tab of the Take Action dialog, choose your desired endpoints.



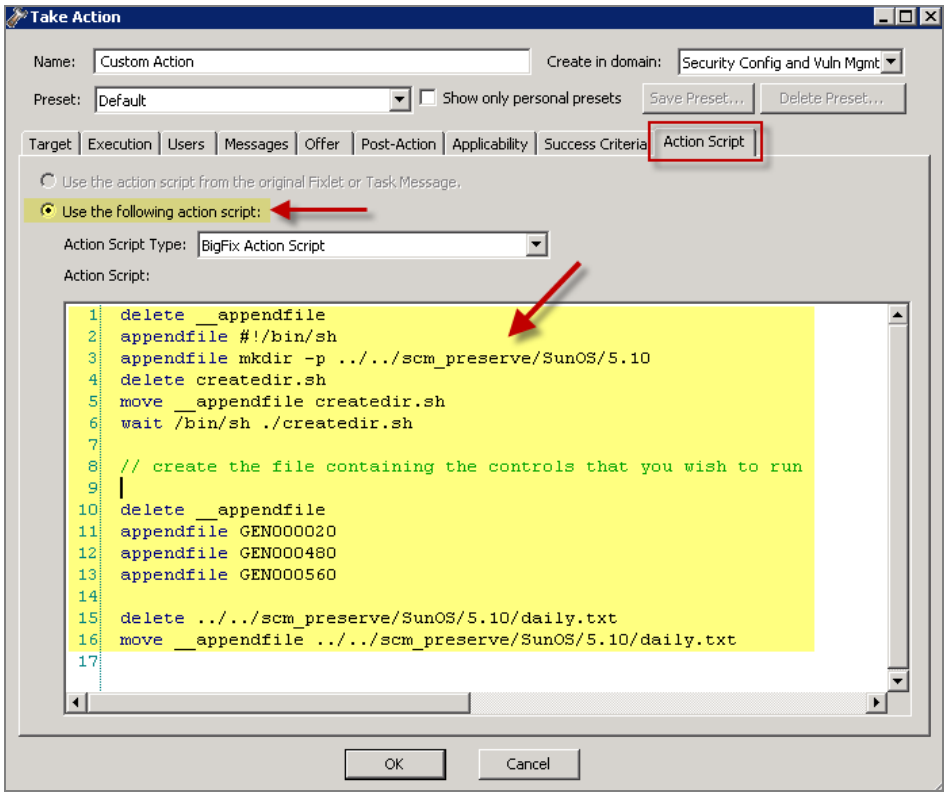
3. On the *Applicability tab,* click the second button to run this Action on computers with a custom Relevance clause.



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
```

4. 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, which 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
```


Parameterize Controls

Many factors can influence an organization's need to customize 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. Custom sites offer even greater flexibility.

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

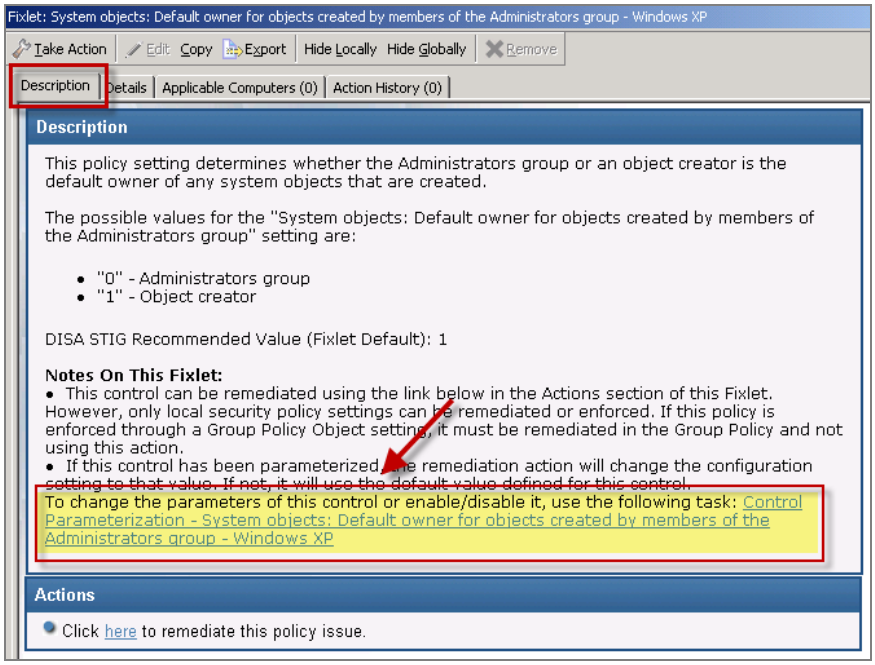
The UNIX SCM controls can be parameterized in two possible ways:

Some can be parameters from within the interface (Console). Others can be set using a customer parameter file that is stored on the UNIX system (System level). See the descriptions below for an explanation of each option.

Console Option

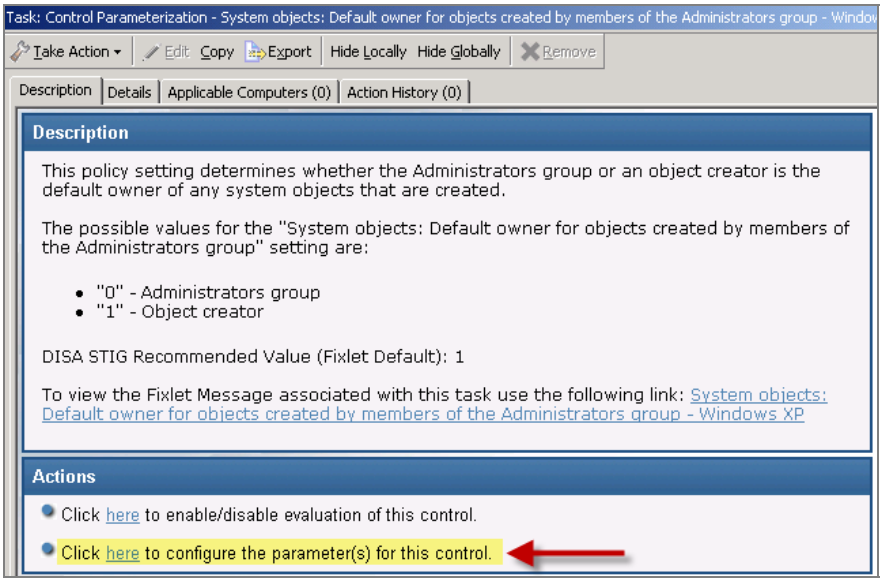
Parameters for Windows content can be modified by using the Task associated with the particular Fixlet message.

1. From the Fixlet site named *SCM Checklist for DISA STIG on Windows 2003*, select a Fixlet message. The Fixlet message opens in the work area as shown below. Make sure that the Description tab is selected.



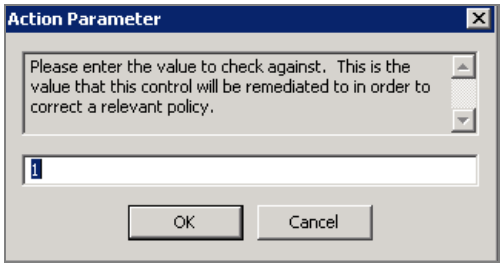
The bottom of the Description box contains a Control Parameterization link. Click the Details tab to analyze the Relevance clause attached to this Fixlet message. Click the Applicable Computers tab to see which computers in your enterprise are affected.

2. Then click the Control Parameterization link under the Description tab. This opens a task like the following in the work area.



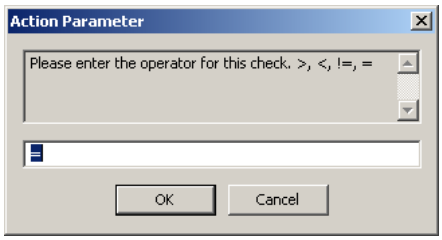
You will see two Actions associated with this Task located in the Actions box. The first lets you toggle the evaluation and the second lets you modify the parameter associated with the control.

3. Click 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 to or equal to the specified parameter.



In this case, accept the equivalence operator "=", and then click *OK*. This will open the Take Action dialog.

5. Select the parameters of your action in the Take Action dialog, click *OK,* and enter your 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.

System Level Option

In some cases, the UNIX SCM content may not have a parameter task in the Console. The content can still be parameterized at the system level. At the system level, you will be modifying the customer_params file via a task.

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
```

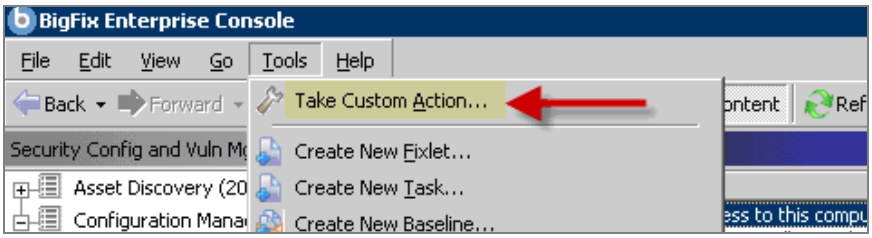
For example, if you wish to specify a minimum length of 6 and one alphabetic character in each password, you will need to customize two controls. The file would therefore have two lines, one per control:

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

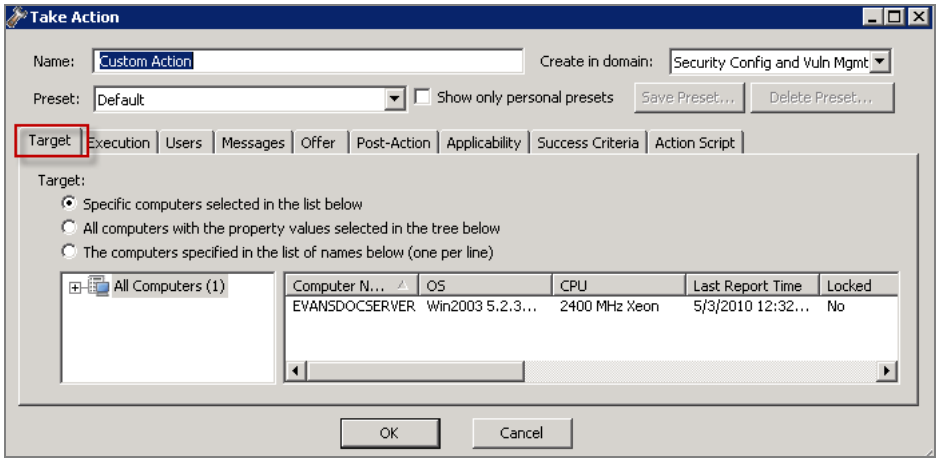
Here, the name of the parameter is VALUE. The various *BigFix SCM Parameter Guides* located on the BigFix support site discuss the individual controls, their parameter names, and the default values of each. Consult those documents to see which controls can be parameterized and their default values.

The basic steps for parameterization are as follows:

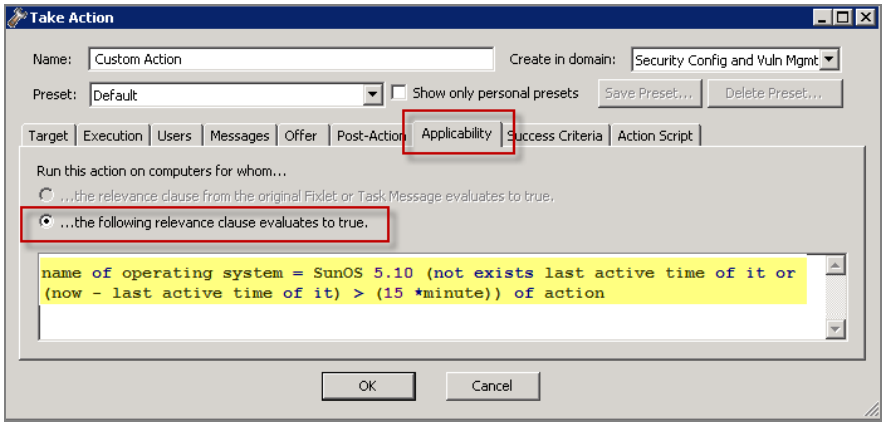
1. Begin by creating a custom Action that you will use to create and deploy the override file to the appropriate endpoints. To do this, select *Take Custom Action* from the Tools dropdown menu. The Take Action Dialog appears.



2. Under the *Target* tab of the Take Action Dialog, select the computers you wish to customize from the list.



3. Click the *Applicability* tab and select the second button to run the action on computers with a custom relevance clause.



In the text box, enter following relevance expression:

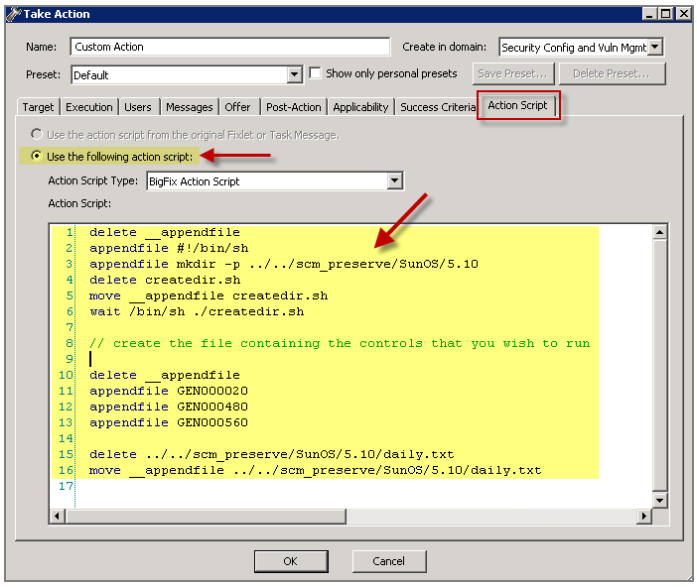
```
name of operating system = “SunOS 5.10” AND (not exists
last active time of it or (now - last active time of it) >
(15 *minute)) of action
```

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

For a list of the various operating system strings that could be used, see the table below:

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

4. 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.

Below is a sample script that would customize the password parameters:

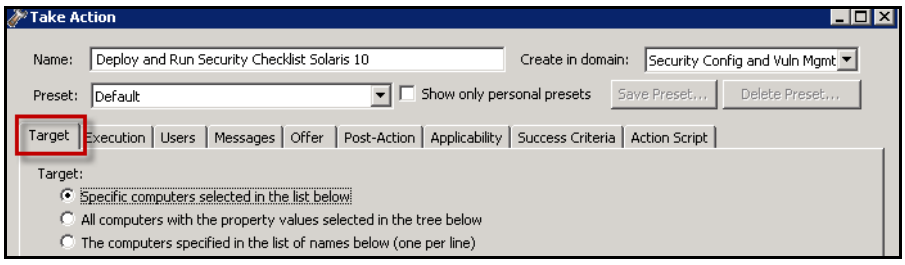
```
// create a script that will make the necessary directory
delete __appendfile
appendfile #!/bin/sh
appendfile mkdir –p ../../scm_preserve/SunOS/5.10
delete createdir.sh
move __appendfile createdir.sh
wait /sbin/sh ./createdir.sh

// 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
```

Running Your Benchmark

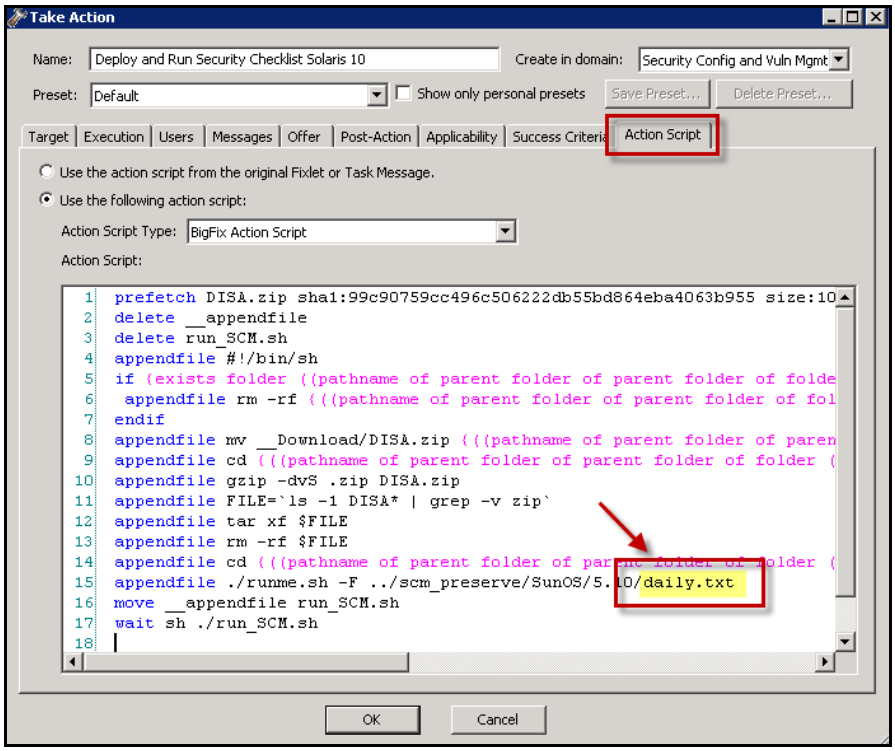
Modify Run Behavior

The Master Run script (runme.sh) is used to execute the individual control check scripts located on the UNIX system when the *Deploy and Run Security Checklist* task is executed. By default, the master script will run all BigFix control scripts, but this behavior can be modified by using the –F option.

Make a custom copy of the *Deploy and Run Security Checklist* task (for the given operating system) that comes with the content. Find this task, double-click it, and select your desired endpoints in the Take Action dialog.



Click the *Action Script* tab. Modify the Action Script to make runme.sh use the –F option and point to the file that contains the control list. In the example below, the file is named daily.txt (file names are arbitrary).



Below 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
```

In addition to the –F option, there are several other options that can be used on the master run script to change the behavior:

Options	*Behavior*
-g	This is the default option. Run globalfind and execute all scripts.
-t	Turn on tracing. The master script will create a trace file of the commands executed by the OS-specific script(s). This option is used for debugging only.
–f <source id>	Run a single control, where <control> is the name of the control that will be run.
–F <FILE>	Runs all scripts listed in <FILE>. This allows you to run 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.

Note: When using the –F option, the contents of the <FILE> will include a list similar to the following:

GEN000020
GEN000400
GEN000440

5. 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		

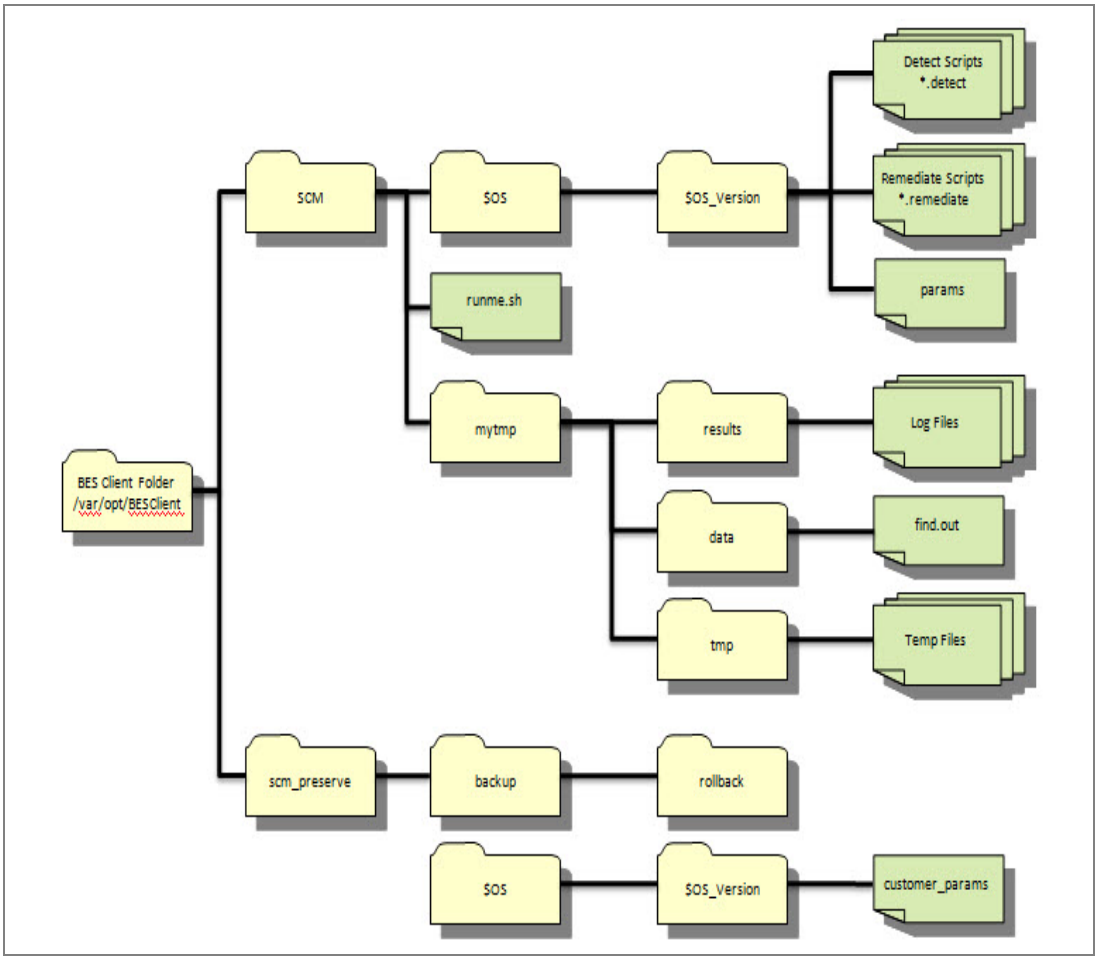
Understanding the Output

With most BigFix content, Fixlet messages constantly evaluate conditions on each endpoint and results are displayed 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, which 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. Below is a graphical representation of the directory structure:



<BES Client Folder> / SCM	This is the base directory for the OS-specific control scripts and the master script (runme.sh). The contents of this directory will be overwritten each time the 'Deploy and Run Security Checklist' task is run from the BigFix Console.
../SCM/util	A subdirectory of the BES Client Folder / SCM directory, this contains utility scripts that are used by the master script and in the individual detection and remediation scripts. The primary utility found in this directory is the 'globalfind' script.
../SCM/$OS/$OS_version	This directory will be specific to the platform on which it runs as specified by $OS and $OS_version. For example, the Red Hat Enterprise Linux 4 will show as (../SCM/Linux/4). This directory path will contain the specific detection scripts, remediation scripts, and the base parameter file used by the scripts. Each control script is named with the corresponding control ID that is used to describe the control. Each corresponding Fixlet will also reference the control ID.
../SCM/runme.sh	This is the master script that is called by the 'Deploy and Run Security Checklist' task within the BigFix Console. This script in turn will execute the 'globalfind' script and the individual control scripts.
../SCM/mytmp/results	This folder is where the OS-specific detection scripts write their log files. These logs are examined by Fixlet messages and used to determine if a control is compliant or non-compliant. Each log file will correspond to the control ID for the given control.
../SCM/mytmp/data	This folder contains the **find.out** file. This file is generated by the **globalfind** script and contains a directory listing of all locally mounted file systems and other information. This file is used by many of the OS-specific scripts and will be updated only when the **globalfind** script is run.
<BES Client Folder>/scm_preserve	This is the base directory that is used to retain the rollback scripts, custom controls, parameters, and other information that is not intended to be overwritten each time the 'Deploy and Run Security Checklist' task is executed.
../scm_preserve/backup/rollback	Each time a remediation script is executed, a corresponding rollback script is created. This enables the administrator to roll back to the previous setting associated with the specific control.
../scm_preserve/$OS/$OS_version	This directory may contain custom scripts produced by the administrator and not provided by BigFix. Scripts that reside in this directory must conform to the input / output specifications and will be run in

	conjunction with out of the box controls when executing the 'Deploy and Run Security Checklist' task.
../scm_preserve/$OS/$OS_version/customer_params	This file is used to store any custom parameters that are defined by the administrator. Any parameters defined in this file will override the default parameters specified in the **params** file stored in <BES Client Folder>/SCM/$OS/$OS_version/params).

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]
```


Each of the sections found within the log file output are described in the table below.

Section Name	Description
[RUN_DATE]	Contains the date that the script was run.
[DESCRIPTION] and [FIXLET_DESCRIPTION] Deprecated	No longer used – deprecated file
[CONTROL_COVERAGE]	Contains the names of the regulations to which this Fixlet message applies. (No longer used – deprecated files)
[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 a semicolon). On output into this file, spaces are converted to semicolons for display purposes. This is not representative of how the parameters are set.
[TIMETAKEN]	Contains the number of seconds of wall-clock time that the script took to 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
```

Modifying Global Scan Options

The UNIX SCM content includes a global scan script that is used to perform a full system scan. The results of this scan are used in a number of the scripts. The purpose of this global scan script is to eliminate the need to run a full system scan multiple times when evaluating a set of controls on a single system. This feature allows BigFix to be more efficient and cause less impact on the system when running a configuration scan. The global scan script runs by default when using the BigFix provided *Deploy and Run Security Checklist* task. It is invoked by the Master

Run script using the –g option. The behavior of the global scan script can be controlled through the following parameters:

EXCLUDEFS	A list of specific file systems to exclude from scanning. This must be a space-separated list of all the file system types to exclude from the search. By default, the global find script will exclude the following file system types from its search: ▪ cdrfs ▪ procfs ▪ ctfs ▪ fd ▪ hsfs ▪ proc ▪ mntfs ▪ smbfs ▪ iso9660 ▪ nfs ▪ msdos
EXCLUDEMOUNTS	A list of specific mount points to exclude from scanning. This parameter must be defined as a space-separated list of all the file system mounts to exclude from the search. This will prevent the shared file system from being scanned from multiple systems. For example, if several systems mount a shared directory on a Storage Area Network named /san, you might want to exclude them with a parameter such as: EXCLUDEMOUNTS="/san" By default, this parameter is not used and is represented as an empty value.
EXCLUDEDIRS	List of directories to exclude from scanning. Any directory names specified in EXCLUDEDIRS will be omitted from the directory listing. By default, this parameter excludes the lost+found directory.

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 global find parameters are represented by default in the *params* file located in the <BES Client Folder>\$OS\$OS_version directory. The parameters are represented in this file as follows:

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

These parameter values can be overwritten by adding the above-noted lines (with desired modifications) to the *customer_params* file located in the <BES Client Folder>/scm_preserve/$OS/$OS_version folder.

Scheduling Specific Controls

The default behavior for UNIX SCM deployment is to run the scripts as a single batch. 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. 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>
```

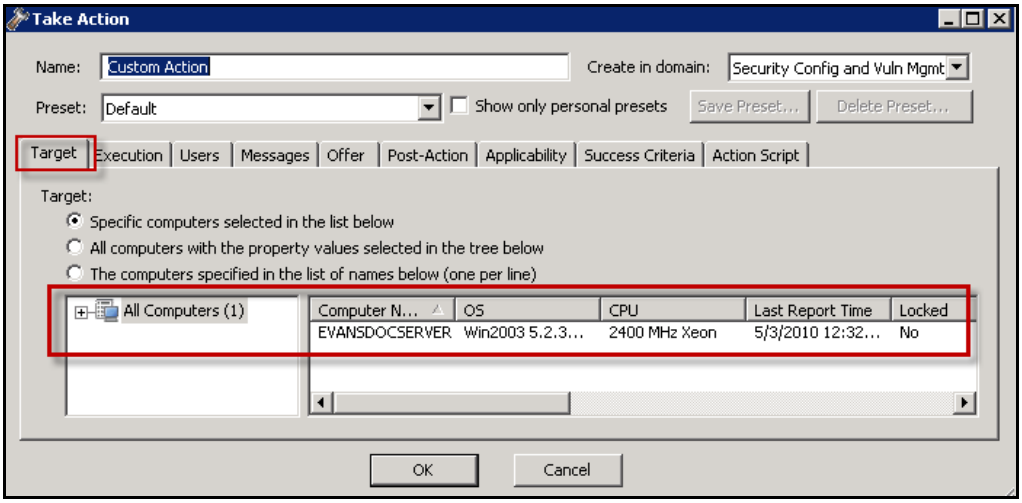
This causes runme.sh to execute *only* the set of controls specified in <FILE>. As mentioned, this is a 7-bit ASCII file with UNIX newlines containing a list of the specific controls you want to run, of the form:

```
GEN000020
GEN000480
GEN000560
```

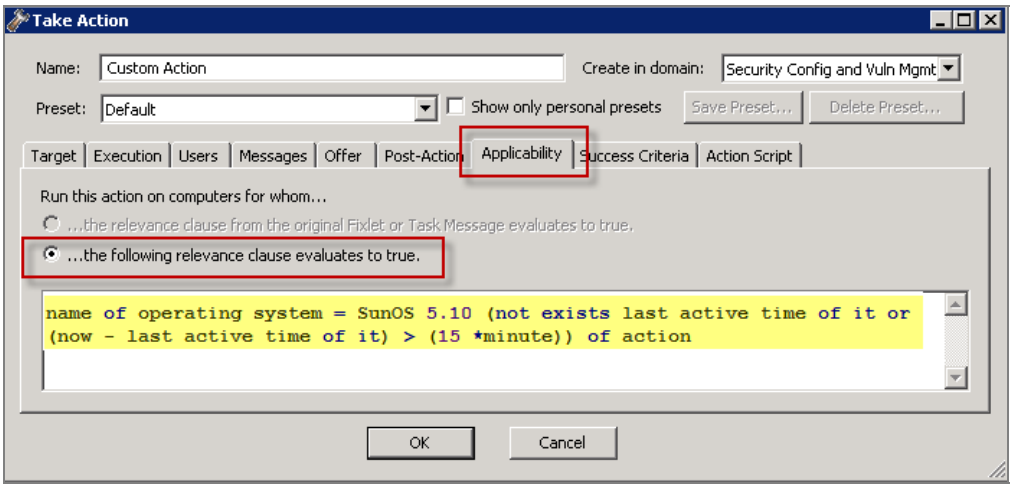
This allows you to run just the scripts you desire, when you desire. To enable this functionality, you need to create a Custom Action. This Action will create the file containing the list of controls and then deploy it to the desired BigFix Clients. This action is similar to the creation of a custom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

To create a Custom Action, see the steps below:

1. Select *Take Custom Action* from the Tools dropdown menu in the Console to bring up the Take Action dialog.



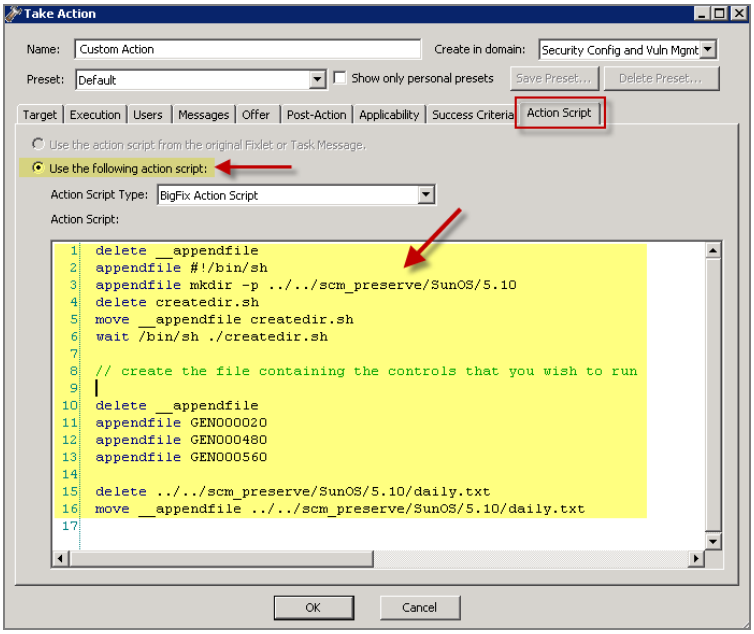
2. Click the *Applicability* tab and then select the second button to run this Action on computers with a custom Relevance clause.



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
```

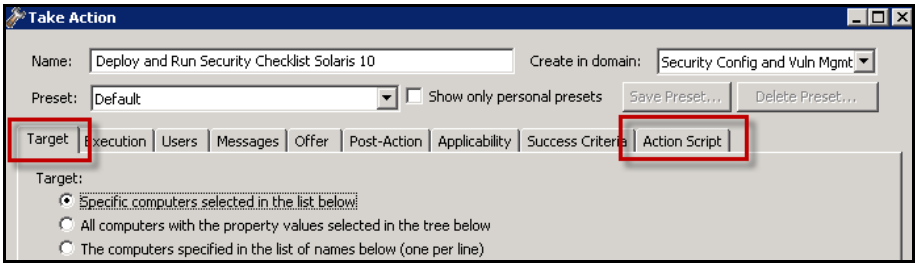
3. Click the *Action Script* tab to create a script that will copy your file onto the target computers. Click the second button and then enter a script like the one below.



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 in the Take Action dialog.



5. Under the *Action Script tab,* 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).

   Below 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
```


Part 2

Configuring Windows Benchmarks

The SCM benchmarks for Windows systems are delivered as a set of Fixlet messages and Tasks that can help you find the information you want.

- **Name** – A descriptive title for the Fixlet message
- **Description** – A plain-text explanation of the source of the problem and various remedies
- **Source ID** – An identifier based on the standard addressed by the particular Fixlet site
- **Category** – Fixlet messages are grouped into categories that allow you to sort, group and find them by function
- **Source** – Indicates the originating standard and version from which the configuration setting was drawn

Understanding Windows-based SCM

The SCM benchmarks for Windows-based platforms will be distributed by BigFix in externally provided Fixlet sites. Each site represents a single platform / standard combination (i.e. DISA STIG on Windows XP, FDCC on Windows Vista).

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:

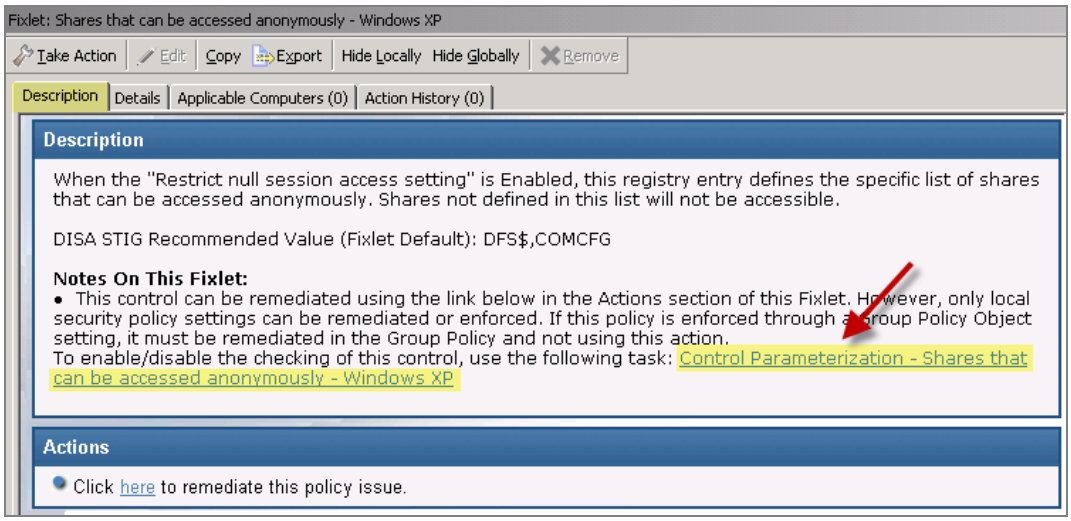
- **Enable/Disable Fixlet evaluation** – allows you to exclude the given Fixlet message from evaluation on one or more endpoints. This is a toggle that you can turn back on to include the Fixlet message again.
- **Parameterize Fixlet message** – allows you to change the parameter value of a Fixlet message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

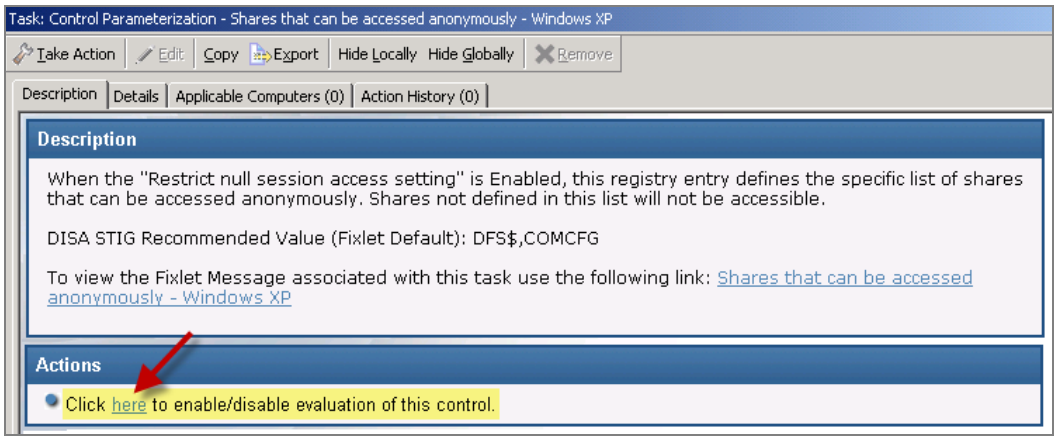
You may want to stop the Relevance evaluation of a Fixlet message for a certain segment of your endpoints. There are two ways to do this: create a custom site and simply leave this Fixlet message out, or disable the Fixlet message for specific computers.

To disable a Fixlet message for a given set of computers, follow the steps below:

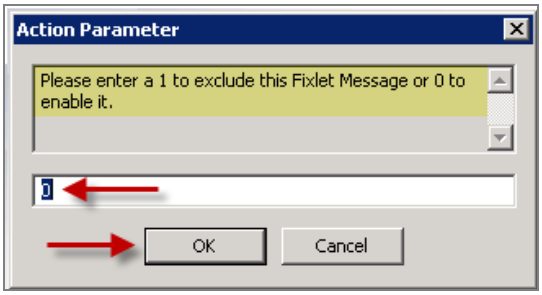
1. After opening a Fixlet message for viewing, click the *Description* tab to see the message associated with this particular control.



2. If the selected Fixlet message can be disabled, you should see a *Control Parameterization* link at the bottom of the description. 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". Be sure to select the *Description* tab.
4. At the bottom of the description, you will see an Actions box. Click on the link to Enable or Disable the evaluation of the control.



5. An Action Parameter dialog will open. Enter a "1" to disable the Fixlet control.

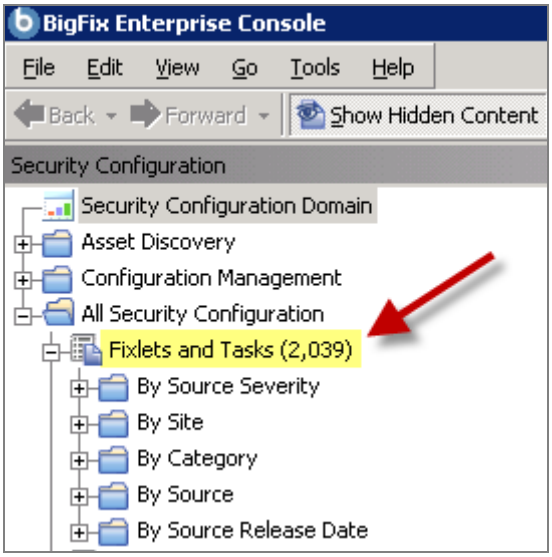


6. The Take Action dialog will open, where you can target the set of machines on which you would like to disable the control. Click *OK* and supply your password to deploy the Action. If you disable the control on all applicable computers, this Fixlet message will disappear from the list of relevant Fixlet messages.

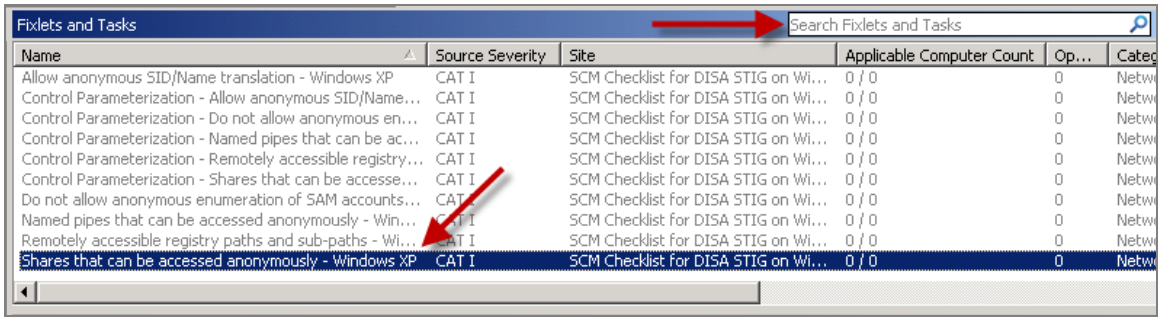
Enabling Windows Controls

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 necessary.

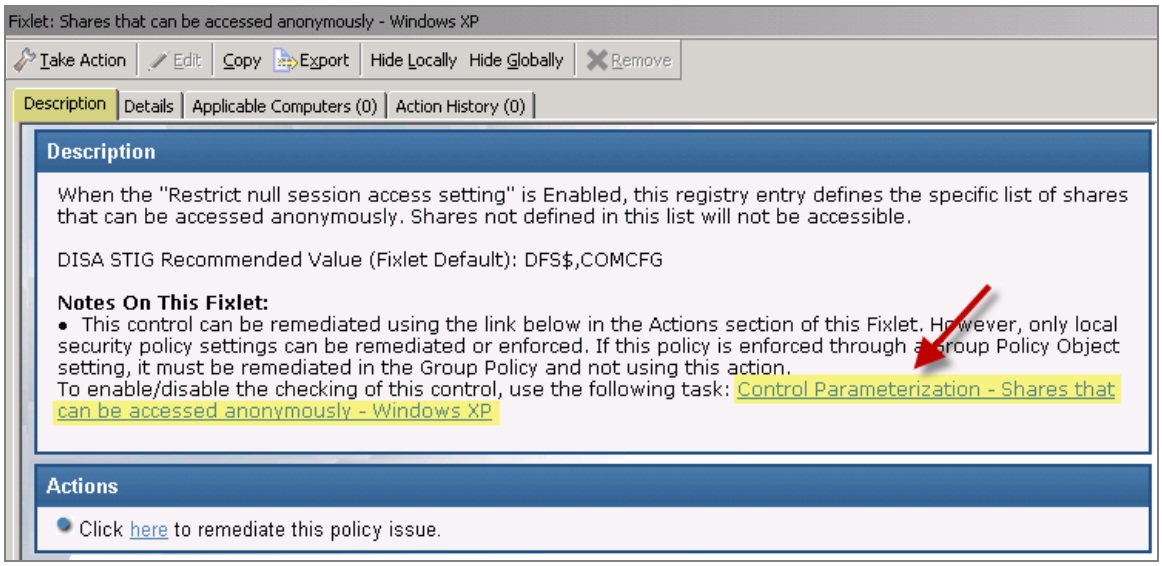
1. To locate the disabled Fixlet message, click *All Security Configuration* node and expand the *Fixlets and Tasks* sub-node. This allows you to view all Fixlet messages related to the entire Security Configuration domain, regardless of their relevance to a particular SCM site.



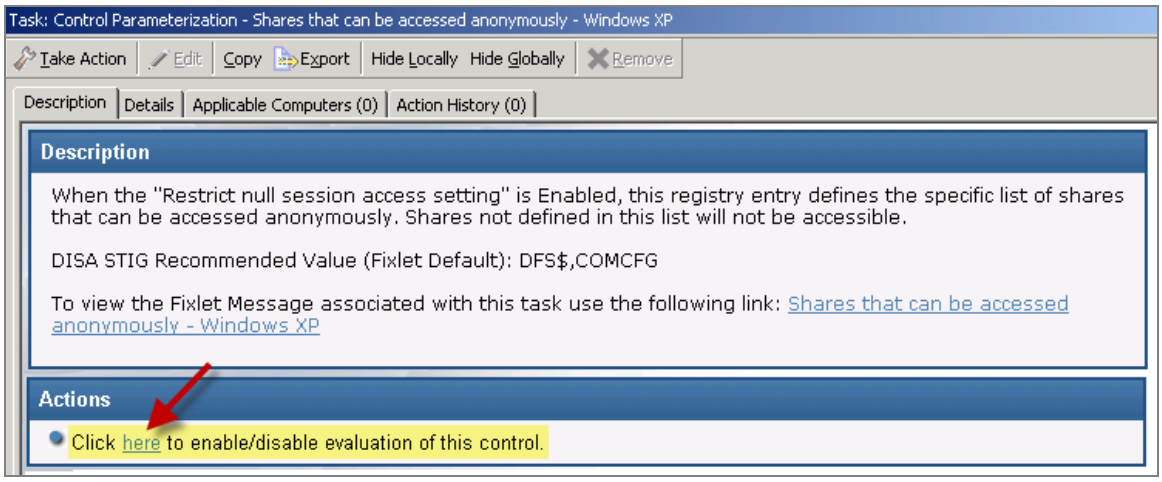
2. Search for the desired Fixlet messages by clicking the sub-folders (Source Severity, Site, etc.). Double-click the Fixlet message to view it in the work panel, or enter the desired Fixlet name in the Search box in the upper right of the Console.



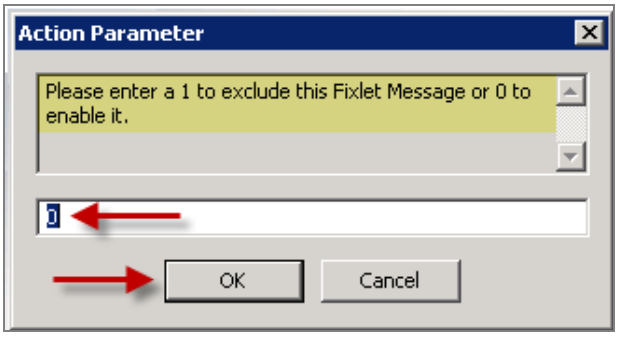
3. When the Fixlet window opens in the work panel, click the *Description* tab and scroll down to see the link labeled *Control Parameterization*.



4. Click the *Control Parameterization* link to bring up the related settings Task.



5. Click the enable/disable link and enter a “0” (zero) in the Action Parameter dialog to enable the Fixlet message.



6. The Take Action dialog opens. As before, target the desired computer(s), click *OK* and enter your Private Key Password to deploy the Action. If there are any computers out of compliance with this issue, the control will re-appear in the Fixlet list after several minutes.

It is important to note that by using this method for enabling and disabling Windows controls, the Fixlet will always display as Not Relevant (i.e. Compliant). This means that the control will always show as compliant in the dashboard and reports. This feature can be applied to any set of computers by using the Take Action dialog.

Another method for enabling and disabling these controls includes use of the new Exception Management capability. For detailed information, see the Exception Management Dashboard section of the *SCM User's Guide*.

Setting Windows Fixlet Parameter Values

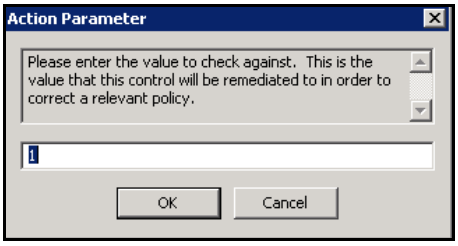
Every organization requires different levels of security. Organizations typically customize security policies based on variables such as applications and security thresholds. Part of this customizing process includes changing the values for defined configuration settings to meet specific corporate policies.

BigFix enables you to customize the content in the default Fixlet site by special targeting, customizing parameters, and disabling controls. By giving you flexibility, custom sites provide tremendous latitude in your deployment options, helping you to craft finely-targeted security policies and apply those policies to selected endpoints.

You may parameterize Fixlet controls to suit each individual situation. These parameters are stored as site settings, which parameterize the same control differently for each site containing a copy of the control.

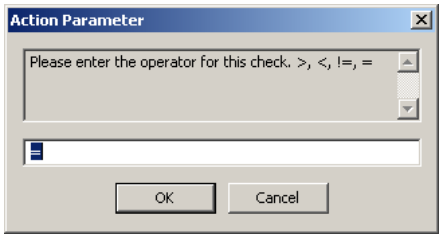
Parameters for Windows content can be modified by using the Task associated with the particular Fixlet message, as shown in the steps below:

1. From the Fixlet site named *SCM Checklist for DISA STIG on Windows 2003*, select a Fixlet message. The Fixlet message opens in the work area The Fixlet message displayed in the Description tab contains a *Control Parameterization* link.
2. Click the *Control Parameterization* link. This opens a task in the work area. 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. Scroll down to the Actions box to find 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 the second Actions 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 to or equal to the specified parameter.



   In this case, use the equivalence operator and click *OK*. This aspect of parameterization allows you to conduct a "relative check" (i.e. greater than, less than) as an alternative to an "absolute check" (equal to, not equal to). The default behavior is to conduct an "equal" check (e.g. > 10).

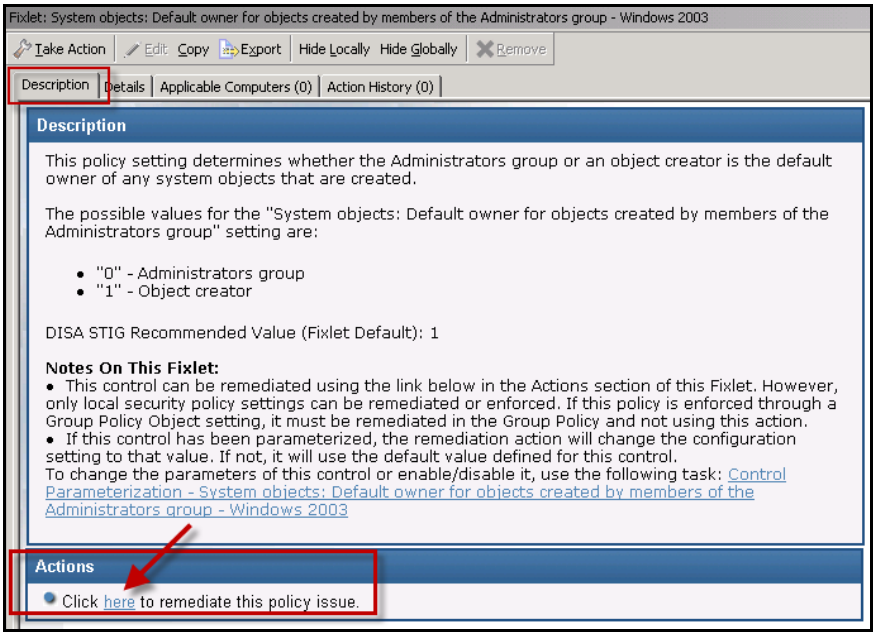
5. The Take Action dialog opens, which enables you to target any desired subset of computers. For more information on Take Action dialogs, see the BigFix Console Operator's Guide.

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. Click the *Description* tab and scroll down to the Actions box (if one exists) at the bottom of the message.



3. Click the Actions box link to remediate the specified policy issue.
4. Set your desired parameters in the Take Action dialog, 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.

Note: Not all Fixlets have a remediation action. For more information, see the Knowledge Base on the BigFix support website.

Part 3

Support

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

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

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

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

