BIGFIX™

Security Content Automation Protocol (*SCAP*)

QuickStart Guide

July, 2010

© 2010 BigFix, Inc. All rights reserved.

BigFix®, Fixlet®, Relevance Engine®, Powered by BigFix™ and related BigFix logos are trademarks of BigFix, Inc. All other product names, trade names, trademarks, and logos used in this documentation are the property of their respective owners. BigFix's use of any other company's trademarks, trade names, product names and logos or images of the same does not necessarily constitute: (1) an endorsement by such company of BigFix and its products, or (2) an endorsement of the company or its products by BigFix, Inc.

(1) No part of this documentation may be reproduced, transmitted, or otherwise distributed in any form or by any means (electronic or otherwise) without the prior written consent of BigFix, Inc., and (2) you may not use this documentation for any purpose except in connection with your properly licensed use or evaluation of BigFix software and any other use, including for reverse engineering such software or creating derivative works thereof, is prohibited. If your license to access and use the software that this documentation accompanies is terminated, you must immediately return this documentation to BigFix, Inc. and destroy all copies you may have.

All inquiries regarding the foregoing should be addressed to:

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

Contents

CONTENTS

Use it in 5 Steps

As part of the BigFix Security Configuration Management product, *Security Content Automation Protocol* (SCAP) is a method for automating the definition, consumption and assessment of system configurations on desktop systems throughout an organization's infrastructure. This *SCAP QuickStart Guide* displays the five primary steps to using this product. For more detailed information, review the *SCAP User's Guide* that is also available as part of this release.

Although BigFix provides continuous and timely updates based on changes made to specific SCAP data streams, you may choose not to use the subscription-based content. Instead, you may choose to leverage the SCAP tools to either generate their own custom SCAP content or download SCAP configuration checklists on your own. BigFix has provided a SCAP Import Wizard to enable you to generate your own content.

1. Install BigFix SCAP Subscription Content

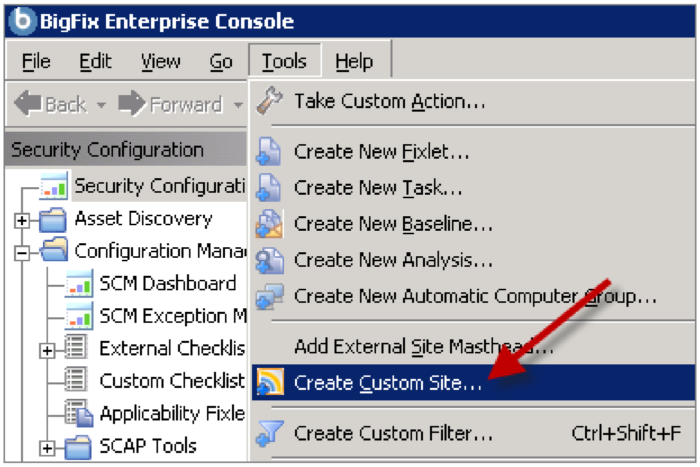
The process for site subscription depends on the version of the BigFix Console that you have. Click **here** to get specific site subscription directions from the BigFix Knowledge Base.

> **Note:** When BigFix generates Fixlet sites from an SCAP data stream, the Common Platform Enumeration (CPE) strings associated with the SCAP data stream is used to determine what types of systems should evaluate themselves against the content. Once subscribed, systems will evaluate the content if it matches the defined CPE string. This behavior can be altered if desired. See the *BigFix SCAP User's Guide* for further details.

2. Create a Custom Site

A BigFix custom site is used as a container to hold any number of Fixlets, Tasks, Dashboards, Wizards and other BigFix content. Although not required when using a BigFix-generated SCAP Fixlet site, an Administrator should create a custom site to hold the SCAP Fixlet Messages. When using the SCAP Import Wizard, a custom site should be created first to contain the created Fixlets. This can be done from within the BigFix Console.

1. Click *Tools* and select *Create Custom Site*. This will open the *Manage Sites* window.

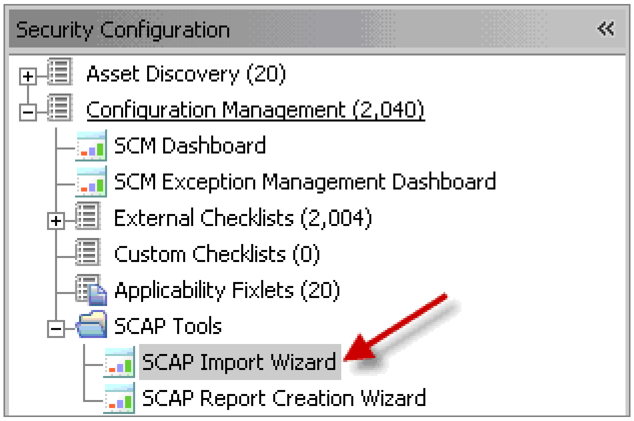


2. When prompted, enter a name for your custom site and click *OK*.

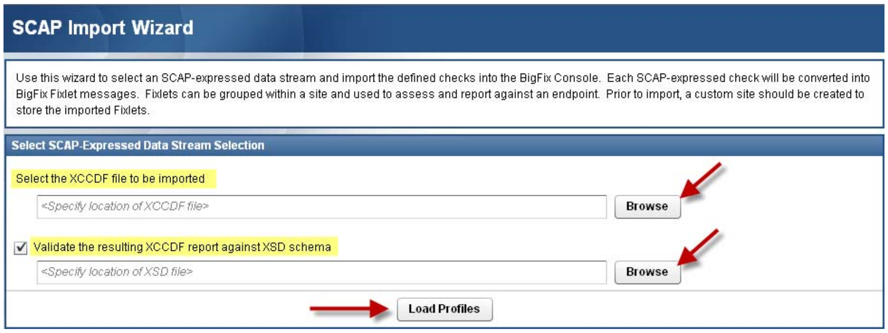
3. When the *Create Custom Site* dialog opens, use the tabs at the top of the dialog to enter a description, subscribe computers to your custom site, and add permissions.

3. Use the SCAP Import Wizard

From the SCM navigation tree, click *SCAP Tools* and then select the *SCAP Import Wizard*.


Security Configuration
Asset Discovery (20)
Configuration Management (2,040)
SCM Dashboard
SCM Exception Management Dashboard
External Checklists (2,004)
Custom Checklists (0)
Applicability Fixlets (20)
SCAP Tools
SCAP Import Wizard
SCAP Report Creation Wizard

This will open the Wizard in a window below.


SCAP Import Wizard

Use this wizard to select an SCAP-expressed data stream and import the defined checks into the BigFix Console. Each SCAP-expressed check will be converted into BigFix Fixlet messages. Fixlets can be grouped within a site and used to assess and report against an endpoint. Prior to import, a custom site should be created to store the imported Fixlets.

Select SCAP-Expressed Data Stream Selection

Select the XCCDF file to be imported

<Specify location of XCCDF file>

☑ Validate the resulting XCCDF report against XSD schema

<Specify location of XSD file>

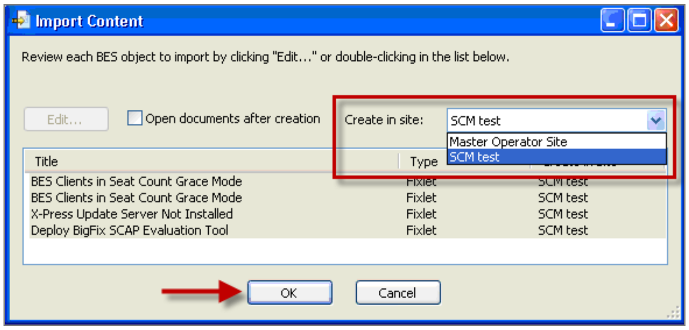
1. Click *Browse* and select an XCCDF file.

2. Specify a Validation Schema (optional).

3. Click *Load Profiles*. This process will take 1-2 minutes and will load a window for selecting XCCDF profiles.

4. Select an XCCDF profile from the pull-down menu.

5. Click *Import*. This will pop up an Import screen. Select the custom site from the pull-down menu and click *OK.*



Review each BES object to import by clicking "Edit..." or double-clicking in the list below.

□ Open documents after creation

Create in site: SCM test

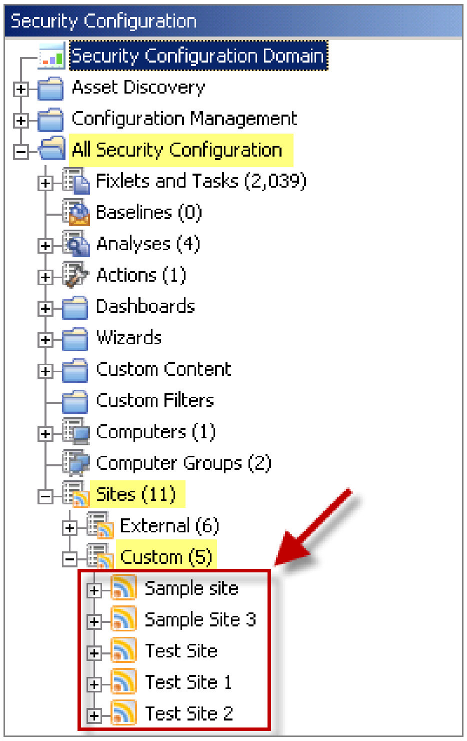
Title	Type	
BES Clients in Seat Count Grace Mode	Fixlet	SCM test
BES Clients in Seat Count Grace Mode	Fixlet	SCM test
X-Press Update Server Not Installed	Fixlet	SCM test
Deploy BigFix SCAP Evaluation Tool	Fixlet	SCM test

4. Subscribe to a Custom SCAP Fixlet Site

Unlike out-of-the-box content provided by BigFix, which automatically subscribes itself to all relevant computers, custom content must be manually subscribed to computers or computer groups.

1. With the BigFix Console still open, navigate to the *All Security Configuration* node in the SCM navigation tree.

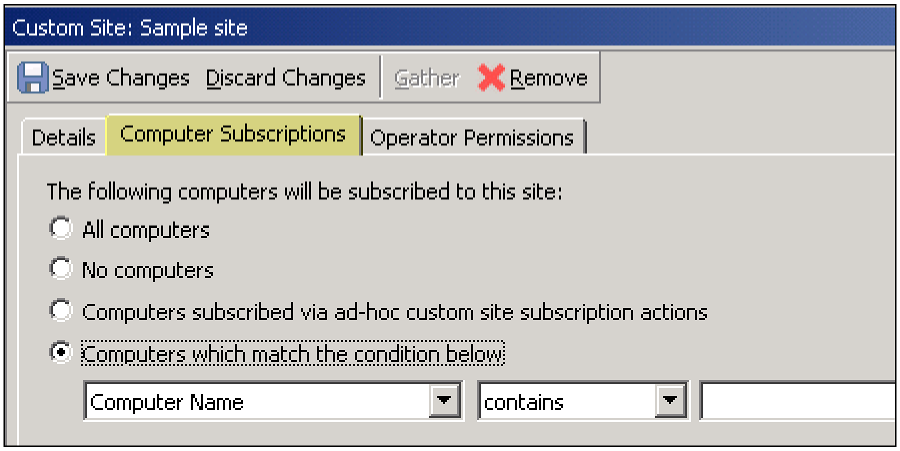
2. Select *Sites* and expand the *Custom* sub-node. Click on an existing custom site.



Security Configuration

- Security Configuration Domain
  - Asset Discovery
  - Configuration Management
  - All Security Configuration
    - Fixlets and Tasks (2,039)
    - Baselines (0)
    - Analyses (4)
    - Actions (1)
    - Dashboards
    - Wizards
    - Custom Content
    - Custom Filters
    - Computers (1)
    - Computer Groups (2)
    - Sites (11)
      - External (6)
      - Custom (5)
        - Sample site
        - Sample Site 3
        - Test Site
        - Test Site 1
        - Test Site 2

3. In the *Custom Site* window that opens, click the *Subscriptions* tab. This will allow you to subscribe specific computers or computer groups to your custom site through properties of those computers.



Custom Site: Sample site

The following computers will be subscribed to this site:

○ All computers

○ No computers

○ Computers subscribed via ad-hoc custom site subscription actions

● Computers which match the condition below:

Computer Name | contains |

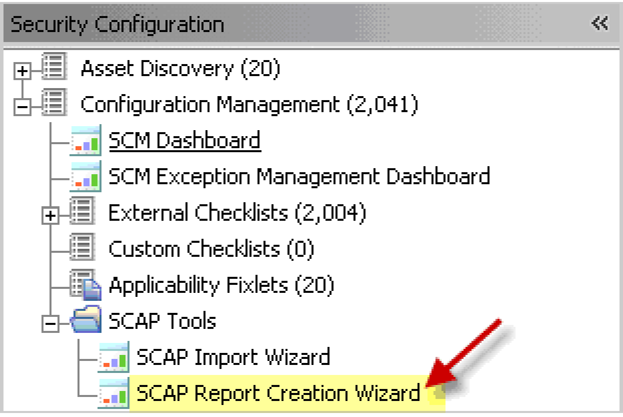
4. Click *Save Changes* at the top of the window when complete.

The BigFix Server will send a UDP request to the client. The client will then obtain a list of the content available in the new site to which it is now subscribed. Once the client receives the request or obtains the subscription request, it will evaluate itself against the defined SCAP data stream and the BigFix Console will begin to receive updates on the evaluation results.

Note: If a client is running on a computer configured with the FDCC settings in place, the UDP message will be blocked. The computer, in this case, will not receive the UDP request. The client does, however, check in periodically and will receive the new subscription at this time. Customers can decide if they wish to override the configuration setting and generate an exception to the FDCC standard.

5. Use the SCAP Report Creation Wizard

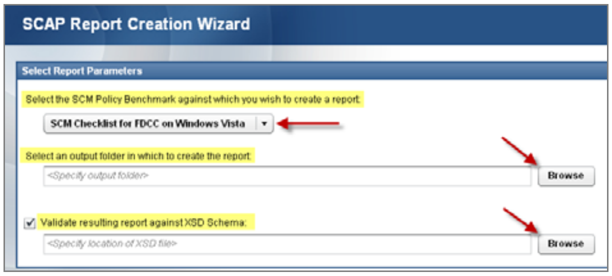
Follow the instructions below to output the results of the current configuration status of a system or group of systems using the SCAP Report Creation Wizard. From the SCM navigation tree, click the *SCAP Report Creation Wizard.*


Security Configuration
«
Asset Discovery (20)
Configuration Management (2,041)
SCM Dashboard
SCM Exception Management Dashboard
External Checklists (2,004)
Custom Checklists (0)
Applicability Fixlets (20)
SCAP Tools
SCAP Import Wizard
SCAP Report Creation Wizard

The Wizard organizes content into 3 separate windows:

- Select Report Parameters
- Target Computers
- Select Additional Report Properties

1. Select Report Parameters


SCAP Report Creation Wizard

Select Report Parameters

Select the SCM Policy Benchmark against which you wish to create a report:

SCM Checklist for FDCC on Windows Vista ▾

Select an output folder in which to create the report:

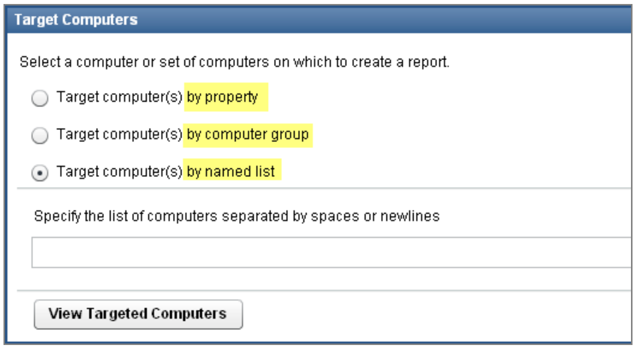
<Specify output folder>

☑ Validate resulting report against XSD Schema:

<Specify location of XSD file>

- Specify a Policy Benchmark from the pulldown menu.
- Specify an Output folder by clicking *Browse.*
- Specify a Validation Schema by clicking *Browse. (This is an optional step)*.

2. Target Your Computers



Target Computers

Select a computer or set of computers on which to create a report.

○ Target computer(s) by property

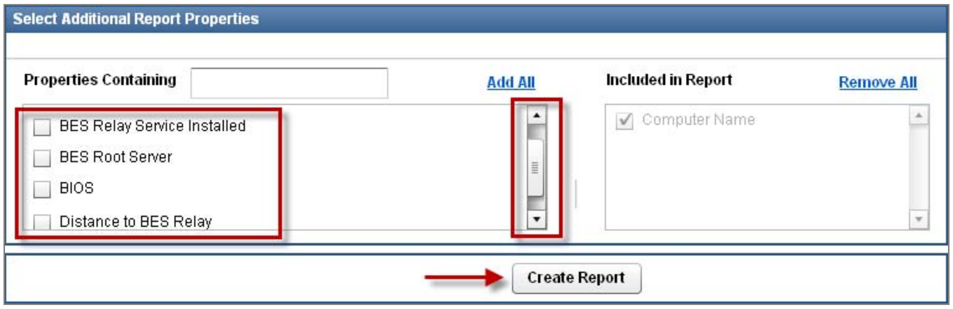
○ Target computer(s) by computer group

● Target computer(s) by named list

Specify the list of computers separated by spaces or newlines

You can target computers by name, property, or computer group. You may also manually enter a list a computers in the designated box. Click the *View Targeted Computers* button to check your selection.

3. Select Additional Report Properties



Select Additional Report Properties

Properties Containing

□ BES Relay Service Installed

□ BES Root Server

□ BIOS

□ Distance to BES Relay

Included in Report

☑ Computer Name

Use the scroll bar to view a list of available report properties. Check any applicable boxes and view each selection in the corresponding *Included in Report* box on the right.

4. Click *Create Report* when you have set all report parameters.

Note: Allocate adequate time for the creation of these reports. The amount of time to generate a report depends on the size of your deployment. For example, creating a report for a deployment of 5000 computers will take about 15 minutes.

Additional Documentation

The following additional documents, located on the documentation page of the BigFix support site, are available as part of this release:

- *SCAP User's Guide*
- *SCM Setup Guide*
- *SCM User's Guide*
- *Guide to Configuring UNIX and Windows Benchmarks*

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