# Contents

## Part 1

*Overview* 4
- Introduction 4
- System Requirements 4

## Part 2

*Setup* 5
- Installing SCM 5
- Navigating SCM in the BigFix Console 5
  - Components 6
  - Working with Content 8
- Modifying External Site Subscription 10
- Using the Default SCM Benchmarks 13
- Modifying Control Parameters 14
- Disabling Controls 16
- Remediating Out-of-Compliance Controls 17
- Accessing the Control Dashboard and Reporting 17

## Part 3

*Support* 21
Introduction

BigFix Security Configuration Management (SCM) combines automation in the form of 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.

This guide will take you through the SCM installation and setup process. For a detailed methodology of how to use SCM, see the SCM User’s Guide. For Security Content Automation Protocol (SCAP) guidance, see the BigFix SCAP Setup Guide and User’s Guide, available on the BigFix support site.

System Requirements

Your BigFix SCM deployment must be configured according to the following requirements.

Minimum supported browser versions:

- IE 6.0

Minimum Adobe Flash player version:

- Flash Player 9.0

Minimum BigFix component versions:

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

Each SCM benchmark (also referred to as ‘checklists’ or ‘baselines’) 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 automatically delivered.

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](http://support.bigfix.com/bes/install/airgapnetwork.html) to get specific site subscription directions from the BigFix Knowledge Base.

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](http://support.bigfix.com/bes/install/airgapnetwork.html).

The Fixlet messages in this site can be implemented as-is or customized 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.

Navigating SCM in the BigFix Console

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

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

The BigFix Console organizes content into four parts:

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

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

The Domain Panel is the area on the left side of the Console that includes a Navigation Tree and a list of all domains. The Navigation Tree includes a list of nodes and sub-nodes containing site content.

In the image below, you will see a navigation “tree” at the top with expandable and collapsible nodes, and a list of domains at the bottom. By clicking the Security Configuration domain at the bottom of the domain panel, a list of sites associated with that particular domain will display in the navigation tree at the top.
The red-outlined area represents the entire Domain Panel (including the navigation tree and list of domains), and the blue box contains just the Navigation Tree for the Security Configuration domain.

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

The upper panel, called the List Panel (blue), contains columns that sort data according to type, such as Status, Name, Site, Applicable Computer Count, etc.

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

The “nodes” in the Configuration Management navigation tree expand and collapse to enable you to easily navigate and manage relevant components in your deployment.

```
Security Configuration
  + Security Configuration Domain
    + Asset Discovery
    + Configuration Management
    + All Security Configuration
```

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

You will use this same expand/collapse method to move through the entire navigation tree. Click each “+” to display each piece of related SCM content.
You can see from the image above that Configuration Management content is organized into 2 primary nodes – *External Checklists* and *SCAP Tools*, along with two dashboards located at the top of the navigation tree.

Each node expands into sub-nodes that contain additional content. In the image below, you can see how each sub-node under External Checklists expands to display additional tasks and content:

Use the same approach of clicking the "+" and "-" to open and close each node and sub-node.
Composite View

For an overall view of the “type” of SCM content, click on the External Checklists node and review the List Panel on the right. This will display a list of all of the Fixlets related to each particular SCM checklist.

<table>
<thead>
<tr>
<th>Security Configuration</th>
<th>External Checklists</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Name</td>
</tr>
<tr>
<td></td>
<td>Deploy and Run Security Checklist Solaris 10</td>
</tr>
<tr>
<td></td>
<td>Deploy and Run Security Checklist Solaris 9</td>
</tr>
<tr>
<td></td>
<td>Configure Filesystem Scan Options</td>
</tr>
<tr>
<td></td>
<td>Configure Filesystem Scan Options</td>
</tr>
<tr>
<td></td>
<td>Right to “Replace a process level token” - Windows 2003</td>
</tr>
<tr>
<td></td>
<td>Right to “Replace a process-level token” - Windows XP</td>
</tr>
<tr>
<td></td>
<td>Right to “Deny logon through Terminal Services” - Windows XP</td>
</tr>
<tr>
<td></td>
<td>Right to “Deny logon through Terminal Services” - Windows 2000</td>
</tr>
<tr>
<td></td>
<td>Right to “Enable computer and user accounts to be trusted for impersonation” - Windows 2000</td>
</tr>
<tr>
<td></td>
<td>Right to “Deny access to this computer from the network” - Windows XP</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Modifying External Site Subscription

When deploying an SCM checklist or benchmark, special consideration should be given to the selection of configuration settings implemented on a given system. In many cases, organizations define a single benchmark for a single class of systems or type of systems, and apply that benchmark 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 you want to be evaluated on the systems. Without properly subscribing the sites, the Dashboard may not report correctly. Generally, when you subscribe a BigFix-provided SCM checklist, the BigFix Console distributes the sites to all BigFix Clients by default.

To properly target your Clients, follow the steps below:

1. From the BigFix Console, click the Tools pull-down menu and select Add External Site Masthead.
2. Browse to locate the desired masthead file, then click Open. Select a security site from the list that is targeted to a specific OS, such as the SCM Checklist for DISA STIG on Windows 2003.

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

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

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

6. Click the Computers which match the condition below button and review the dropdown list to select filter criteria.
7. From this dialog, you need to distinguish the group of computers you wish to target. For this example, select OS from the pull-down property list, then enter Win2003 in the property value box. This will only subscribe Win2003 OS computers to this particular site. Follow this procedure with each site to ensure that only the appropriate computers are subscribed to each out-of-the-box SCM site. Below are the group definitions for other operating systems:

<table>
<thead>
<tr>
<th>Operating System</th>
<th>String</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows XP</td>
<td>WinXP</td>
</tr>
<tr>
<td>Windows Vista</td>
<td>WinVista</td>
</tr>
<tr>
<td>Windows 2003</td>
<td>Win2003</td>
</tr>
<tr>
<td>Sun Solaris 10</td>
<td>SunOS 5.10</td>
</tr>
<tr>
<td>Sun Solaris 9</td>
<td>SunOS 5.9</td>
</tr>
<tr>
<td>Sun Solaris 8</td>
<td>SunOS 5.8</td>
</tr>
<tr>
<td>IBM AIX 5.1</td>
<td>AIX 5.1</td>
</tr>
<tr>
<td>IBM AIX 5.2</td>
<td>AIX 5.2</td>
</tr>
<tr>
<td>IBM AIX 5.3</td>
<td>AIX 5.3</td>
</tr>
<tr>
<td>HP-UX 11.0</td>
<td>HP-UX B.11.00</td>
</tr>
<tr>
<td>HP-UX 11.11</td>
<td>HP-UX B.11.11</td>
</tr>
<tr>
<td>HP-UX 11.23</td>
<td>HP-UX B.11.23</td>
</tr>
<tr>
<td>Red Hat Enterprise Linux 3</td>
<td>Linux Red Hat Enterprise AS 3</td>
</tr>
<tr>
<td></td>
<td>Linux Red Hat Enterprise ES 3</td>
</tr>
<tr>
<td></td>
<td>Linux Red Hat Enterprise WS 3</td>
</tr>
<tr>
<td>Red Hat Enterprise Linux 4</td>
<td>Linux Red Hat Enterprise AS 4</td>
</tr>
<tr>
<td></td>
<td>Linux Red Hat Enterprise ES 4</td>
</tr>
<tr>
<td></td>
<td>Linux Red Hat Enterprise WS 4</td>
</tr>
<tr>
<td>Red Hat Enterprise Linux 5</td>
<td>Linux Red Hat Enterprise AS 5</td>
</tr>
<tr>
<td></td>
<td>Linux Red Hat Enterprise ES 5</td>
</tr>
<tr>
<td></td>
<td>Linux Red Hat Enterprise WS 5</td>
</tr>
</tbody>
</table>
This is the basic procedure for viewing and using an SCM checklist on all supported platforms. There are differences between the Windows and UNIX platforms and how you set parameters on each. The BigFix SCM Benchmarks Guide will address this topic.

Using the Default SCM Benchmarks

After subscribing to the SCM sites, go to the navigation tree to locate your SCM checklists.

Click the “+” next to each checklist to view the available related content:
The Fixlet messages displayed in Fixlets and Tasks 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 any Fixlet message from the list to view it. The Fixlet opens in the work area with the following tabs: Description, Details, Applicable Computers and Action History. Click the Description tab to view 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. Depending on the issue, the description tab could offer a procedure for maintaining compliance or a list of active remediations found in the Actions box. Click the applicable link to deploy a remediation.

When you select a Fixlet Action, the Take Action dialog opens, allowing you to fine tune the deployment. For more information on the Take Action dialog, review the BigFix Console Operator’s Guide.

Once you have targeted your desired set, click OK and enter your Private Key Password. This immediately sends the Action to the appropriate endpoints. 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 will disappear from the list of relevant Fixlet messages. 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 Control Parameters

As well as monitoring and remediating, you can modify certain parameters to adjust the sensitivity of the controls. For example, you might want to observe a stringent policy of using 14-character passwords. 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.
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 Control Parameterization Task opens with a description of the parameter function, the possible range, and the recommended values.

At the bottom of the Task window is an Actions box. You will see a link allowing you to configure the parameter(s) of this control.
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 needs for each detail of your security policy.

**Note:** Not all controls can be parameterized. For more detailed information on parameterization for the UNIX platforms, see the AIX, Linux and Solaris parameterization guides available on the BigFix support site.

### Disabling Controls

You can disable certain controls on a computer-by-computer basis. For instance, you may have 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. 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 supply your password to deploy this Action. The selected computers will then be displayed as *compliant* within the Dashboards and Reports and, therefore, will no longer evaluate the control.
Remediating Out-of-Compliance Controls

If an endpoint is out of compliance with a 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 the Fixlet message to review the specific issue and then scroll to the bottom of the description. If the Fixlet message offers remediation, it will appear as a link in the Actions box.

Click 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 Operator’s Guide.

Accessing the Control Dashboard and Reporting

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 subset of your deployment 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 view it in real time.

**Note:** The SCM Reporting masthead needs to be loaded into the Console.

To see it in action, select SCM Dashboard located at the top of the navigation tree.
When the Dashboard opens, click the *Create New Report* button on the right side of the window and supply a name.

After information from your endpoints is gathered, the Dashboard will create its display. You will see a Filter Panel on the left side of the work area allowing you controls for how you want the data to display in the pie charts.

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 elements. To save your report, click on the disk icon in the upper right.
Security Configuration Management Report Template

Current Compliance Level

Cumulative Compliance State

Computers by Compliance Percentage

Non-Compliance by Category

Average Compliance by Category

Top 15 Non-Compliant Controls

Average Compliance by Type

SCM Setup Guide 19 © 2010 BigFix, Inc.
The three icons on the top right of the work area enable you to save, print, or refresh the Console.

BigFix also offers a Web Reports application that allows you to view aspects of your deployment. If you have never used the BigFix Web Reports application, start by reviewing the BigFix Web Reports Guide. Then for specific information about SCM Web Reports, see the BigFix SCM User’s Guide.
Global Support

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

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

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

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