Note: Before using this information and the product it supports, read the information in Notices.
Contents

Part One ____________________________ 1
   Introduction ________________________ 1
      System Requirements _____________ 1
      General Usage Concepts __________ 2

Part Two ___________________________ 7
   Reporting __________________________ 7
      Overview Reports _______________ 7
      List Reports ____________________ 7
      Check Results Reports __________ 9
      Exceptions Reports _____________ 9
      Saved Reports _________________ 10
      Chart Types ____________________ 11

Part Three _________________________ 13
   Management Tasks _________________ 13
      Computer Groups _______________ 13
      Computer Properties ____________ 14
      Data Sources ____________________ 15
      Imports ________________________ 15
      Roles __________________________ 16
      Server Settings _________________ 16
      Users __________________________ 17
      Exceptions ______________________ 17
      Account Preferences _____________ 18

Part Four __________________________ 19
   Appendix __________________________ 19
      Example Reports ________________ 19
      Technical Support _______________ 24

Part Five __________________________ 25
   Notices ____________________________ 25
Part One

Introduction

Tivoli® Endpoint Manager for Security and Compliance Analytics (SCA) is a web-based application for security and risk assessment. SCA archives security compliance check results to identify configuration issues and report levels of compliance toward security configuration goals.

SCA is a component of Tivoli® Endpoint Manager for Security and Compliance, which includes libraries of technical controls and tools based on industry best practices and standards for endpoint and server security configuration. The technical controls enable continuous, automated detection and remediation of security configuration issues. More information about the technical controls is available in the Security Configuration Management documentation on the BigFix support website at http://support.bigfix.com/resources.html#SCM. SCA provides reporting tools for managing Security Configuration Management checks.

System Requirements

Your SCA deployment must be configured according to the following requirements:

Supported browser versions:
- Internet Explorer 7.0 or 8.0
- FireFox 3

Supported Tivoli Endpoint Manager component versions:
- Console V7.2.5.21, 8.0, or 8.1
- Web Reports V7.2.5.21, 8.0, or 8.1
- Windows Client V7.2.5.21, 8.0, or 8.1
- UNIX Client V7.2.5.21, 8.0, or 8.1

SCA server operating system requirements:
- Microsoft Windows Server 2003
- Microsoft Windows Server 2008
- Microsoft Windows Server 2008 R2
- Oracle Java JDK 6 update 21 or later (available at http://www.oracle.com/technetwork/java/javase/downloads/)

SCA database server requirements:
- Microsoft SQL Server 2005
- Microsoft SQL Server 2008
SCA server, SCA database, and Tivoli Endpoint Manager database user permissions:

- To install and configure the SCA server, you must have Administrator privileges on the target SCA server, dbcreator permissions on the target SCA database server, and db_owner permissions on the associated Tivoli Endpoint Manager database.

SCM mastheads and Fixlet sites:

- You might have “legacy” BigFix Fixlets, Tivoli Endpoint Manager Fixlets, and custom Fixlets for security compliance in your deployment. These Fixlets continue to function correctly, but only certain Fixlets display within the SCA reports.
- For a current list of SCM content sites that are supported with SCA, click here for the related Knowledge Base article.

General Usage Concepts

Navigation

Using SCA, you can navigate and explore security configuration check results. Each computer in your deployment evaluates the appropriate SCM checks that you have activated using the Tivoli Endpoint Manager console, and each computer reports a pass, fail, or not applicable status for each check. Each computer also reports computer properties and analysis values, such as SCM check measured values that are active in your deployment.

SCM check results are aggregated by the SCA server and augmented by computer properties and analysis values to provide compliance overviews and detailed lists of results.

There are four primary navigation mechanisms in SCA:

- Global navigation
- Linked navigation
- Sub-navigation (or scoped navigation)
- Saved Reports navigation

Global Navigation

Global Navigation refers to the primary dropdown menus at the top of the SCA primary dashboard. Click the Reports dropdown menu to navigate through the different report types. Users with appropriate permissions also see a Management drop-down menu to view and manage the deployment configuration.
Linked Navigation

You can use linked text to navigate through report types. For example, click *5 Computer Groups* on the Overview report to display the related Computer Groups report.

Sub-navigation

You can also explore reports within a given scope from the sub-navigation menu. To view all checks, all computers, or all exceptions appropriate for a given checklist, click the *Overview* dropdown menu located on the upper-right side of most reports.
Saved Reports navigation

When you save a report view, it is available as a link on the Saved Reports list as well as from the Saved Reports menu on the left side of the report. Selecting a saved report from the menu regenerates the report view using the settings originally saved with the report. Click Saved Reports from the Reports dropdown menu, or click Save As from within any report to save the current view preferences.

Graphical Report View

You can view a variety of graphical charts that display different aspects of the security data in your deployment. You can select the columns to be displayed, change column arrangement, and filter data.
Exception Management

You can also set exceptions for excluding data from your compliance reports. From the Management dropdown menu, click *Exceptions*.

Exporting

You can export the data view of most report views to a .CSV formatted file on your local computer. Click the .CSV link on the right side of the report window.
SCA reports display graphical and tabular views of different aspects of your deployment compliance status.

There are four main report types available, each of which displays a different, configurable view of the current and historical compliance status of the deployment. All users with accounts on the system can see all report types, but the data visible to each user depends on the computers to which they have been granted visibility.

A description of each report is shown below. For a graphical representation of each report type, see Example Reports in the Appendix.

### Overview Reports

The following graphical reports are available from the primary Overview screen in the SCM dashboard:

- **Deployment Overview** – shows deployment information (such as quantity of computers and quantity of checks) and overall, historical aggregate compliance for all checks on all computers visible to the logged-in user.
- **Checklist Overview** – shows information about a single checklist (such as quantity of checks in the checklist) and overall, historical aggregate compliance for the checklist as applied to all computers visible to the logged in user.
- **Computer Overview** – shows information about a single computer (such as number of checks evaluated on the computer) and overall, historical aggregate compliance of all checks evaluated by the computer.
- **Computer Group Overview** – shows information about a computer group (such as number of children/sub-groups and number of member computers) and overall, historical aggregate compliance of the group.
- **Check Overview** – shows information about a single check (such as check source and check description) and overall, historical aggregate compliance of the check as evaluated by all computers visible to the logged in user.

### List Reports

The following reports can be found by clicking the **Reports** drop-down menu:

- **Checklist List** – shows the list of checklists in the deployment along with attributes of each checklist and the overall, historical aggregate compliance results of all checks on all visible computers for each checklist.
- **Checks List** – shows the list of checks in the given scope along with attributes of each check and the overall, historical aggregate compliance results (the aggregate of all visible computer’s pass and fail score) of each check.
- **Computers List** – shows the list of all computers in the given scope visible to the logged-in user along with attributes of each computer and the overall, historical aggregate compliance results of all checks evaluated on the computer.
- **Computer Groups List** – shows the list of all computer groups in the given scope visible to the logged-in user along with attributes of each group and the overall, historical aggregate compliance results of all checks on all computers in each group.

The annotated screen images below provide a summary of the function of each report type.
Check Results Reports

This report shows the list of all checks and computers, attributes of each computer and check, and the historical compliance result for each check on each computer.

Exceptions Reports

This report shows the list and status of exceptions in the given scope applied to each computer visible to the logged -n user, along with attributes of each check, each computer, and each exception.

To customize the settings of each report, such as filtering the view or adding additional columns, click Configure View to create custom settings.

From the Configure View menu, you can set parameters for how your data is displayed in reports.
Saved Reports

The Saved Reports feature retains a specific report format (including the displayed columns and filters you used to customize the view) for future use, without creating the same settings each time. When you save a report, it becomes available in the Saved Reports list report and visible in the drop-down box on the left side of the sub-navigation area when viewing that report type.
Chart Types

SCA displays summaries of compliance data through the following chart types:

- **Compliance Overview** – Displays compliance history over time as an overall percentage
- **Computers by Compliance Quartile** - Bar chart that provides compliance data by quartile
- **Compliance History Detail Chart** - Win loss chart that displays compliance history over time
- **Check Results History** - Total number of check results over time:
  - Not applicable – A check that does not apply to a given computer
  - Noncompliant – A check that is noncompliant on a given computer
  - Excepted – (NC) – A check that is noncompliant on a given computer, but that has been excepted through a manually-created exception
  - Excepted – (C) -- A check that is compliant on a given computer, but that has been excepted through a manually-created exception
  - Compliant – A check that complies with the checklist desired values
Part Three

Management Tasks

The Management Tasks function within SCA gives you control over various aspects of your compliance deployment. From the Management drop-down list, users with appropriate permissions can manage computer groups, computer properties, datasources, imports, roles, server settings, users, and exceptions.

Computer Groups

You can create and edit computer groups using computer property-based filters. You can also create computer groups based on existing groups using the "Parent" menu.
Note: You must perform an import after saving your changes to enact them.

Computer Properties

You can create computer properties from the Tivoli Endpoint Manager datasource available for reporting and filtering within the Analytics interface.

Note: You must perform an import after saving your changes to enact them.
Data Sources

You can view information about the Tivoli Endpoint Manager database upon which your SCA compliance data is based. You can also view information about the Web Reports database that is the source of some or all of your SCA users. The Web Reports connection provides a single-sign-on capability for users between Web Reports and SCA. You cannot edit these settings after initial setup, but you can add the Web Reports database information if you originally skipped this step.

Imports

Use the Imports interface to schedule a recurring import, disable recurring imports, start a manual import, view current import status, and view logs of previous imports.
Roles

Use the Roles interface to assign new roles to users or edit existing roles. In this current version of SCA, the assignable permissions include Edit Computer Groups, Edit Exceptions, and Run Imports.

Server Settings

Use the Server Settings interface to configure the HTTP port and SSL. Any changes to the port or SSL settings require a service restart.
Users

You can create and edit users, assign roles, and assign a set of computer groups to which a user has access. Administrators can edit user passwords, email addresses, and contact information.

<table>
<thead>
<tr>
<th>General</th>
</tr>
</thead>
<tbody>
<tr>
<td>Computer Groups</td>
</tr>
<tr>
<td>Computer Properties</td>
</tr>
<tr>
<td>Datasources</td>
</tr>
<tr>
<td>Imports</td>
</tr>
<tr>
<td>Roles</td>
</tr>
<tr>
<td>Server Settings</td>
</tr>
<tr>
<td>Users</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Username</th>
<th>Roles</th>
<th>Authentication Method</th>
<th>Computer Group</th>
</tr>
</thead>
<tbody>
<tr>
<td>bightx</td>
<td>Administrators</td>
<td>Password</td>
<td>All Computers</td>
</tr>
<tr>
<td>exceptions</td>
<td>Exit Exceptions</td>
<td>Password</td>
<td>xp</td>
</tr>
<tr>
<td>normal</td>
<td>No Roles</td>
<td>Web Reports (Datasource)</td>
<td>No Computers</td>
</tr>
<tr>
<td>readonly</td>
<td>No Roles</td>
<td>Web Reports (Datasource)</td>
<td>win7</td>
</tr>
<tr>
<td>vincent1</td>
<td>Exit Exceptions</td>
<td>Web Reports (Datasource)</td>
<td>xp</td>
</tr>
<tr>
<td>import</td>
<td>import</td>
<td>Password</td>
<td>xp</td>
</tr>
<tr>
<td>xp22</td>
<td>No Roles</td>
<td>Password</td>
<td>32</td>
</tr>
</tbody>
</table>

Exceptions

You can use the Exceptions menu to create and edit exceptions for checks, computers, computer groups, and checklists with or without an expiration date. You can also view a list of existing and active exceptions. To edit an exception, click an exception name in the list, and the Edit Exception and Exception History menus display.
Account Preferences

Use the Account Preferences interface to change your password, contact information, or API token. Click the *Account* dropdown menu from the top of the window.
Example Reports

The following are examples of the reports that can be generated in the SCA application.

Checklist List Report

![Checklist List Report](image-url)
Checklist Overview Report

87% Compliant

Checks List Report

<table>
<thead>
<tr>
<th>Check Description</th>
<th>Compliance</th>
<th>Number of Computers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrators Have Right To Debug Programs</td>
<td>50%</td>
<td>2 Computers</td>
</tr>
<tr>
<td>read.exe Permissions</td>
<td>100%</td>
<td>2 Computers</td>
</tr>
<tr>
<td>Clipboard Service Disabled</td>
<td>100%</td>
<td>2 Computers</td>
</tr>
<tr>
<td>Do Not Show First Use Dialog Boxes</td>
<td>100%</td>
<td>2 Computers</td>
</tr>
<tr>
<td>attrib.exe Permissions</td>
<td>100%</td>
<td>6 Computers</td>
</tr>
<tr>
<td>nexec.exe Permissions</td>
<td>100%</td>
<td>6 Computers</td>
</tr>
<tr>
<td>Audit: Audit the access of global system objects</td>
<td>100%</td>
<td>6 Computers</td>
</tr>
<tr>
<td>Display Error Notification</td>
<td>100%</td>
<td>6 Computers</td>
</tr>
<tr>
<td>FTP Publishing Service Disabled</td>
<td>100%</td>
<td>1 Computers</td>
</tr>
<tr>
<td>Enable user control over installs</td>
<td>0%</td>
<td>1 Computers</td>
</tr>
<tr>
<td>Error Reporting Service Disabled</td>
<td>100%</td>
<td>1 Computers</td>
</tr>
<tr>
<td>Audit System Events</td>
<td>100%</td>
<td>1 Computers</td>
</tr>
</tbody>
</table>
### Check Overview Report

#### Compliance History
- 100% compliant

#### Check Results History

#### Check Properties
- **Checklist:** ITG XCCDF for macOS 10.6.2
- **Category:** Security Options Settings
- **Source Release Date:** 11/18/2009

### Computers List Report

#### Computers

<table>
<thead>
<tr>
<th>Computer Name</th>
<th>Last Seen</th>
<th>Compliance</th>
<th>01/01/2011 - 03/31/2011</th>
</tr>
</thead>
<tbody>
<tr>
<td>Kathleen Gutierrez</td>
<td>40 minutes ago</td>
<td>100%</td>
<td>2 Checklists</td>
</tr>
<tr>
<td>Patrick Young</td>
<td>40 minutes ago</td>
<td>100%</td>
<td>4 Checklists</td>
</tr>
<tr>
<td>Daniel J</td>
<td>40 minutes ago</td>
<td>100%</td>
<td>4 Checklists</td>
</tr>
<tr>
<td>Michelle Green</td>
<td>40 minutes ago</td>
<td>100%</td>
<td>1 Checklists</td>
</tr>
<tr>
<td>Scott Thompson</td>
<td>40 minutes ago</td>
<td>100%</td>
<td>3 Checklists</td>
</tr>
<tr>
<td>Frank Diaz</td>
<td>40 minutes ago</td>
<td>100%</td>
<td>2 Checklists</td>
</tr>
<tr>
<td>Kimberly Williams</td>
<td>40 minutes ago</td>
<td>100%</td>
<td>4 Checklists</td>
</tr>
<tr>
<td>Sharon Robinson</td>
<td>40 minutes ago</td>
<td>100%</td>
<td>2 Checklists</td>
</tr>
</tbody>
</table>
Computer Overview Report

100% Compliant

Computer Groups List Report

<table>
<thead>
<tr>
<th>Name</th>
<th>Compliance</th>
<th>03/01/2011 - 02/28/2011</th>
<th>0%</th>
<th>20%</th>
<th>40%</th>
<th>60%</th>
<th>80%</th>
<th>100%</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Geographic Area</td>
<td>8</td>
<td>80%</td>
<td>97%</td>
<td>100%</td>
<td>9 Computers</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Organizational Unit</td>
<td>6</td>
<td>60%</td>
<td>98%</td>
<td>100%</td>
<td>8 Computers</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Computer Group 1</td>
<td>2</td>
<td>20%</td>
<td>98%</td>
<td>100%</td>
<td>20 Computers</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Computer Group 2</td>
<td>2</td>
<td>40%</td>
<td>98%</td>
<td>100%</td>
<td>20 Computers</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Computer Group Overview Report

Check Results List Report
Technical Support

The Tivoli Endpoint Manager technical support site offers a number of specialized support options to help you learn, understand, and optimize your use of this product:

- Tivoli Endpoint Manager Info Center
- Support Site
- Documentation
- Knowledge Base
- Forums and Communities
Part Five

Notices

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
1623-14, Shimotsuruma, Yamato-shi
Kanagawa 242-8502 Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.
Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
2Z4A/101
11400 Burnet Road
Austin, TX 78758 U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided "AS IS", without warranty of any kind. IBM shall not be liable for any damages arising out of your use of the sample programs.

TRADEMARKS:

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both.

If these and other IBM trademarked terms are marked on their first occurrence in this information with a trademark symbol (® or ™), these symbols indicate U.S. registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at http://www.ibm.com/legal/copytrade.shtml.

Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.
Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Other company, product, and service names may be trademarks or service marks of others.