

*Tivoli Endpoint Manager for
Security and Compliance Analytics*

User's Guide





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

© Copyright IBM Corporation 2003, 2011.

US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP
Schedule Contract with IBM Corp.



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.

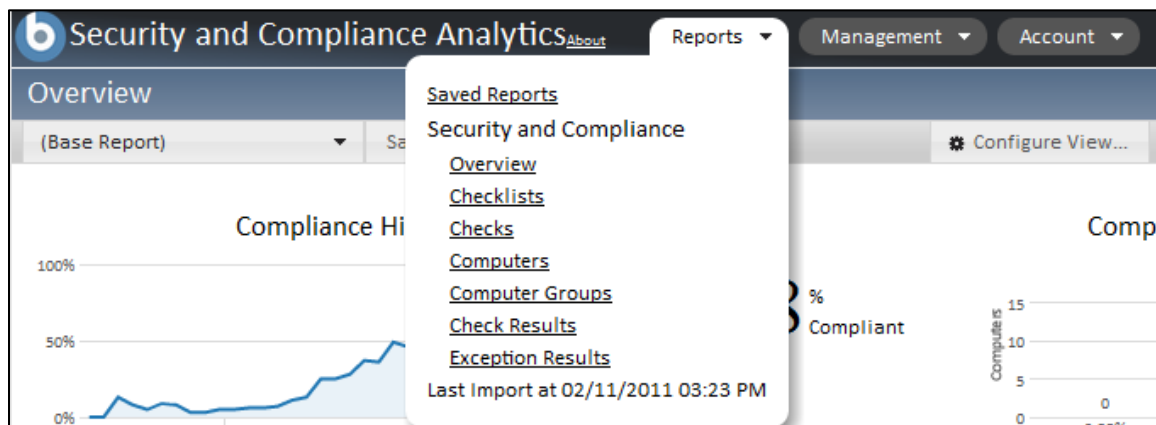
SCM check results are aggregated by the SCA server and augmented by computer properties and analysis values to provide compliance overviews and detailed lists of results.

There are four primary navigation mechanisms in SCA:

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

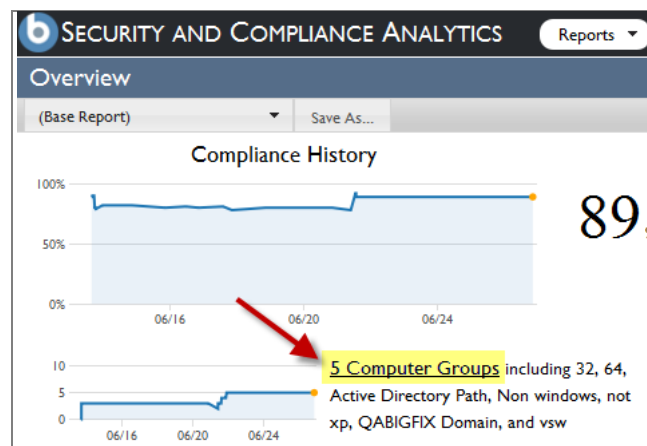
Global Navigation

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.



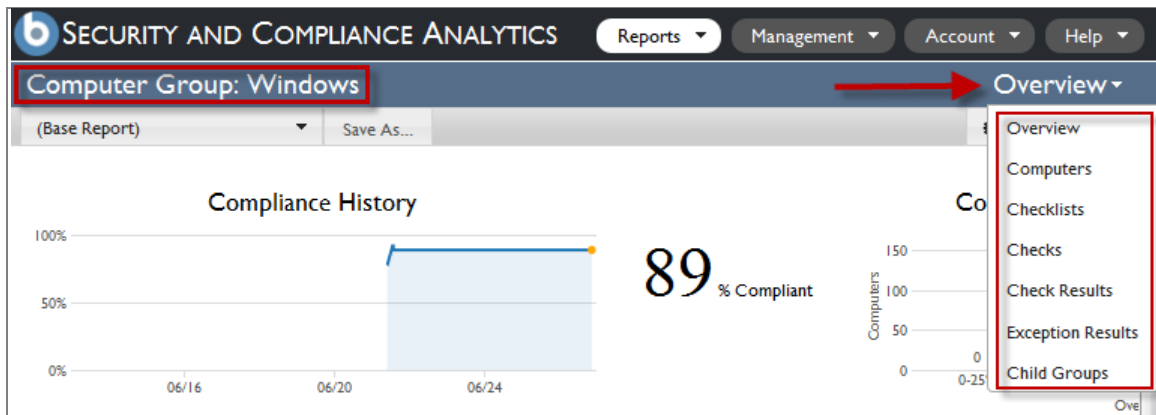
Linked Navigation

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.

The screenshot shows the IBM Security and Compliance Analytics interface with the 'Computer Groups' report. The 'Save As...' button is highlighted. The table below displays compliance data for two computer groups.

Name	Children Count	Compliance
Windows	3	89% (71,705)
Active Directory Path	0	89% (71,705)

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.

SECURITY AND COMPLIANCE ANALYTICS

Reports

Management

Account

Help

Computer Groups

(Base Report)

Save As...

CSV

5 rows

Configure View...

Name	Children Count	Compliance	
		06/13/2011 - 06/27/2011	0% 25% 50% 75% 100%
Windows	3	<div><div></div></div>	89% <div><div>71,705</div></div> 272 Computers
Active Directory Path	0	<div><div></div></div>	89% <div><div>71,705</div></div> 272 Computers
QABIGFIX Domain	0	<div><div></div></div>	88% <div><div>60,924</div></div> 191 Computers
Non windows	0	<div><div></div></div>	91% <div><div>1,447</div></div> 54 Computers
vsw	0	<div><div></div></div>	96% <div><div>828</div></div> 3 Computers

Exception Management

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

The screenshot shows the 'SECURITY AND COMPLIANCE ANALYTICS' interface. The 'Management' dropdown menu is open, displaying options: General, Computer Groups, Computer Properties, Datasources, Imports, Roles, Server Settings, Users, Security and Compliance, and Exceptions. The 'Exceptions' option is highlighted with a red box. In the background, a 'Compliance History' chart is visible, showing a line graph of compliance percentage over time (06/16 to 06/24). A red arrow points from the 'Exceptions' option in the menu to the 'Compliance History' chart.

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.

The screenshot shows the 'Checklists' report window. At the top, there is a dropdown menu set to '(Base Report)'. Below it, there is a 'Save As...' button and a yellow button with a document icon and the text 'CSV'. A red arrow points to the 'CSV' button.





Part Two

Reporting

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.

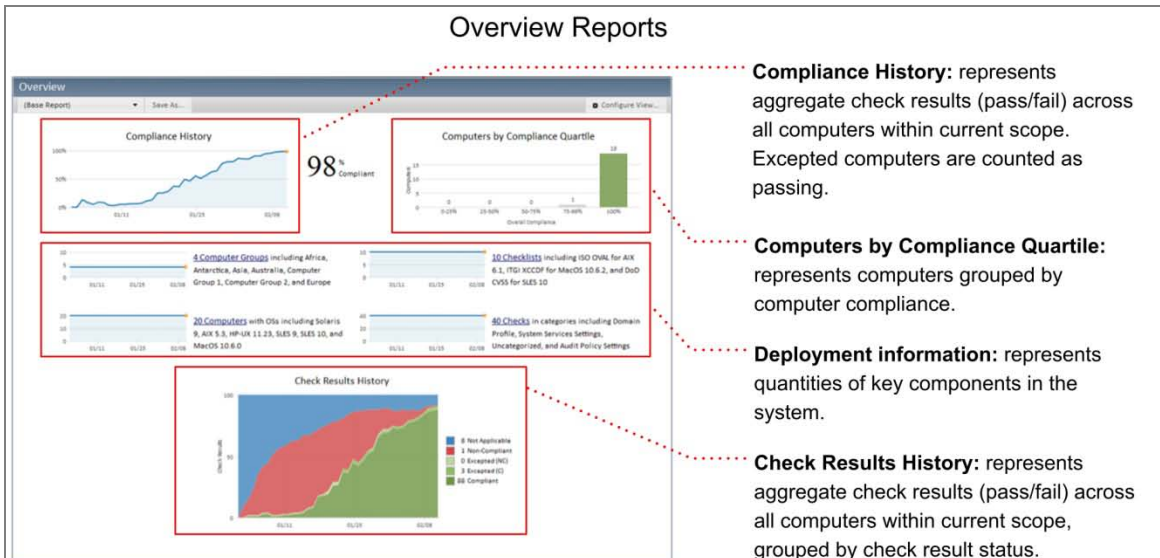
List Reports

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

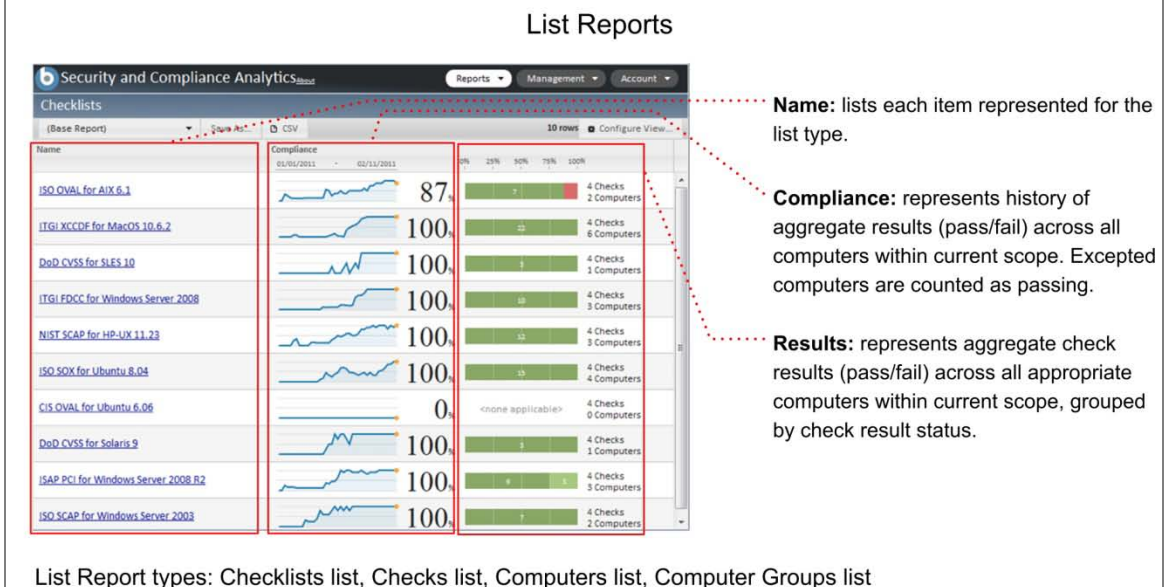
- **Checklist List** – shows the list of checklists in the deployment along with attributes of each checklist and the overall, historical aggregate compliance results of all checks on all visible computers for each checklist.
- **Checks List** – shows the list of checks in the given scope along with 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.



Overview Report types: Deployment Overview, Checklist Overview, Computer Overview, Computer Group Overview, Check Overview



List Report types: Checklists list, Checks list, Computers list, Computer Groups list



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.

Check Results Report

Descriptive columns: Each row represents a single check on a single computer. Columns show information about each computer-check pair. Columns are managed using the "Configure View..." option.

Compliance: pass/fail status for each computer-check pair. Hash marks are scaled within the displayed time range.

Exceptions Report

Descriptive columns: Each row represents a single check on a single computer as specified by an exception. Columns show information about each computer-check pair. Columns are managed using the "Configure View..." option.

Exception information: detailed information about the 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.

Configure View

×

Time Range

☒ All

☐ Last days

☐ to

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.

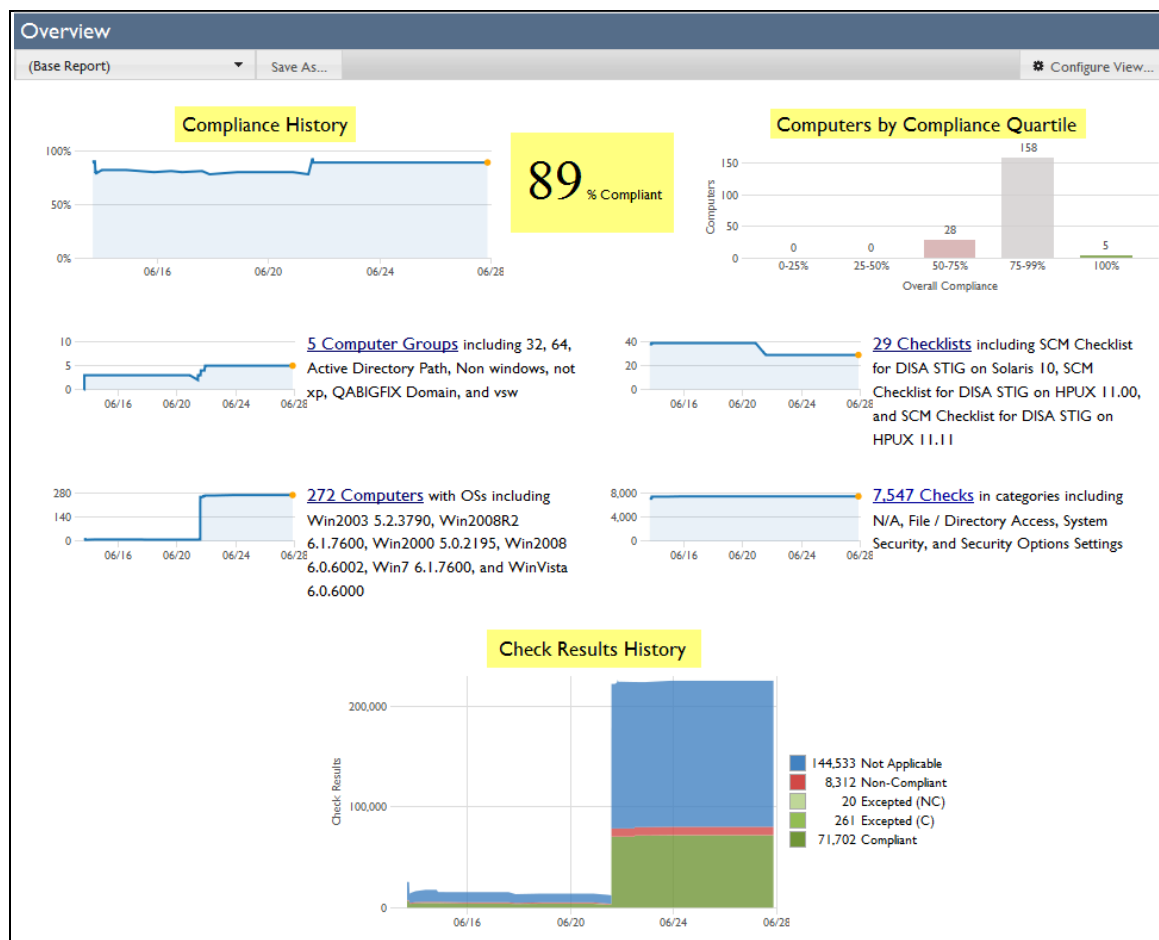
The screenshot shows the 'Security and Compliance Analytics' dashboard. The 'Reports' dropdown menu is open, displaying a list of report types: Overview, Checklists, Checks, Computers, Computer Groups, Check Results, and Exception Results. The 'Saved Reports' option is highlighted in yellow, and a red arrow points to it. The background shows a 'Compliance History' chart and a 'Checklist: SCM Checklist for D' section.



Chart Types

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

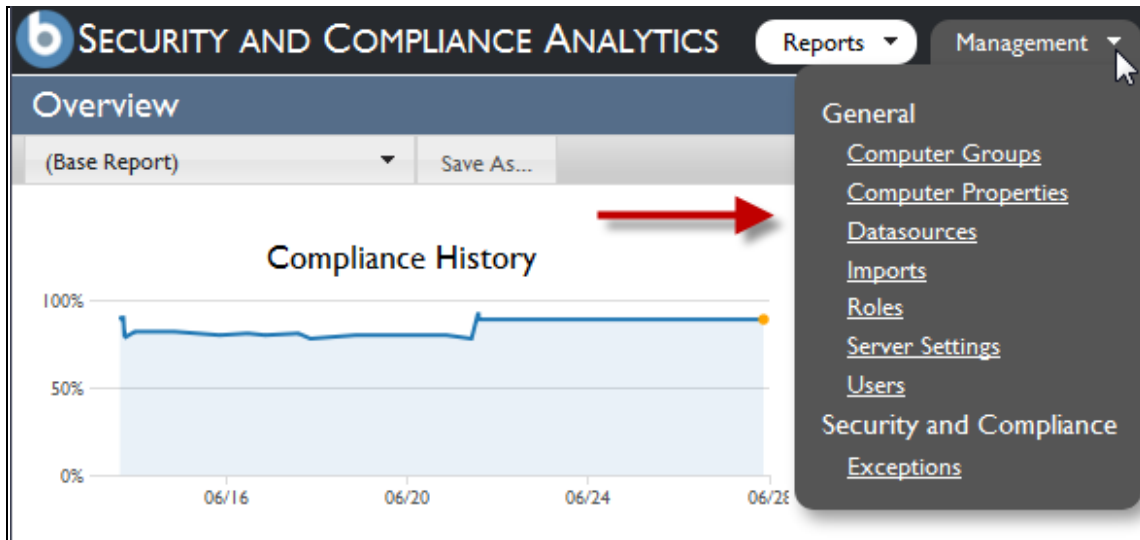
- Compliance Overview – Displays compliance history over time as an overall percentage
- Computers by Compliance Quartile - Bar chart that provides compliance data by quartile
- Compliance History Detail Chart - Win loss chart that displays compliance history over time
- Check Results History - Total 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





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 setting after initial setup, but you can add the Web Reports database information if you originally skipped this step.

General	1 row		
	Host	Database Name	Username
Computer Groups	localhost	BFEnterprise	<no data>
Computer Properties			
Datasources			
Imports			
Roles			
Server Settings			
Users			
Security and Compliance			
Exceptions			

Edit Datasource	
Primary Database	Web Reports Database (optional)
Host localhost	Host localhost
Database Name BFEnterprise	Database Name BESReporting
Authentication <input checked="" type="radio"/> Windows Authentication <input type="radio"/> SQL Server Authentication	Authentication <input checked="" type="radio"/> Windows Authentication <input type="radio"/> SQL Server Authentication
Save	

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.

General	Schedule
Computer Groups	Schedule times are based on client timezone.
Computer Properties	Time of day 08:58PM (PDT)
Datasources	Import Now
Imports	
Roles	
Server Settings	
Users	
Security and Compliance	
Exceptions	

Import		
Start Time	Username	Duration
06/28/2011 08:58 PM	Scheduled	0:02:25
06/27/2011 08:58 PM	Scheduled	0:04:25
06/26/2011 08:58 PM	Scheduled	0:02:54
06/25/2011 08:58 PM	Scheduled	0:02:23
06/24/2011 08:58 PM	Scheduled	0:03:14
06/23/2011 08:58 PM	Scheduled	0:02:53
06/22/2011 08:58 PM	Scheduled	0:03:55

Import Log	
Start Time: Wed Jun 29 03:58:10 UTC 2011	
Status: Successful	
Duration: 0:02:25	
# Logfile created on Wed Jun 29 03:58:10 +0000 2011 by logger.rb/99999	
2011-06-29 03:58:11 (+0100:00.000) Starting import tasks	
2011-06-29 03:58:11 (+0100:00.000) calling Model.before_snapshot	
2011-06-29 03:58:12 (+0100:00.983) Initialize datasource Datasource: Success	
2011-06-29 03:58:12 (+0100:00.015) ETL from Datasource - DatasourceUser Success	
2011-06-29 03:58:12 (+0100:00.000) ETL from Datasource - User Success	

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.

General	
Computer Groups	
Computer Properties	
Datasources	
Imports	
Roles	
Server Settings	
Users	
Security and Compliance	
Exceptions	

+ New Delete 3 rows	
Name	Permissions
Administrators	Edit Computer Groups,
Exit Exceptions	Edit Exceptions
import	Manage Imports

Edit Role	
Name	Administrators
Permissions	<input checked="" type="checkbox"/> Edit Computer Groups <input checked="" type="checkbox"/> Edit Exceptions <input checked="" type="checkbox"/> Manage Imports <input checked="" type="checkbox"/> Edit Computer Properties <input checked="" type="checkbox"/> Edit Datasources <input checked="" type="checkbox"/> Edit Roles <input checked="" type="checkbox"/> Edit Users <input checked="" type="checkbox"/> Edit Server Configuration
Save	

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.


General	
Computer Groups	
Computer Properties	
Datasources	
Imports	
Roles	
Server Settings	
Users	

Server Settings	
Port*	443
	<input checked="" type="checkbox"/> Use SSL
Certificate	replace
Common name	arroyo.qabigfix.com
Expiration date	06/14/2012
Restart service Save	



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.

General	
Computer Groups	<div><div>+ New</div><div> Delete</div><div>8 rows</div></div>
Computer Properties	
Datasources	
Imports	
Roles	
Server Settings	
Users	

Username	Roles	Authentication Method	Computer Group
bigfix	Administrators	Password	All Computers
exceptions	Exit Exceptions	Password	xp
normal	No Roles	Web Reports (Datasource)	No Computers
readonly	No Roles	Web Reports (Datasource)	win7
vincent I	Exit Exceptions	Web Reports (Datasource)	xp
import	import	Password	xp
xp32	No Roles	Password	32

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.

Server Settings	Reason	Checklist / Checks	Group / Computers	Expiration Date	Last edit by	Status
Users	DISA Stig XP	Checklist: DISA STIG on Windows...	1 computer	Never	exceptions	Active
Security and Compliance	Win 7	Checklist: DISA STIG on Windows...	1 computer	Never	bigfix	Active
	No passwords needed on Vista	2 checks	1 computer	Never	bigfix	Active
Exceptions						

Edit Exception

Reason

Enter a reason for this exception

Affected Checks

☒ All checks in checklist
 ☐ Selected checks

Checklist

DISA STIG on Windows 7 v1r2

Affected Computers

☐ All computers in group
 ☒ Selected computers

Computers

VSW7ULT32-01

add computers here

Expires

☐ 06/29/2012
 ☒ Never

Save

Exception History

Edit action	Action date	Reason	Checklist / Ch...	Group / Comp...	Expiration Date	Last edit by
create	06/16/2011 11:31...	Win 7	Checklist: DISA...	1 computer	Never	bigfix

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.

Tivoli Endpoint Manager Analytics

Reports
Management
Account
Help

Edit User

Username
admin

Roles
Administrators

Computer Group
All Computers

Password
Change

API Token
a20ede1ddcf8b71d67327718a50dedbe9ee660db
Regenerate

Email Address

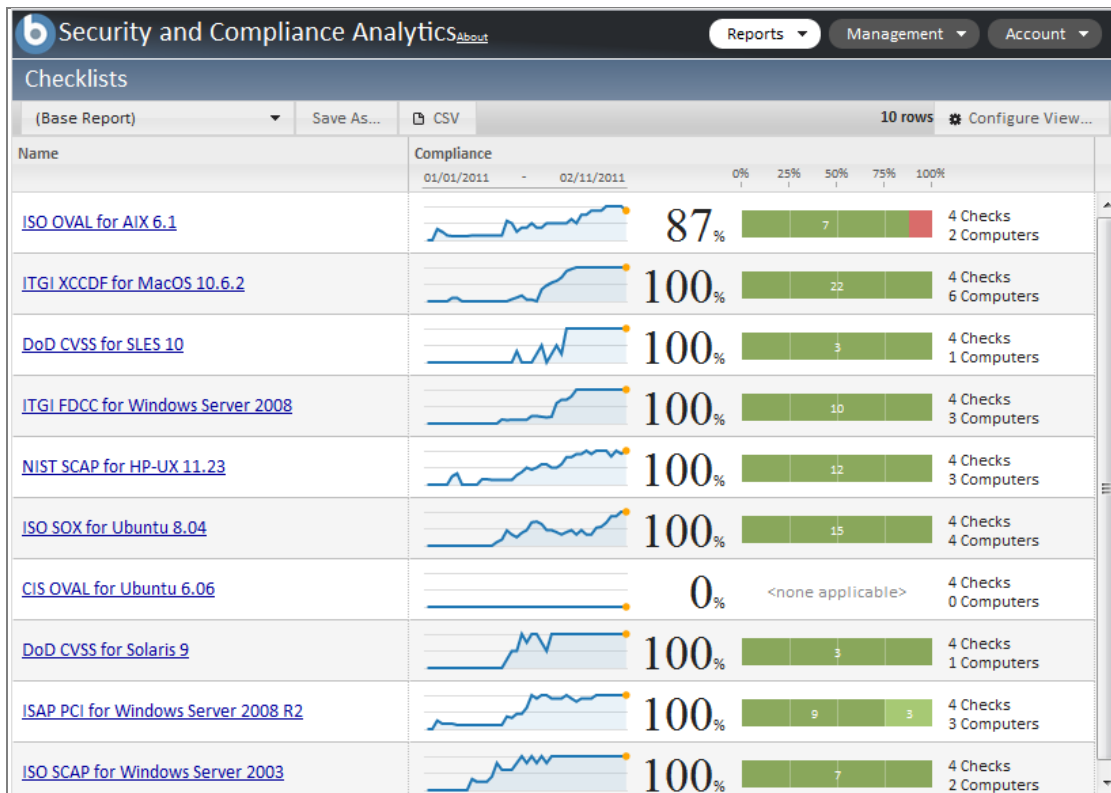
Contact Info

Save

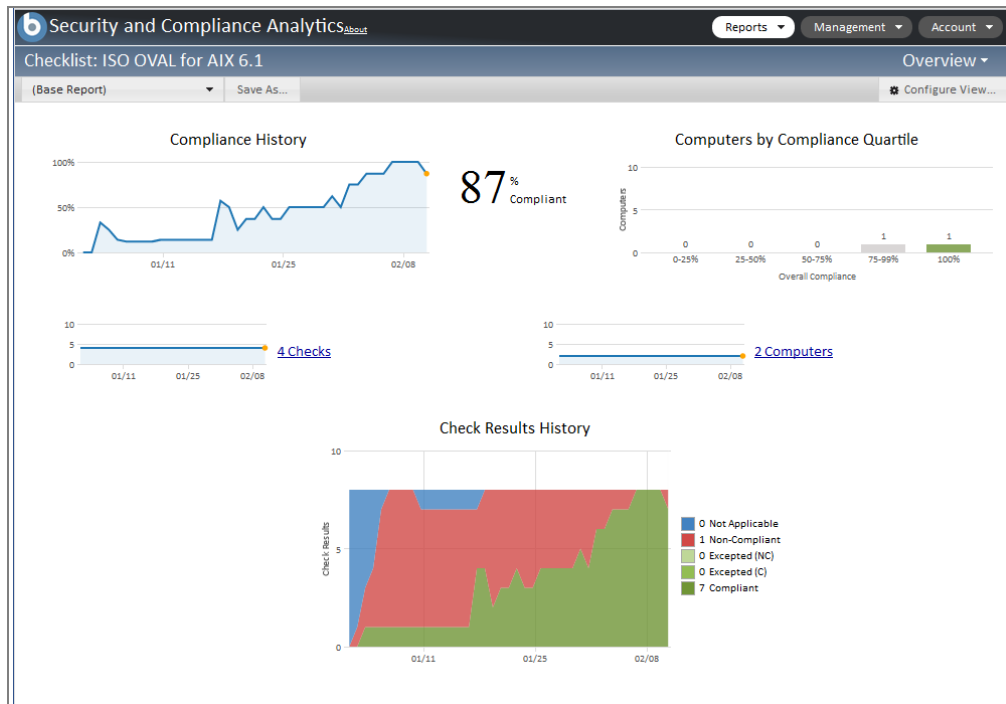
Example Reports

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

Checklist List Report



Checklist Overview Report



Checks List Report

Security and Compliance Analytics

Reports

Management

Account

Checks

(Base Report)

Save As...

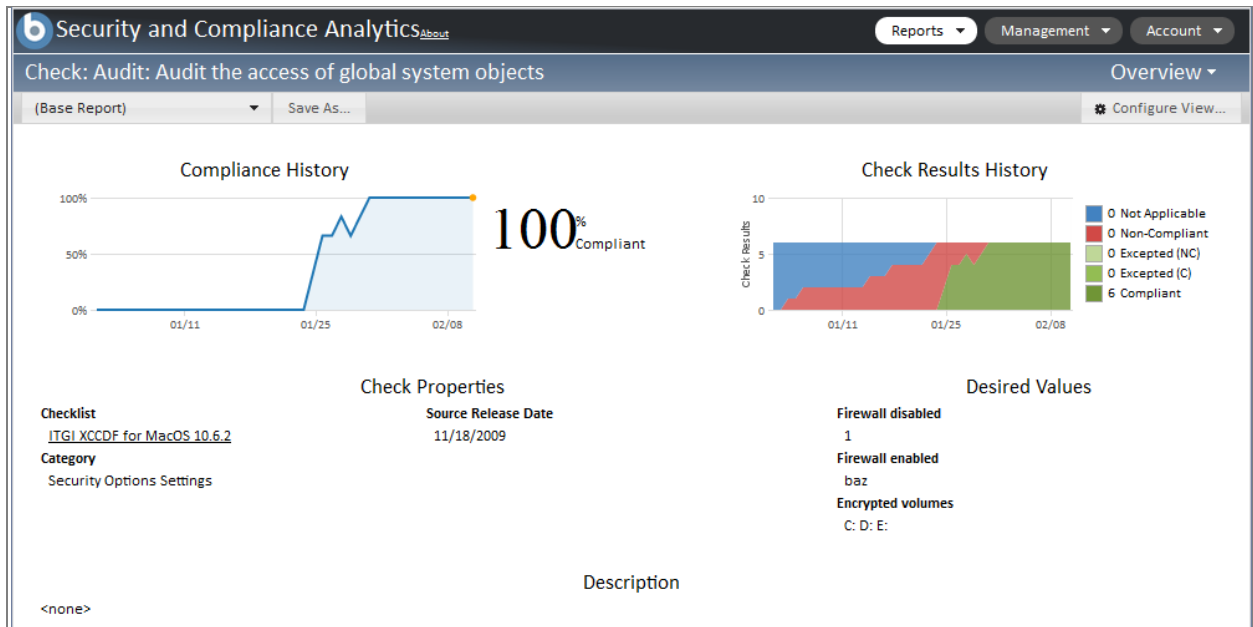
CSV

40 rows

Configure View...

Name	Compliance	0%	25%	50%	75%	100%
Administrators Have Right To Debug Programs		50%		2 Computers		
route.exe Permissions		100%		2 Computers		
ClipBook Service Disabled		100%		2 Computers		
Do Not Show First Use Dialog Boxes		100%		2 Computers		
attrib.exe Permissions		100%		6 Computers		
rexc.exe Permissions		100%		6 Computers		
Audit: Audit the access of global system objects		100%		6 Computers		
Display Error Notification		100%		6 Computers		
FTP Publishing Service Disabled		100%		1 Computers		
Enable user control over installs		0%	<none applicable>	1 Computers		
Error Reporting Service Disabled		100%		1 Computers		
Audit System Events		100%		1 Computers		

Check Overview Report



Computers List Report

b

Security and Compliance Analytics

About

Reports

Management

Account

Computers

(Base Report)

Save As...

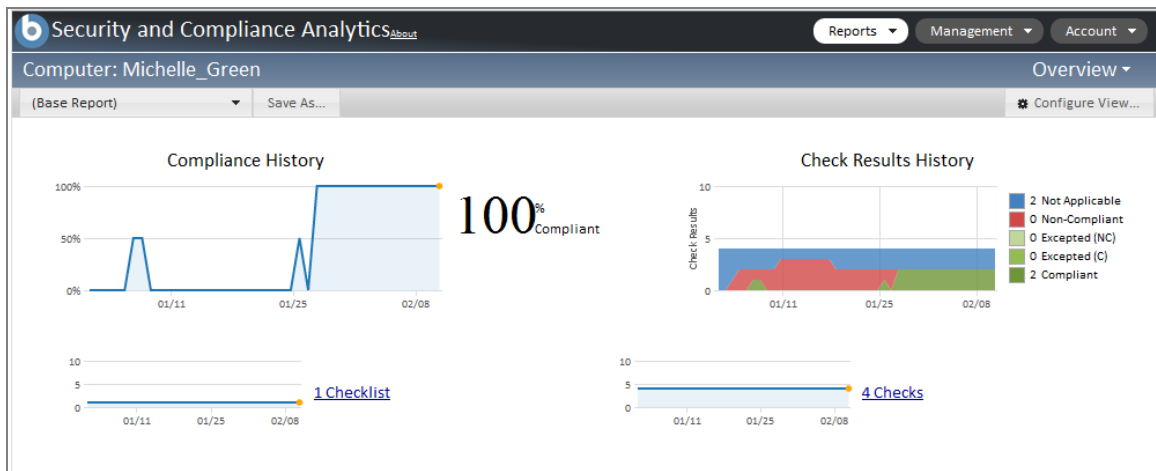
CSV

20 rows

Configure View...

Computer Name	Last Seen	Compliance	01/01/2011	02/11/2011	0%	25%	50%	75%	100%	
Kathleen_Gutierrez	40 minutes ago		100%		3	1	1 Checklists	4 Checks		
Patrick_Young	40 minutes ago		100%		4		1 Checklists	4 Checks		
Daniel_J	40 minutes ago		100%		7		2 Checklists	8 Checks		
Michelle_Green	40 minutes ago		100%		2		1 Checklists	4 Checks		
Scott_Thompson	40 minutes ago		100%		4		1 Checklists	4 Checks		
Frank_Diaz	40 minutes ago		100%		7		2 Checklists	8 Checks		
Kimberly_Williams	40 minutes ago		100%		4		1 Checklists	4 Checks		
Sharon_Robinson	40 minutes ago		100%		6		2 Checklists	8 Checks		

Computer Overview Report

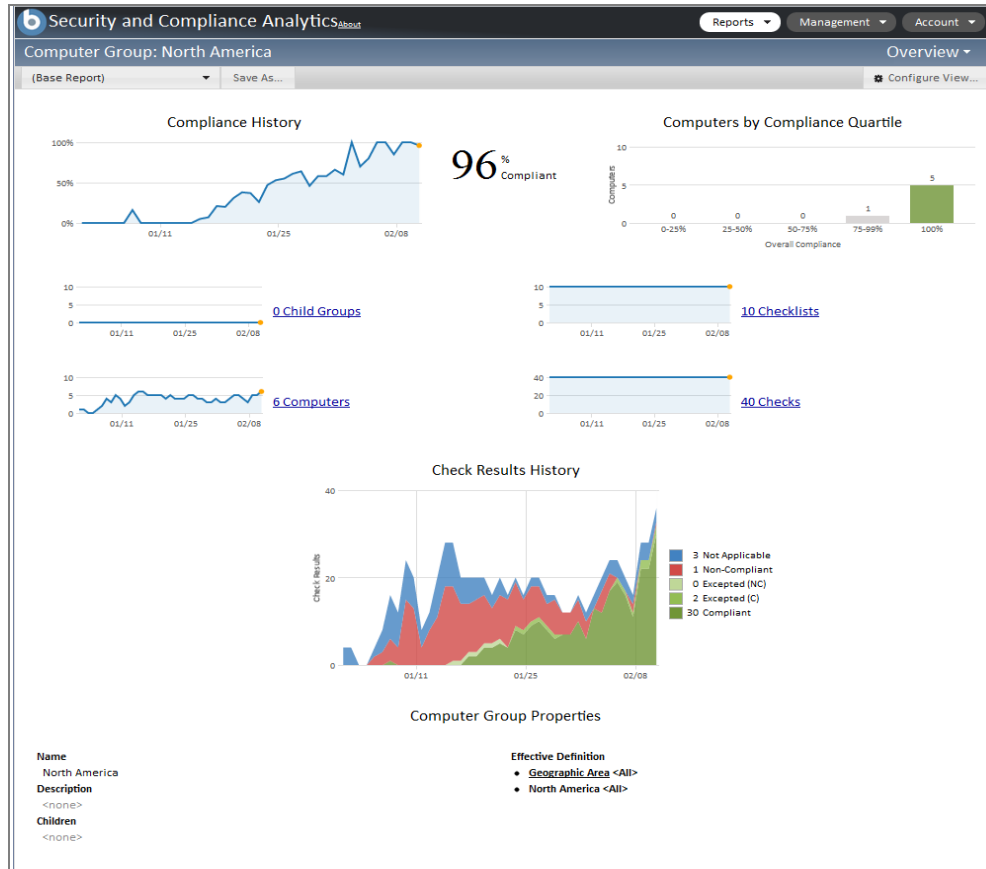


Computer Groups List Report





Computer Group Overview Report



Check Results List Report

Security and Compliance Analytics				
Check Results				
Checklist	Check Name	Computer Name	Last Seen	Compliance
ISO OVAL for AIX 6.1	Administrators Have Right To...	Pamela Collins	about an hour ago	Compliant
ISO OVAL for AIX 6.1	Administrators Have Right To...	Stephen Johnson	about an hour ago	Non-Compliant
ISO OVAL for AIX 6.1	route.exe Permissions	Pamela Collins	about an hour ago	Compliant
ISO OVAL for AIX 6.1	route.exe Permissions	Stephen Johnson	about an hour ago	Compliant
ISO OVAL for AIX 6.1	ClipBook Service Disabled	Pamela Collins	about an hour ago	Compliant
ISO OVAL for AIX 6.1	ClipBook Service Disabled	Stephen Johnson	about an hour ago	Compliant
ISO OVAL for AIX 6.1	Do Not Show First Use Dialog...	Pamela Collins	about an hour ago	Compliant
ISO OVAL for AIX 6.1	Do Not Show First Use Dialog...	Stephen Johnson	about an hour ago	Compliant
ITGI XCCDF for MacOS 10.6.2	attrib.exe Permissions	Patrick Young	about an hour ago	Compliant
ITGI XCCDF for MacOS 10.6.2	attrib.exe Permissions	Michelle Green	about an hour ago	Compliant



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
224A/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.