BigFix Compliance
Analytics User Guide

Special notice

Before using this information and the product it supports, read the information in Notices *(on page 123)*.

Edition notice

This edition applies to version 9.5 of BigFix and to all subsequent releases and modifications until otherwise indicated in new editions.

Contents

Chapter 1. Introduction..... 1

System Requirements..... 2

General Usage Concepts..... 6

Navigation..... 6

Graphical Report View..... 9

Configuring a report resource as the default view..... 9

Configuring a report resource as the home page..... 11

Using the autosize columns feature..... 12

Managing exceptions..... 14

Exporting..... 14

Chapter 2. Viewing deployment compliance status reports..... 15

Overview Reports..... 15

List Reports..... 16

Check Results Reports..... 20

Exceptions Reports..... 20

Saved Reports..... 23

Chart Types..... 24

Chapter 3. Working with patch reports..... 27

Enabling patch reporting..... 27

Report types..... 28

Overview reports..... 29

Patches report..... 30

Computers report..... 32

Computer Groups report..... 33
Saved reports..... 34
Managing reports..... 34
Enabling mail settings..... 36
Adding external sites..... 37
System requirements..... 43
Sample use cases..... 45
Chapter 4. Management Tasks..... 48
Computer Groups..... 49
Computer Properties..... 50
Data Sources..... 51
Adding a data source..... 52
Deleting a data source..... 57
Data Imports..... 57
Roles..... 58
Server Settings..... 59
Enabling TLS 1.2 with SQL Server..... 60
Session Settings..... 62
Directory Servers..... 64
Configuring a directory server that has a load balancer or multiple domain controllers..... 65
Adding a directory server..... 67
Single Sign-On Settings..... 68
Adding Exception to Exploit Protection Control Flow Guard in Windows 2019..... 76
Users..... 81

Configuring multiple computer groups..... 82
Configuring LDAP..... 83
Adding LDAP servers..... 83
Linking users to directories..... 84
Authenticating LDAP through user provisioning..... 85
Exceptions..... 85
Policy Management..... 86
Account Preferences..... 87
Chapter 5. Configuring report definitions using REST API..... 88
Create a saved report..... 91
Update a saved report..... 93
Retrieve all saved report items..... 96
Retrieve saved reports by report ID..... 97
Delete a saved report item by ID..... 99
Chapter 6. Disaster Recovery for BigFix Compliance Analytics..... 102
Creating a backup of the application server..... 102
Recovering the backup application server..... 103
Verifying the success of the recovery procedure..... 104
Appendix A. Example Reports - Compliance..... 105
Checklist List Report..... 107
Checklist Overview Report..... 108
Check Overview Report..... 109
Computers List Report..... 109
Checks List Report..... 110
Computer Overview Report..... 110

Computer Groups List Report.....111
Computer Group Overview Report.....112
Check Results List Report.....113
Vulnerabilities Report.....113
Appendix B. Example reports - Patch reports.....116
Overview.....118
Patches list.....119
Patch Details.....119
Computers list.....119
Computers Details.....120
Computer Groups list.....120
Computer Groups Details.....121
Appendix C. Support.....122
Notices.....123

Chapter 1. Introduction

HCL® BigFix Compliance Analytics (formerly known as Security Compliance and Analytics, or SCA) is a component of BigFix Compliance, which includes vulnerability detection libraries and technical controls and tools that are based on industry practices and standards for endpoint and server security configuration (SCM checklists). The vulnerability detection libraries and the technical controls enable continuous, automated detection and remediation of security configuration issues.

BigFix Compliance Analytics provides report views and tools for managing the vulnerability of SCM checks.

BigFix Compliance Analytics generates the following reports, which can be filtered, sorted, grouped, customized, or exported with the use of any set of Endpoint Manager properties:

- Overviews of Compliance Status, Vulnerabilities, and History
- Checklists: Compliance Status and History
- Checks: Compliance Status, Values, and History
- Vulnerabilities: Rollup Status and History
- Vulnerability Results: Detailed Status
- Computers: Compliance Status, Values, Vulnerabilities, and History
- Computer Groups: Compliance Status, Vulnerabilities, and History
- Exceptions: Management, Status, and History

New features

The following features and enhancements are included in BigFix Compliance version 1.9.

- Policy feature, which is a collection of checklists for PCI users that allows for aggreration and rollups across multiple checklists. For more information, see the BigFix Compliance Payment Card Industry (PCI) Add-on User's Guide.
- Receive e-mail notifications for failed imports and when unexpected changes to target reports occur (which includes disparity in expected number of rows and when the number of rows are updated on a saved report.)

- Lines with lengthy content entries are wrapped on the Grid Report View and on PDF grid reports.
- Use of BigFix Compliance and BigFix Inventory on the same server without any session key conflicts.
- Improved viewing - The Overview page does not display the Vulnerability Overview if there is no report about vulnerability
- Upgrade to Ruby on Rails version 4.2
- Update of JRE to 8.0.4.10
- Support of upgrades from earlier versions of Compliance. For more information, see Upgrading from earlier versions of BigFix Compliance Analytics.

System Requirements

Set up your deployment according to the system requirements to successfully deploy BigFix Compliance Analytics.

Configure your BigFix Compliance Analytics deployment according to the following requirements:

Table 1. Supported components and system requirements to deploy BigFix Compliance Analytics

Components	Requirements
Supported browser versions	• Internet Explorer versions 10.0, 11.0 • Firefox 31 and later versions • Firefox Extended Support Release (ESR) versions 24 and 31 • Google Chrome 35.0 and later versions
Supported HCL BigFix component versions	• Console versions 9.0, 9.1, 9.2, 9.5 • Web Reports versions 9.0, 9.1, 9.2, 9.5 • Windows Client versions 9.0, 9.1, 9.2, 9.5 • UNIX Client versions 9.0, 9.1, 9.2, 9.5

Table 1. Supported components and system requirements to deploy BigFix Compliance Analytics

(continued)

Components	Requirements
SCA server operating system requirements	• Microsoft Windows Server 2008 (64-bit only) • Microsoft Windows Server 2008 R2 • Microsoft Windows Server 2012 • Microsoft Windows 2012 R2 • Microsoft Windows Server 2016 **Note:** BigFix Compliance Analytics supports operating systems with the 64-bit versions only.
SCA database server requirements	• Microsoft SQL Server 2008 R2 • Microsoft SQL Server 2012 • Microsoft SQL Server 2014 • Microsoft SQL Server 2016
SCA server	You must have Administrator privileges on the target SCA server.
SCA database	You must have dbcreator permissions on the target SCA database. server.
HCL BigFix database user permissions	HCL BigFix database user permissions
SCM mastheads and Fixlet sites	• You might have earlier BigFix Fixlets, HCL BigFix 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. • To view the current list of SCM sites that are supported with SCA, see the SCM Checklists.

Table 1. Supported components and system requirements to deploy BigFix Compliance Analytics

(continued)

Components	Requirements
HCL BigFix DB2 database permissions	You must have data administration authority (DATAACCESS) to perform the following tasks: • Access to create objects • Access to data within an HCL BigFix DB2 database
HCL BigFix database permissions for datasources	You must have the following MSSQL and DB2 permissions to perform tasks related to datasource. **MSSQL** **Note:** MSSQL requires dbcreator permissions at a minimum. The following permission requirements are required for the datasource related tasks. • SELECT, EXECUTE • During set up or when upgrading: CREATE SCHEMA, CREATE TABLE, CREATE VIEW, CREATE FUNCTION **DB2** • DATAACCESS • During set up or when upgrading: DBADM
Server API credentials for PCI DSS policy sites users	Using the PCI DSS policy sites requires providing additional BigFix API user credentials for each datasource that uses PCI. Users must have master operator credentials or must meet the following minimum requirements:

Table 1. Supported components and system requirements to deploy BigFix Compliance Analytics

(continued)

Components	Requirements
	• Can use REST API • Have reader permission for the PCI DSS Reporting site

BigFix Compliance End of Support (EOS)

BFC Server (or BFC Analytics, previously SCA) is a BigFix Compliance application and so has its own versioning. BigFix Compliance version is the official marketing version of BigFix Compliance, however, it does not denote the version of the BFC Server code. Under each BigFix Compliance version, the BFC development team releases application updates, which are numbered independently. The EOS date of BFC is the same as that of BigFix Compliance.

The following table lists the releases and EOS date of BigFix Compliance (previously Security and Compliance) and BFC Server.

Table 2. End of Support date of BigFix Compliance (previously Security and Compliance) and BFC Server

BigFix Compliance versions	BigFix Compliance Analytics/BFC versions	End of Support date
8.2.x	1.4.x	2016-04-30
9.0.x	1.4.x	2016-04-30
9.1.x	1.5.x	2017-09-30
9.2.x	1.6.x, 1.7.x, 1.8.x	2020-03-31

Table 3. SCA and BES: Support Matrix

BigFix Compliance versions	BigFix Compliance Analytics/BFC versions
9.5.x	1.8.x, 1.9.x, 1.10.x, 2.0.x

General Usage Concepts

Navigation

Using BigFix Compliance Analytics, 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 HCL BigFix 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.

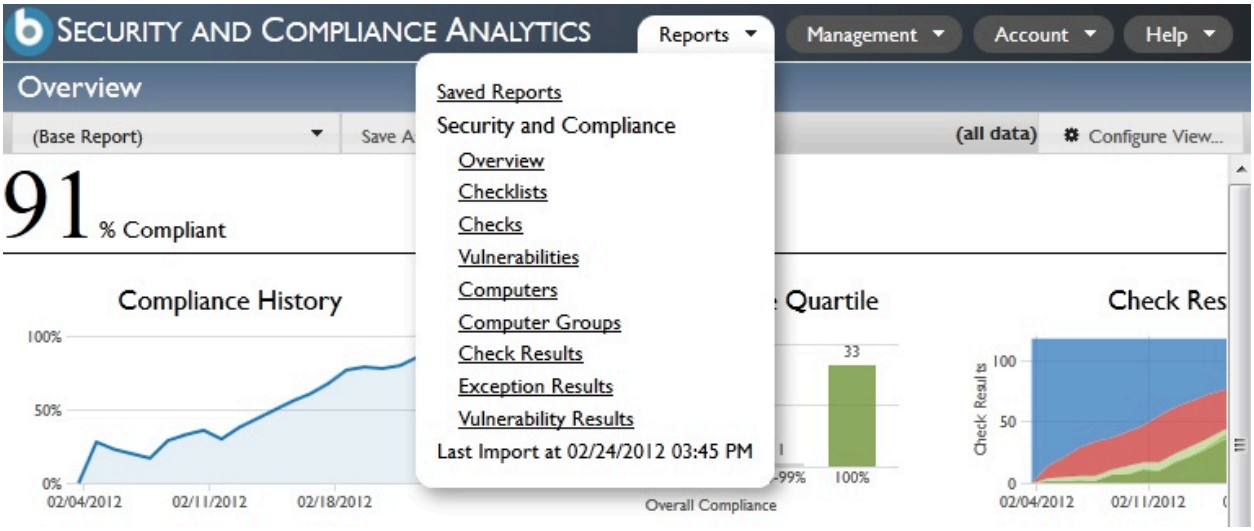
SCM check results are aggregated by the BigFix Compliance Analytics server and augmented by computer properties and analysis values to provide compliance overviews and detailed lists of results.

There are four primary navigation mechanisms in BigFix Compliance Analytics:

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

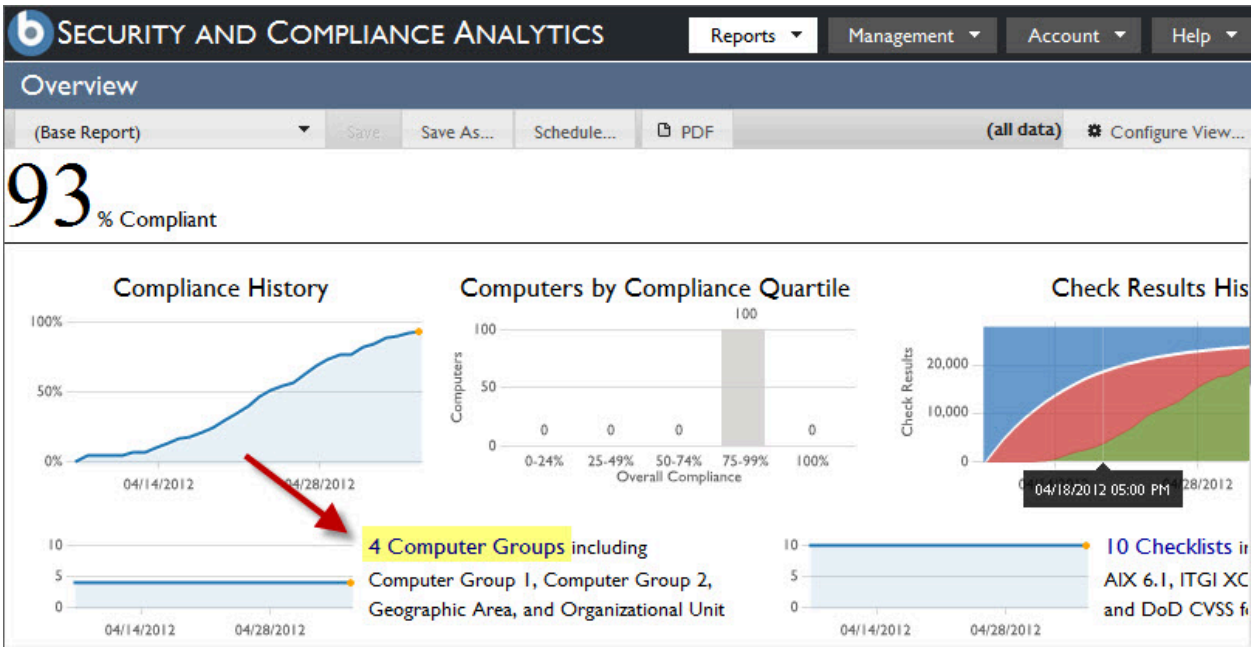
Global Navigation

Global Navigation refers to the primary dropdown menus at the top of the BigFix Compliance Analytics 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.



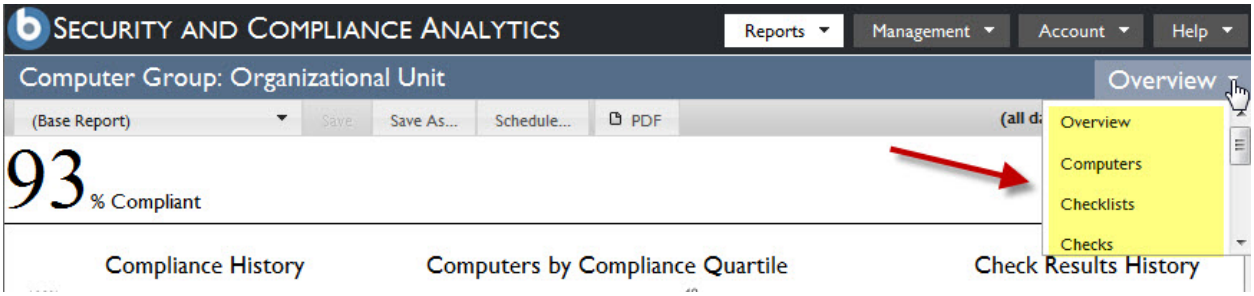
Linked Navigation

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.



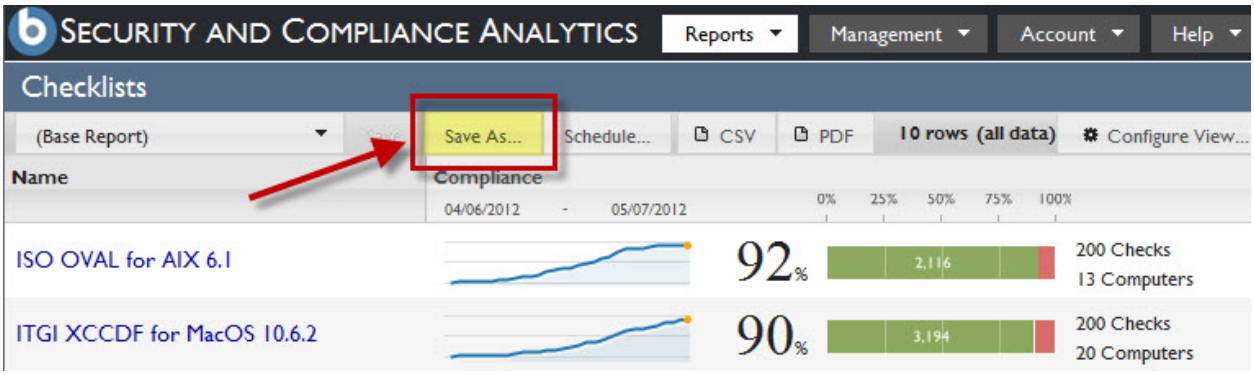
Sub-navigation

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 that is located on the upper-right side of any overview report. The *List View* of reports will not show the *Overview* dropdown.



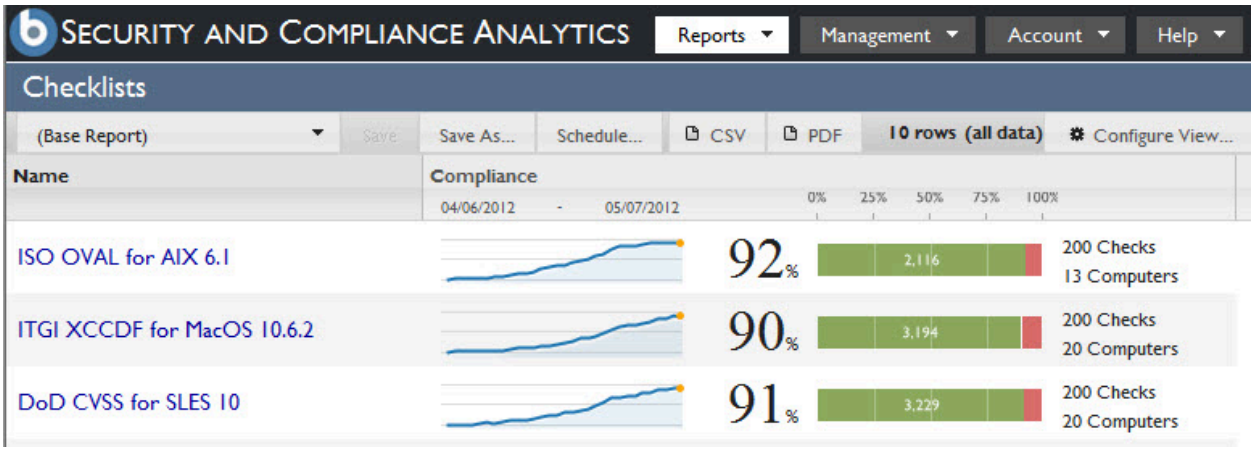
Saved Reports navigation

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.



Configuring a report resource as the default view

Set default views for report resources to reduce steps that are needed to access reports when you are loading resources.

Use the Set as default option to configure a specific report as the default view when you are loading any report. The option reduces the steps that are needed to access reports when you are loading resources, including the following resources.

- Overview
- Detailed report views
- Grid report views for checklists, vulnerabilities, exceptions, computers, and computer groups

Users can set the default view based on their credentials:

- Standard users can configure reports to have private or default view settings.
- Administrators can configure reports to have private, default, or global default view settings.

You can set a report to have the following settings:

Private

This option makes the report private.

Set as default

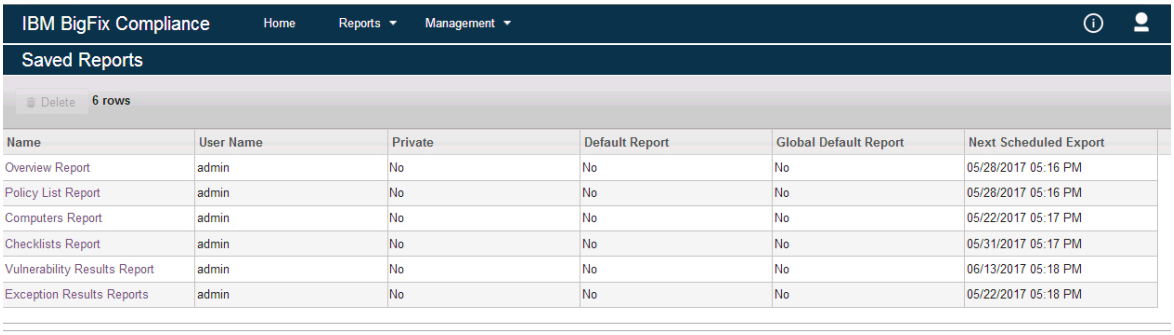
This option saves the report as the default view for the user of that specific report page.

Set as global default

This option saves the report as the global view for all users of that specific report who do not have it set as their default report page.

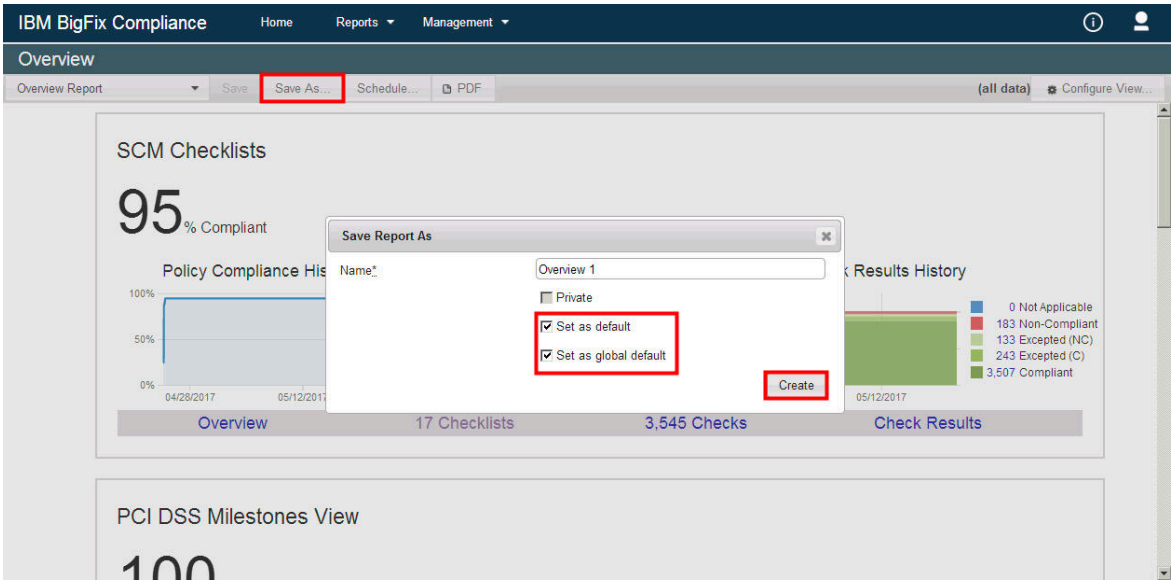
Only administrators can save reports to have a global default view. However, when a standard user already set a report as the default, the administrator cannot overwrite that default report view.

1. Go to **Reports > Saved Reports** and select the report that is to be saved as the default report view.

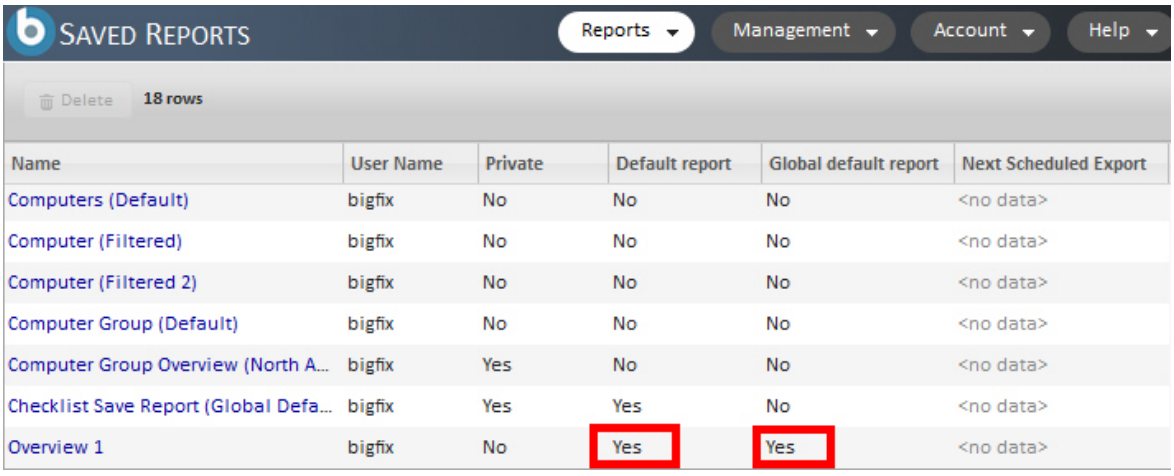


2. From the **Edit Report** panel, configure the report to be viewed with any of the following options.

- Private
- Set as default
- Set as global default



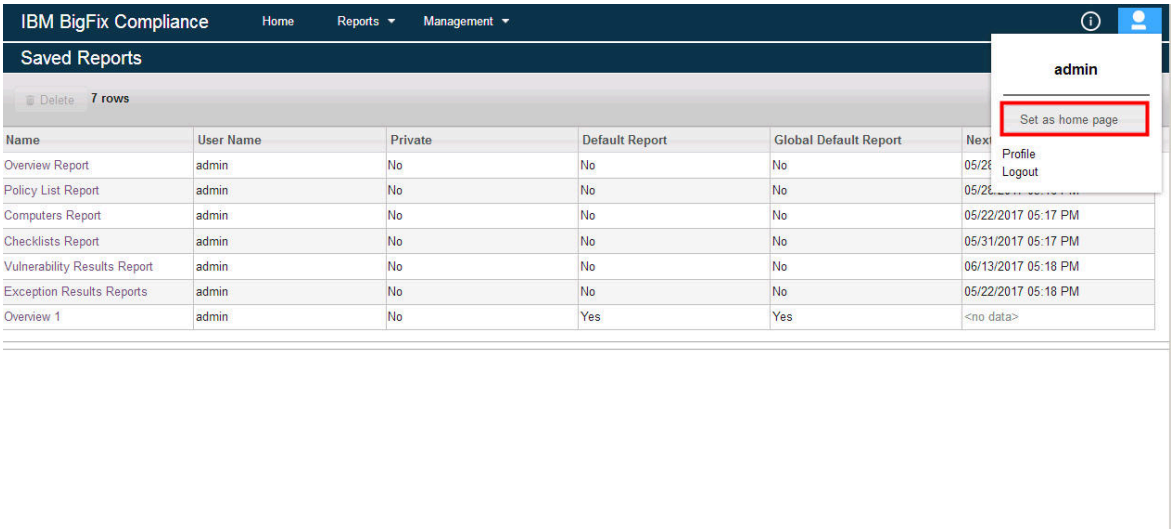
3. Click **Create**.



Configuring a report resource as the home page

Set any page or report resource, including saved reports, as the home page.

1. Go to the page you want to set as the home page.
2. From the upper right corner, select the **Account** menu and click **Set as home page**. When a page is currently set as the home page, the option is disabled.



Your next login will open to the page you selected.

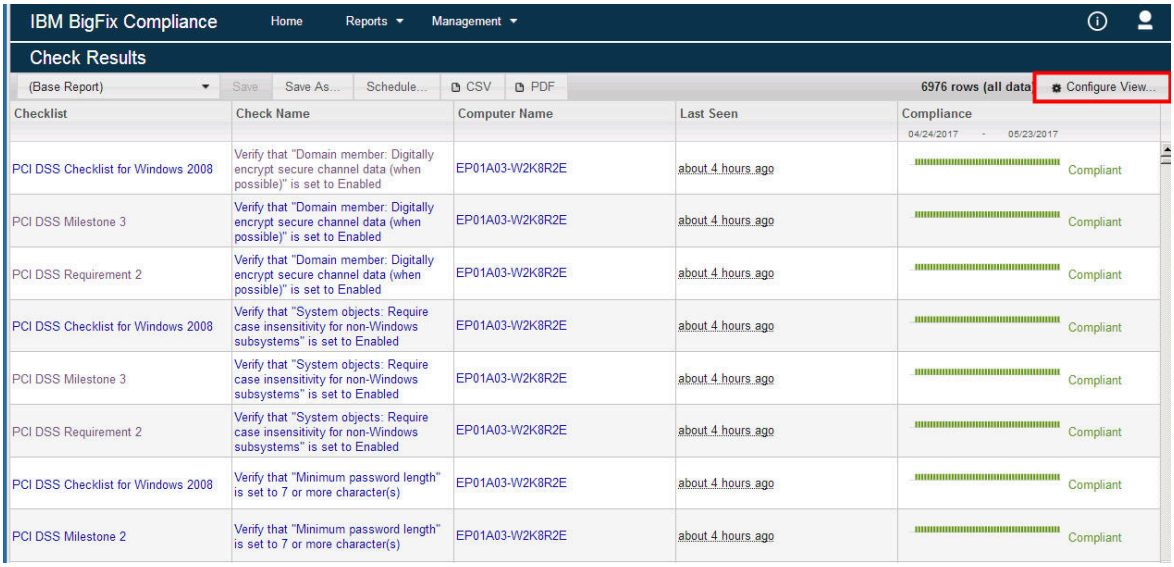
Using the autosize columns feature

Columns in BigFix Compliance Analytics reports are set by default to automatically resize to fit a grid window.

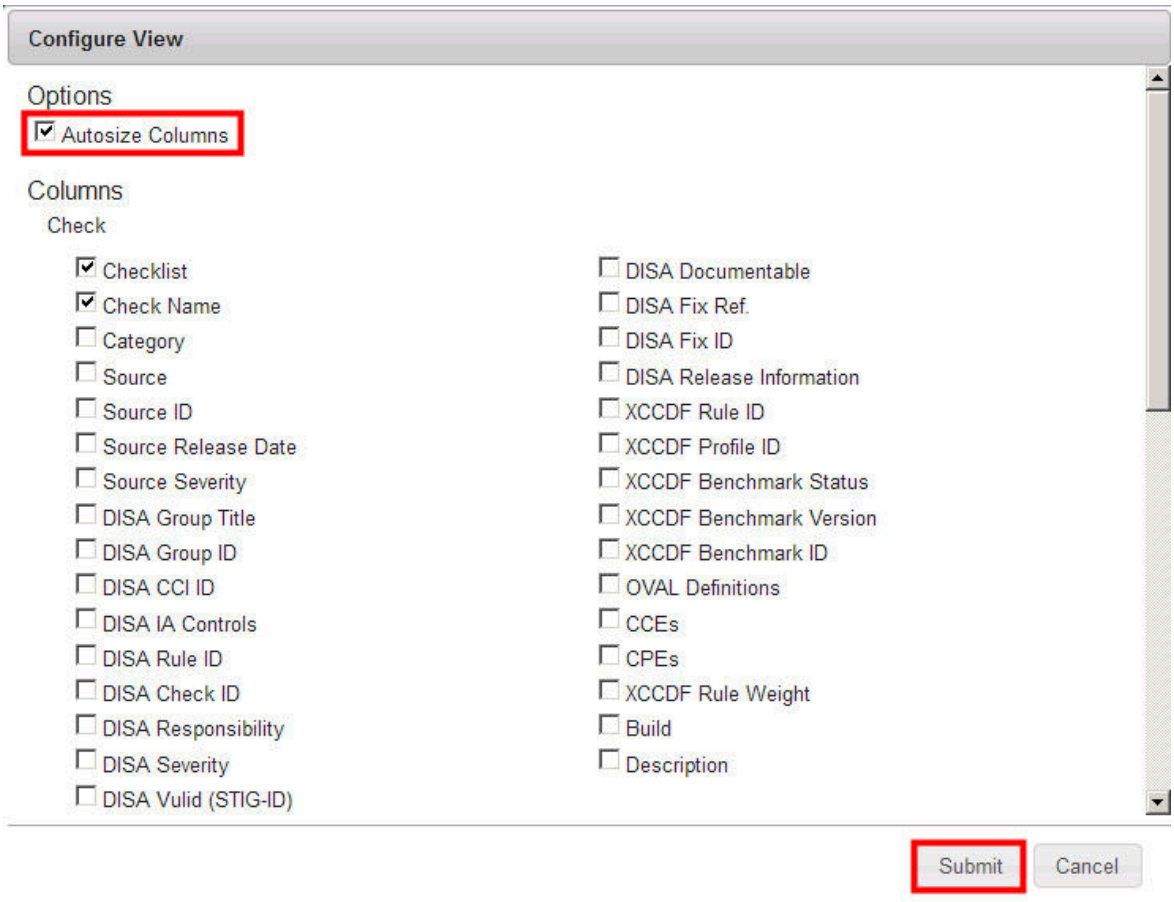
When the report you are using has several columns, you can use the Autosize Columns feature to view several columns without compressing the column views. You can also scroll horizontally across the visible report grid window. You can also set the autosize feature when you are creating a saved report. When creating a saved report with Autosize Columns disabled, it will retain all column widths even if the column widths exceed or are less than the visible grid area.

This feature is enabled by default.

1. From an open report that uses columns, click **Configure View...**.



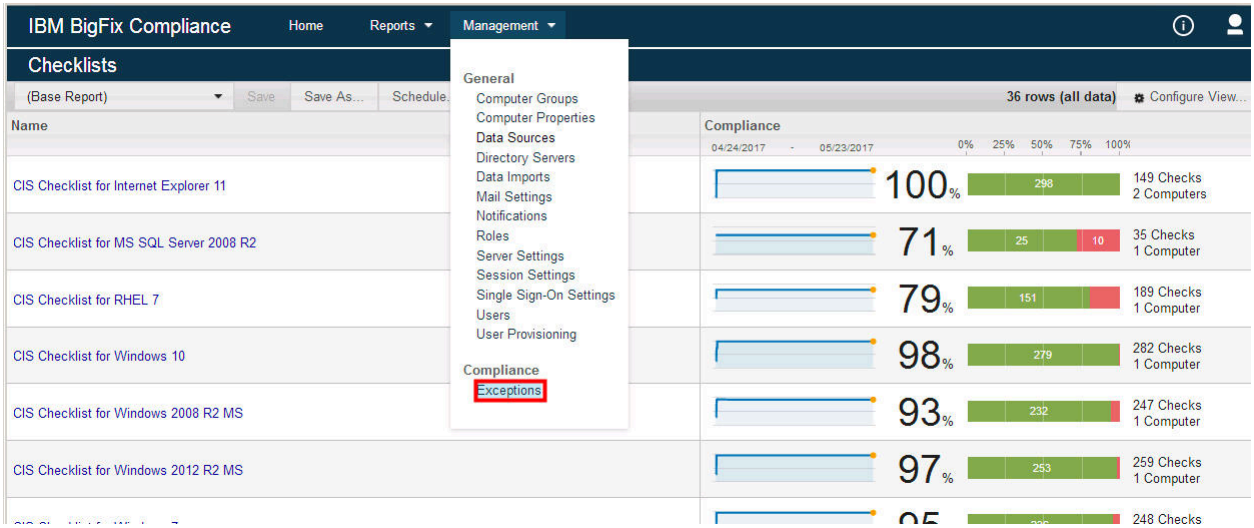
2. From the **Configure View** windows, you can either select or clear the **Autosize Columns** checkbox.



3. Click **Submit**.

Managing exceptions

Set exceptions to exclude data from your compliance reports. From the Management drop-down menu, click *Exceptions*.



Exporting

You can export the data view of most report views to a .CSV or .PDF formatted file on your local computer. Click the *.CSV* or *.PDF* links on the top bar of the console.

Chapter 2. Viewing deployment compliance status reports

You can view the compliance status in your deployment from any of the four report types.

BigFix Compliance Analytics 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.

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 window in the Security Configuration Management 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 logged-in users.

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 logged in users.

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 logged in users.

Vulnerability Overview

Shows information about a single vulnerability check (such as vulnerability properties, CVSS score metrics, and vulnerability description) and overall, historical aggregate compliance for the vulnerability evaluated by all computers visible to logged in users.

Note: The Overview page does not display the Vulnerability Overview if there is no report about vulnerability.

List Reports

Click **Reports** to find the following reports:

Checklist List

Shows the list of checklists in the deployment together 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 together 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

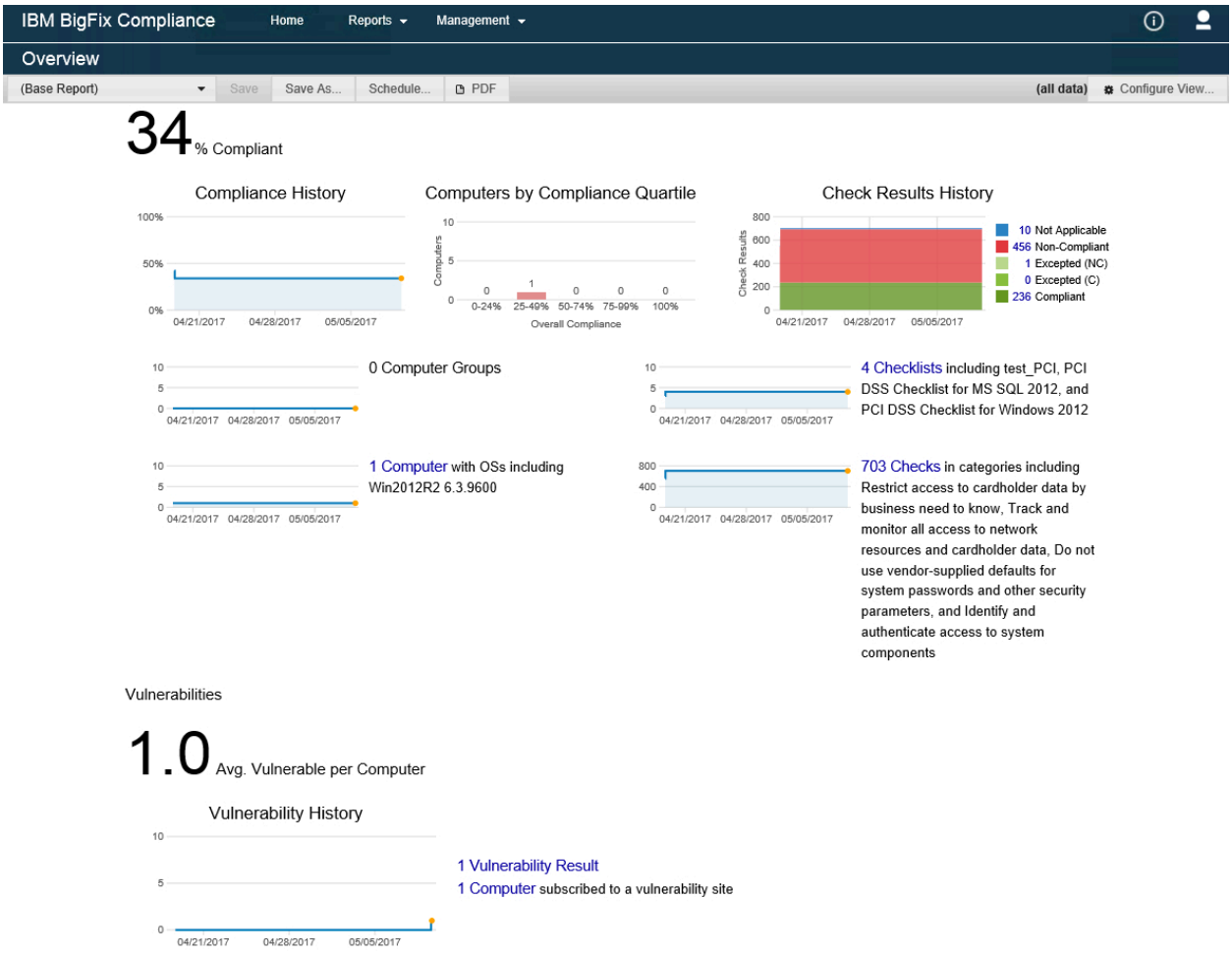
Shows the list of all computers in the given scope visible to the logged-in user together with attributes of each computer and the overall, historical aggregate compliance results of all checks evaluated on the computer.

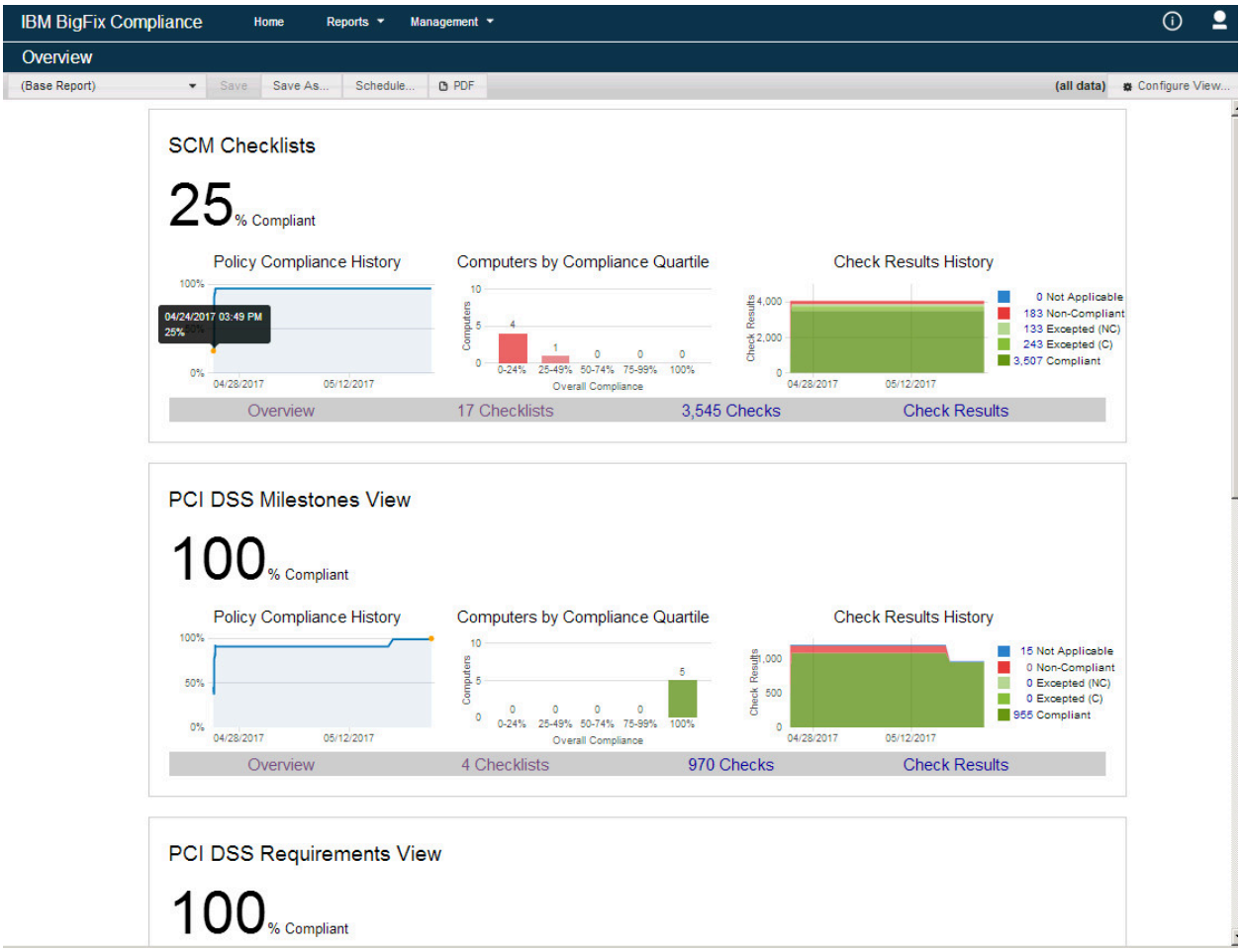
Computer Groups List

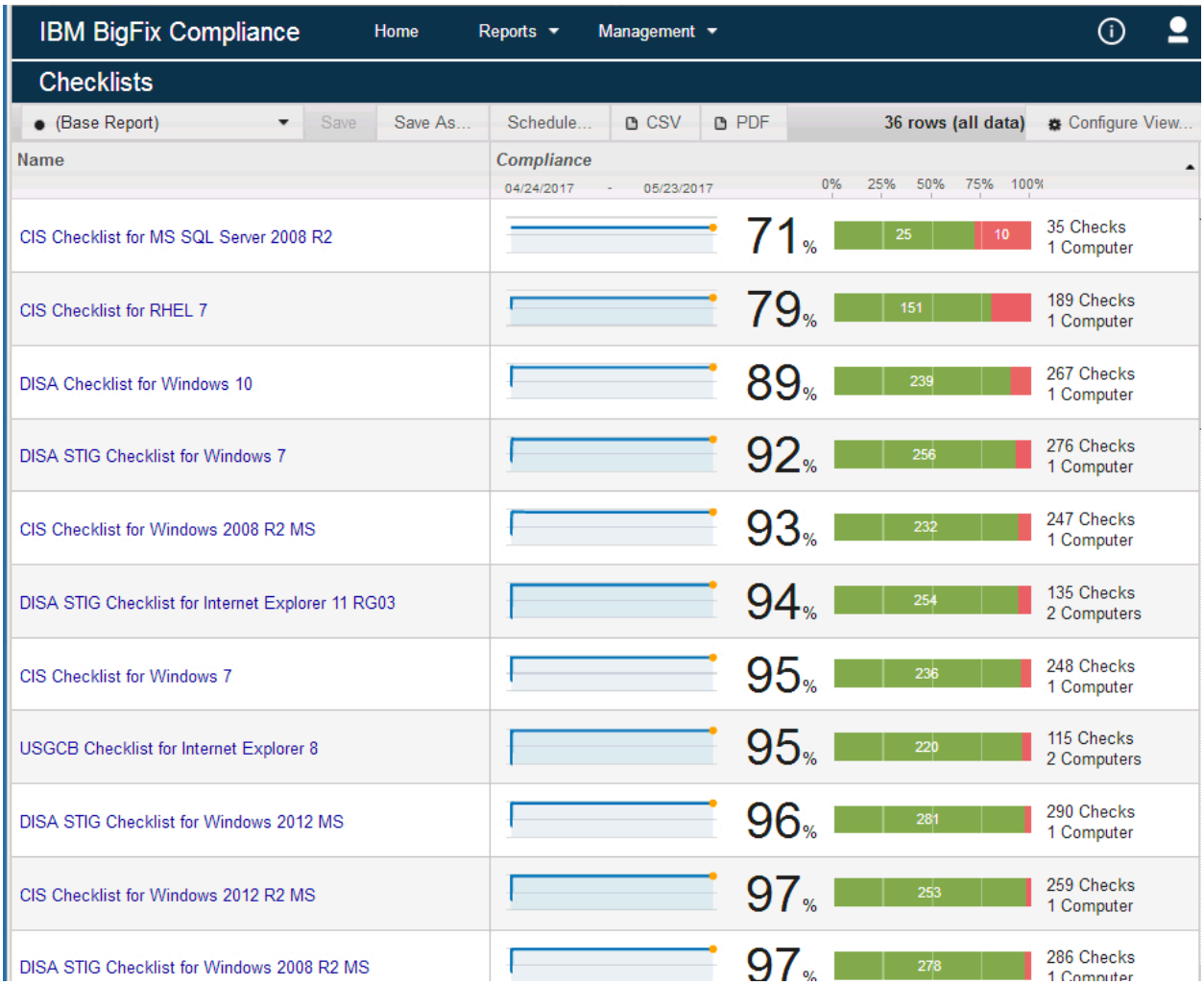
Shows the list of all computer groups in the given scope visible to the logged-in user together with attributes of each group and the overall, historical aggregate compliance results of all checks on all computers in each group.

Vulnerabilities List

Shows the list of vulnerability checks in the given scope visible to the logged-in user together with attributes of each computer and the overall, historical aggregate vulnerability results of all vulnerability checks evaluated on the computer.


IBM BigFix Compliance
Home
Reports
Management
Overview
(Base Report)
Save
Save As...
Schedule...
PDF
(all data)
Configure View...
34 % Compliant
Compliance History
100%
50%
0%
04/21/2017
04/28/2017
05/05/2017
Computers by Compliance Quartile
Computers
10
5
0
0
1
0
0
0
0-24%
25-49%
50-74%
75-99%
100%
Overall Compliance
Check Results History
Check Results
800
600
400
200
0
10 Not Applicable
456 Non-Compliant
1 Excepted (NC)
0 Excepted (C)
236 Compliant
0 Computer Groups
4 Checklists including test_PCI, PCI DSS Checklist for MS SQL 2012, and PCI DSS Checklist for Windows 2012
1 Computer with OSs including Win2012R2 6.3.9600
703 Checks in categories including Restrict access to cardholder data by business need to know, Track and monitor all access to network resources and cardholder data, Do not use vendor-supplied defaults for system passwords and other security parameters, and Identify and authenticate access to system components
Vulnerabilities
1.0 Avg. Vulnerable per Computer
Vulnerability History
1 Vulnerability Result
1 Computer subscribed to a vulnerability site


IBM BigFix Compliance
Home
Reports
Management
Overview
(Base Report)
Save
Save As...
Schedule...
PDF
(all data)
Configure View...
SCM Checklists
25 % Compliant
Policy Compliance History
100%
0%
04/24/2017 03:49 PM
25%
04/28/2017
05/12/2017
Computers by Compliance Quartile
Computers
10
5
0
4
1
0
0
0
0-24%
25-49%
50-74%
75-99%
100%
Overall Compliance
Check Results History
Check Results
4,000
2,000
0
04/28/2017
05/12/2017
0 Not Applicable
183 Non-Compliant
133 Excepted (NC)
243 Excepted (C)
3,507 Compliant
Overview
17 Checklists
3,545 Checks
Check Results
PCI DSS Milestones View
100 % Compliant
Policy Compliance History
100%
50%
0%
04/28/2017
05/12/2017
Computers by Compliance Quartile
Computers
10
5
0
0
0
0
0
5
0-24%
25-49%
50-74%
75-99%
100%
Overall Compliance
Check Results History
Check Results
1,000
500
0
04/28/2017
05/12/2017
15 Not Applicable
0 Non-Compliant
0 Excepted (NC)
0 Excepted (C)
955 Compliant
Overview
4 Checklists
970 Checks
Check Results
PCI DSS Requirements View
100 % Compliant

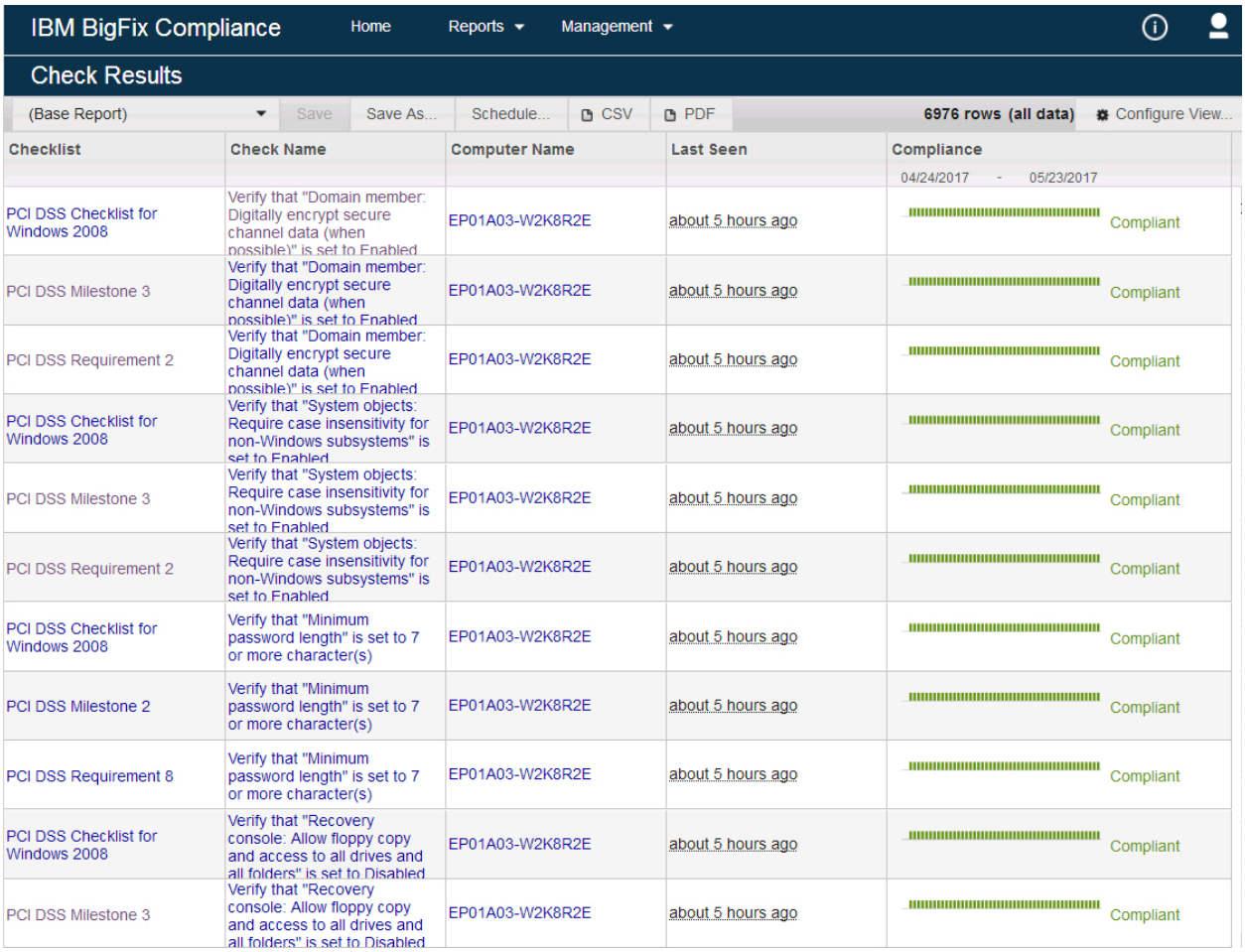


Check Results Reports

The Check Results 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

The Exceptions Report shows the list and status of exceptions in the given scope applied to each computer visible to the logged-in user, together with attributes of each check, each computer, and each exception.

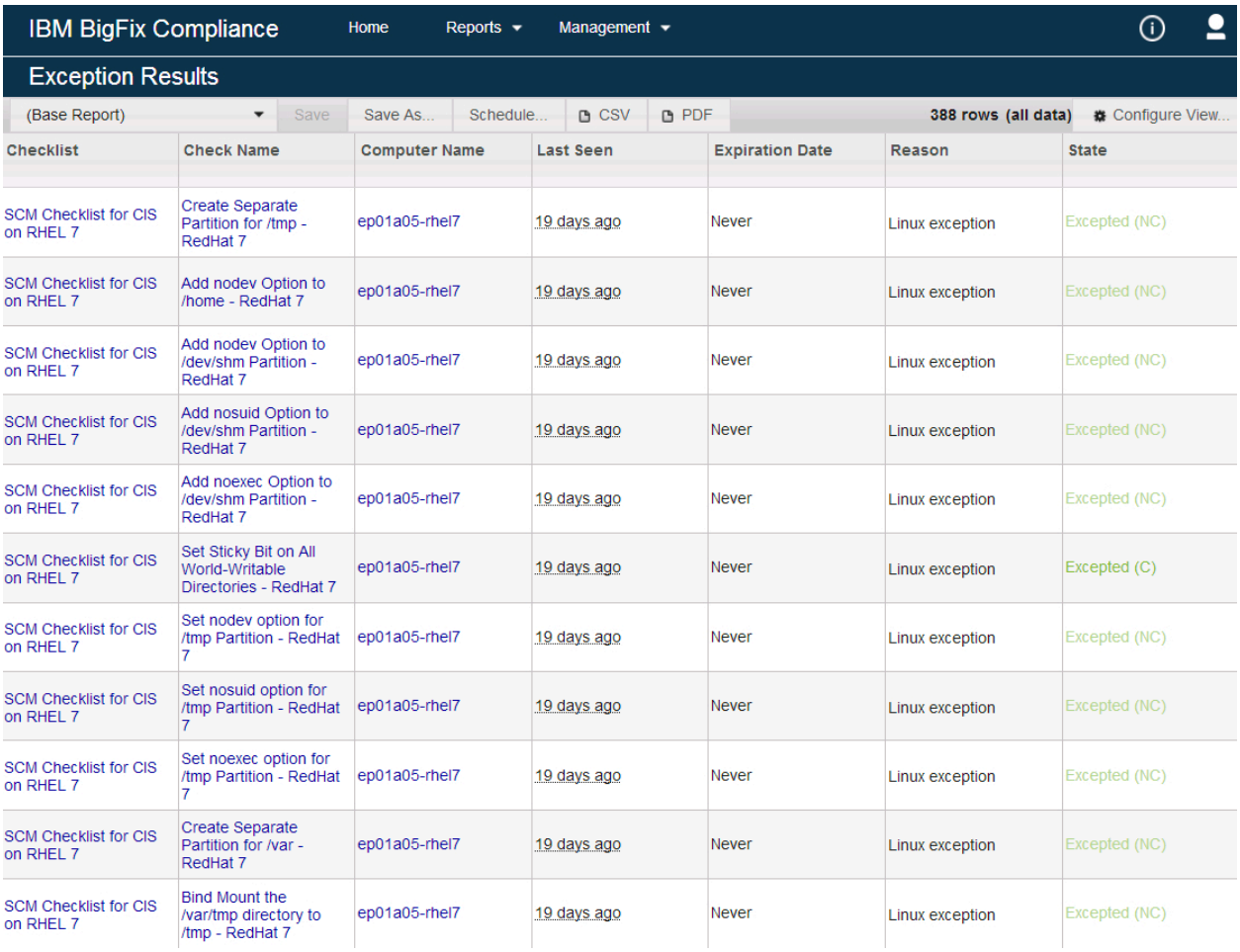


IBM BigFix Compliance Home Reports Management

Check Results

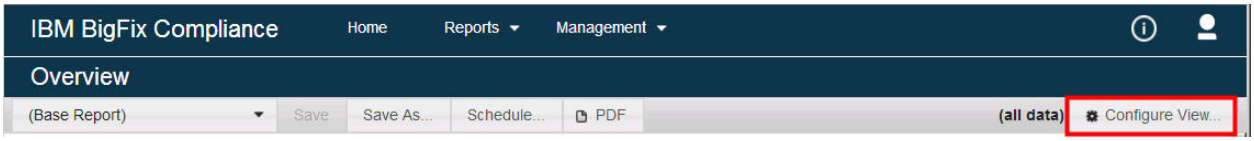
(Base Report) Save Save As... Schedule... CSV PDF 6976 rows (all data) Configure View...

Checklist	Check Name	Computer Name	Last Seen	Compliance 04/24/2017 - 05/23/2017
PCI DSS Checklist for Windows 2008	Verify that "Domain member: Digitally encrypt secure channel data (when possible)" is set to Enabled	EP01A03-W2K8R2E	about 5 hours ago	Compliant
PCI DSS Milestone 3	Verify that "Domain member: Digitally encrypt secure channel data (when possible)" is set to Enabled	EP01A03-W2K8R2E	about 5 hours ago	Compliant
PCI DSS Requirement 2	Verify that "Domain member: Digitally encrypt secure channel data (when possible)" is set to Enabled	EP01A03-W2K8R2E	about 5 hours ago	Compliant
PCI DSS Checklist for Windows 2008	Verify that "System objects: Require case insensitivity for non-Windows subsystems" is set to Enabled	EP01A03-W2K8R2E	about 5 hours ago	Compliant
PCI DSS Milestone 3	Verify that "System objects: Require case insensitivity for non-Windows subsystems" is set to Enabled	EP01A03-W2K8R2E	about 5 hours ago	Compliant
PCI DSS Requirement 2	Verify that "System objects: Require case insensitivity for non-Windows subsystems" is set to Enabled	EP01A03-W2K8R2E	about 5 hours ago	Compliant
PCI DSS Checklist for Windows 2008	Verify that "Minimum password length" is set to 7 or more character(s)	EP01A03-W2K8R2E	about 5 hours ago	Compliant
PCI DSS Milestone 2	Verify that "Minimum password length" is set to 7 or more character(s)	EP01A03-W2K8R2E	about 5 hours ago	Compliant
PCI DSS Requirement 8	Verify that "Minimum password length" is set to 7 or more character(s)	EP01A03-W2K8R2E	about 5 hours ago	Compliant
PCI DSS Checklist for Windows 2008	Verify that "Recovery console: Allow floppy copy and access to all drives and all folders" is set to Disabled	EP01A03-W2K8R2E	about 5 hours ago	Compliant
PCI DSS Milestone 3	Verify that "Recovery console: Allow floppy copy and access to all drives and all folders" is set to Disabled	EP01A03-W2K8R2E	about 5 hours ago	Compliant

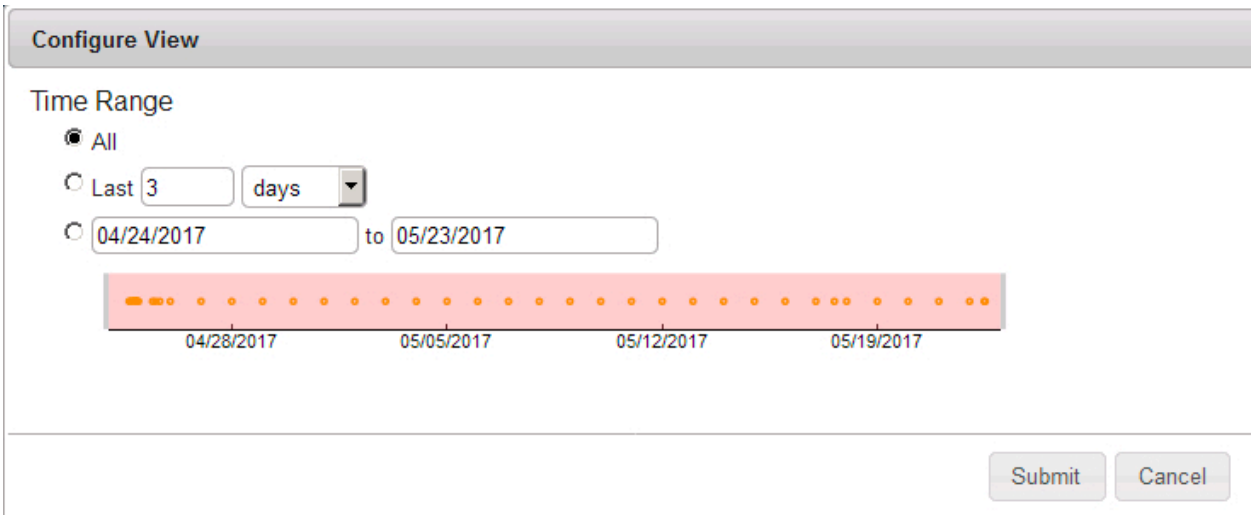


Checklist	Check Name	Computer Name	Last Seen	Expiration Date	Reason	State
SCM Checklist for CIS on RHEL 7	Create Separate Partition for /tmp - RedHat 7	ep01a05-rhel7	19 days ago	Never	Linux exception	Excepted (NC)
SCM Checklist for CIS on RHEL 7	Add nodev Option to /home - RedHat 7	ep01a05-rhel7	19 days ago	Never	Linux exception	Excepted (NC)
SCM Checklist for CIS on RHEL 7	Add nodev Option to /dev/shm Partition - RedHat 7	ep01a05-rhel7	19 days ago	Never	Linux exception	Excepted (NC)
SCM Checklist for CIS on RHEL 7	Add nosuid Option to /dev/shm Partition - RedHat 7	ep01a05-rhel7	19 days ago	Never	Linux exception	Excepted (NC)
SCM Checklist for CIS on RHEL 7	Add noexec Option to /dev/shm Partition - RedHat 7	ep01a05-rhel7	19 days ago	Never	Linux exception	Excepted (NC)
SCM Checklist for CIS on RHEL 7	Set Sticky Bit on All World-Writable Directories - RedHat 7	ep01a05-rhel7	19 days ago	Never	Linux exception	Excepted (C)
SCM Checklist for CIS on RHEL 7	Set nodev option for /tmp Partition - RedHat 7	ep01a05-rhel7	19 days ago	Never	Linux exception	Excepted (NC)
SCM Checklist for CIS on RHEL 7	Set nosuid option for /tmp Partition - RedHat 7	ep01a05-rhel7	19 days ago	Never	Linux exception	Excepted (NC)
SCM Checklist for CIS on RHEL 7	Set noexec option for /tmp Partition - RedHat 7	ep01a05-rhel7	19 days ago	Never	Linux exception	Excepted (NC)
SCM Checklist for CIS on RHEL 7	Create Separate Partition for /var - RedHat 7	ep01a05-rhel7	19 days ago	Never	Linux exception	Excepted (NC)
SCM Checklist for CIS on RHEL 7	Bind Mount the /var/tmp directory to /tmp - RedHat 7	ep01a05-rhel7	19 days ago	Never	Linux exception	Excepted (NC)

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



You can set parameters for how your data is displayed in reports in *Configure View*.



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.

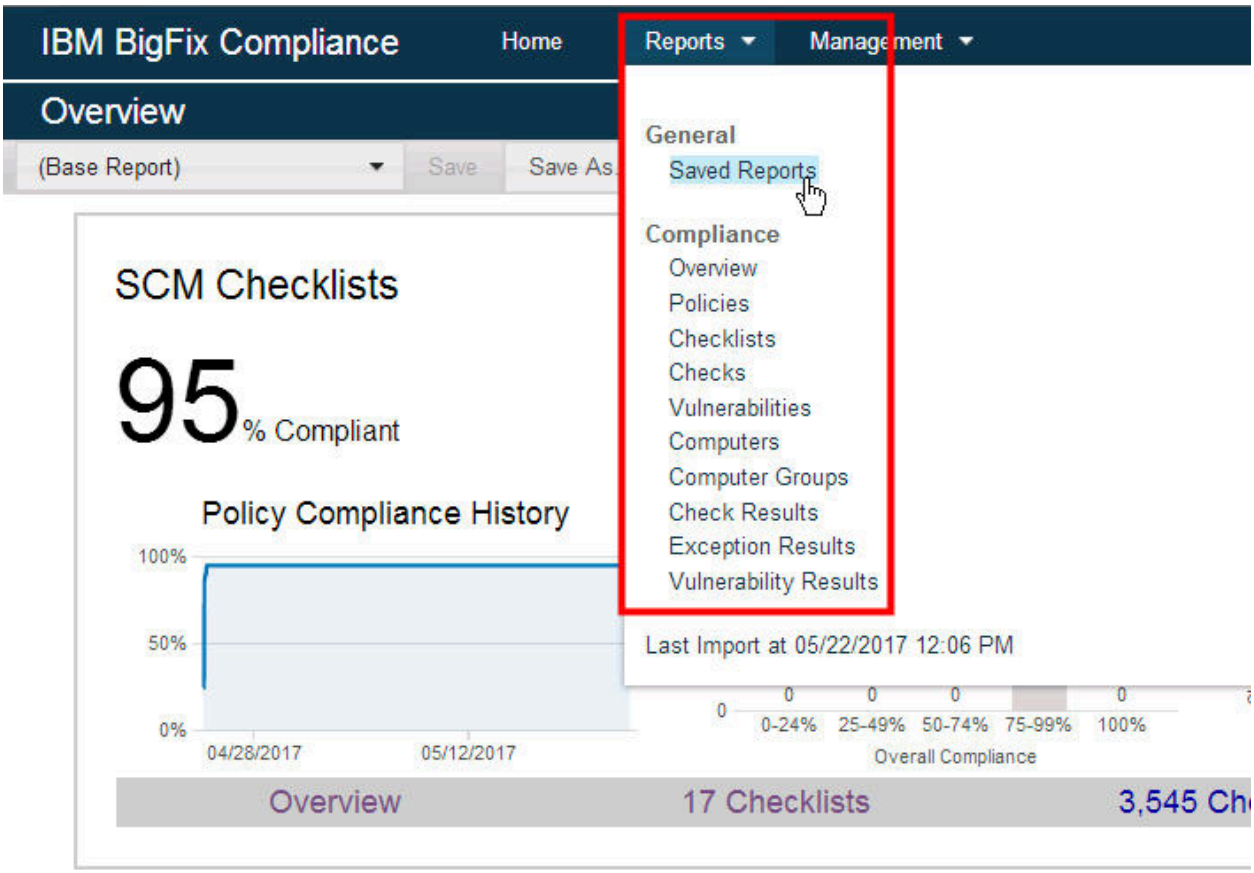


Chart Types

BigFix Compliance Analytics 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)

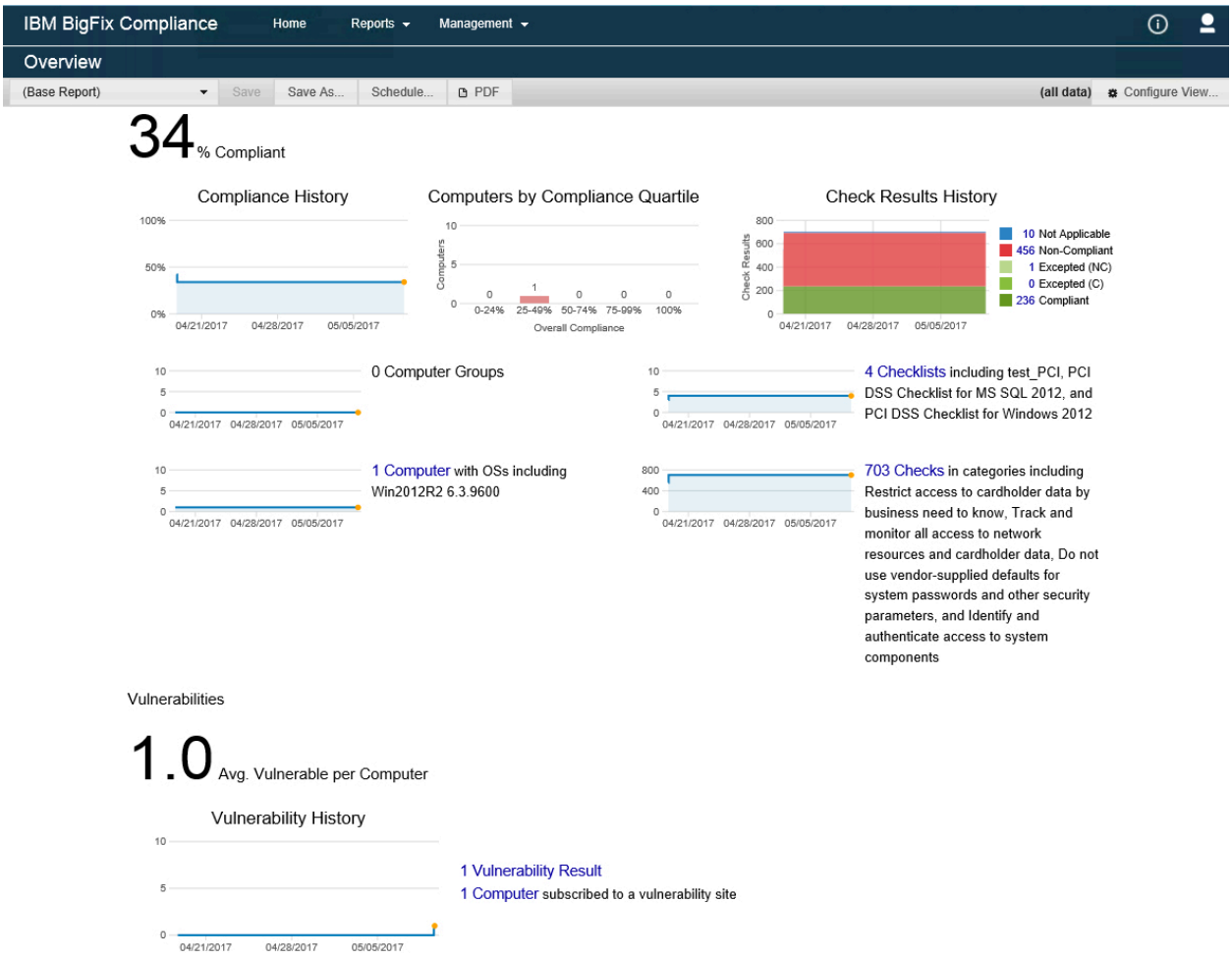
A check that is compliant on a given computer, but that has been excepted through a manually-created exception.

Compliant

A check that complies with the checklist desired values.

Vulnerability History Detail Chart

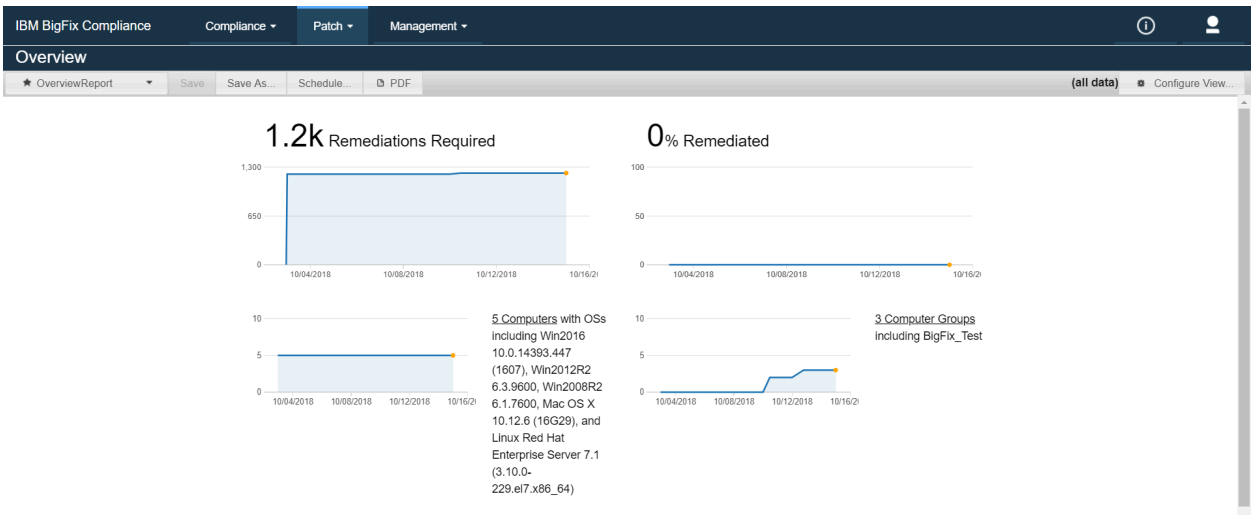
Win loss chart that displays vulnerability history over time.


IBM BigFix Compliance
Home
Reports
Management
Overview
(Base Report)
Save
Save As...
Schedule...
PDF
(all data)
Configure View...
34 % Compliant
Compliance History
100%
50%
0%
04/21/2017
04/28/2017
05/05/2017
Computers by Compliance Quartile
Computers
0-24%
25-49%
50-74%
75-99%
100%
Overall Compliance
Check Results History
Check Results
10 Not Applicable
456 Non-Compliant
1 Excepted (NC)
0 Excepted (C)
236 Compliant
0 Computer Groups
4 Checklists including test_PCI, PCI DSS Checklist for MS SQL 2012, and PCI DSS Checklist for Windows 2012
1 Computer with OSs including Win2012R2 6.3.9600
703 Checks in categories including Restrict access to cardholder data by business need to know, Track and monitor all access to network resources and cardholder data, Do not use vendor-supplied defaults for system passwords and other security parameters, and Identify and authenticate access to system components
Vulnerabilities
1.0 Avg. Vulnerable per Computer
Vulnerability History
1 Vulnerability Result
1 Computer subscribed to a vulnerability site

Chapter 3. Working with patch reports

BigFix Patch Reporting is a component of BigFix Compliance. The application generates a different category of reports. The generated reports can be filtered, sorted, grouped, customized, or exported by using the application tools.

Prerequisites: You have to enable patch reporting to import the patch data. To enable the patch reports, see Enabling patch reporting *(on page 27)*.



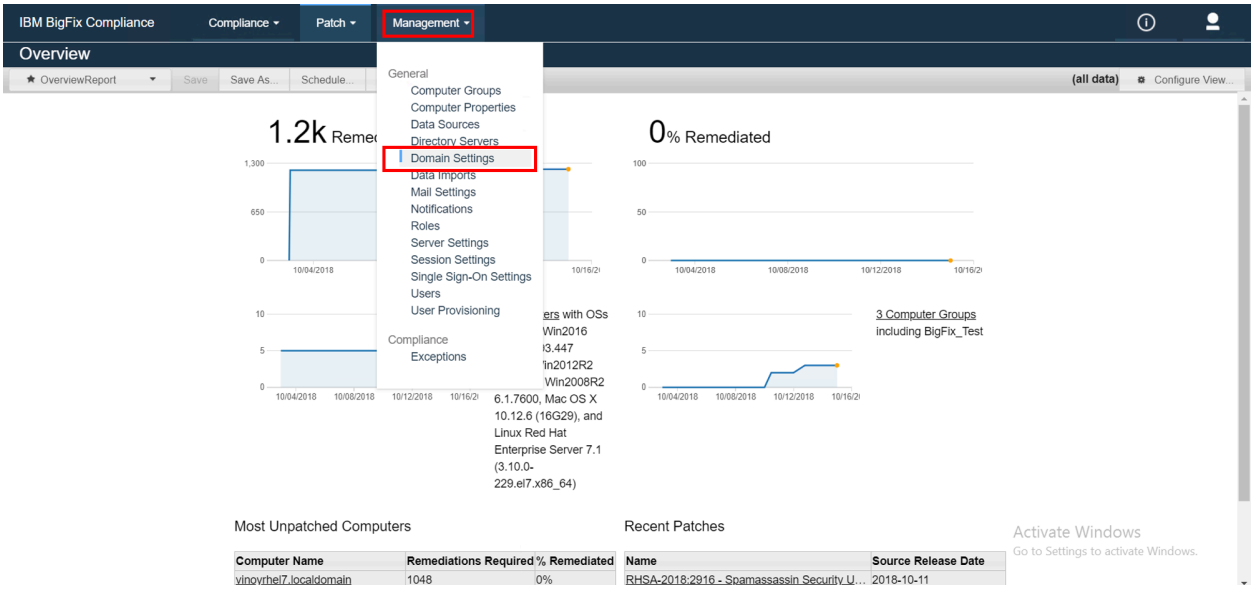
Enabling patch reporting

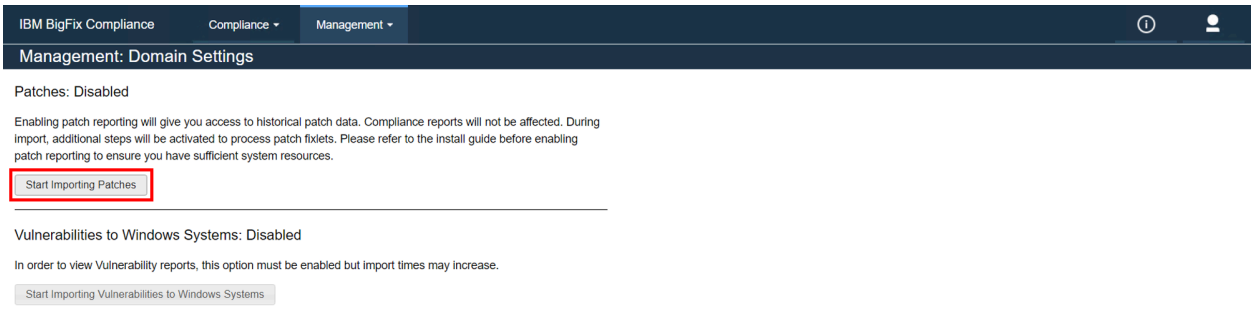
You can enable or disable patch reporting.

If the patch reporting is disabled, the application stops importing the patch data, but previously imported data is retained. If you enable the patch reporting again, legacy data can be accessed from the reporting menu.

To enable the Patch Reporting:

1. On the header bar, click **Management**.
2. Select **Domain Settings** from the menu.
3. Under Patches, click **Start Importing Patches**.
4. In the window that opens, click **Yes, include** to enable the patch reporting.





Note: Enabling the patch reporting increases the duration of import processes and requires additional resources from the BigFix Compliance database. For information about importing data to the patch reporting application, see Data Imports *(on page 57)*.

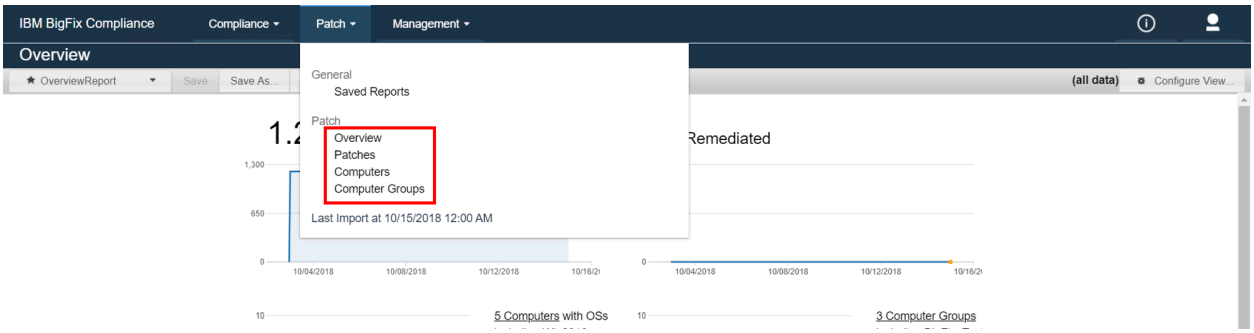
Report types

Four main report types are available. Each type displays a different, configurable view of the current and historical status of a patch deployment. You can grant permissions to the

user roles to access the patch reports, but the data that each user can see depends on the computer to which they have been granted visibility.

You can generate the following category of the reports using the BigFix Patch Reporting application:

- Overview Report
- Patches Report
- Computers Report
- Computer Groups Report



For a graphical representation of each report type, see Example reports - Patch reports *(on page 116)* in the Appendix.

Overview reports

These reports are available from the primary Overview window of the BigFix Patch Reporting dashboard.

Deployment Overview

Displays the current percentage of remediations, the historical aggregate of remediations that are still required, and the applied remediations.

Computer Overview

Displays the current number of computers, the historical aggregate of the computers that are included in the report, and a summary of their operating system platforms.

Computer Groups Overview

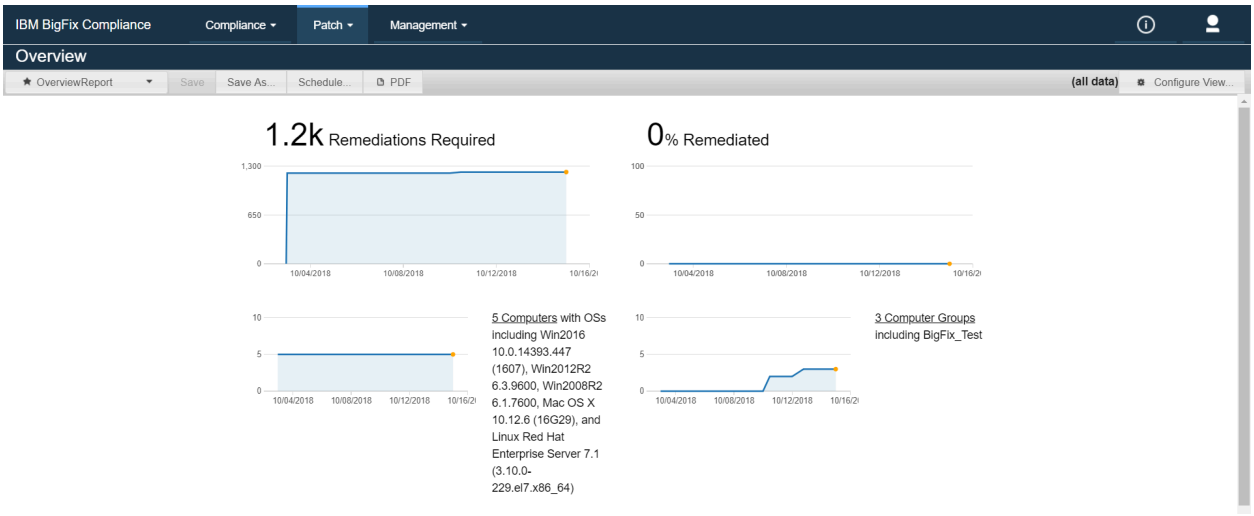
Displays the current number of computer groups, the historical aggregate of computer groups that are included in the report, and a summary of the computer groups.

Most Unpatched Computers Overview

Displays the list of computers that require the most number of patches.

Recent Patch Overview

Displays a list of the most recently available patches



Note: The Overview page does not display information if there is no data about patches.

Patches report

The Patches report displays a list of patches and related details in a grid format.

The report primarily contains this information:

- The severity level of the patch
- The category of the patch
- The source of the patch
- The source release date of the patch
- A historical aggregate of computers that do not have the patch applied yet
- The percentage of remediated computers
- A historical aggregate of remediated Computers

You can further navigate to the sub reports by clicking patch link.
The individual patch contains three sub reports:

Overview

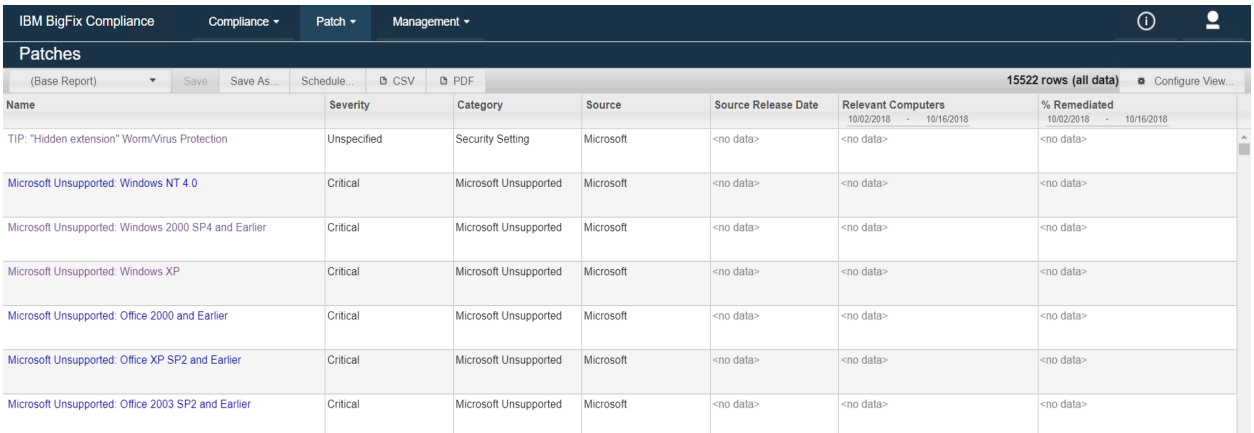
Displays the current number of and historical aggregate of computers that do not have the patch applied yet, the percentage of and a historical aggregate of the remediated computers, and the patch properties.

Subscribed Computers

Displays the list of computers that are subscribed to the selected patch.

Computer Groups

Displays the list of computer groups that are subscribed to the selected patch.



Important: By default, the columns will be sorted in the descending order. You can sort the columns manually by clicking the Relevant Computers and percentage Remediated column titles.

Computers report

This report provides information about all computers, patches, and remediations.

The Computers report displays a list of all the computers and each computer's total number of applicable patches, the average number of the days for the patches to be applied, the number of remediations that are still required, and the remediation percentage and historical aggregate of remediations. You can access the sub reports of the Computers report by clicking a required computer on the list.

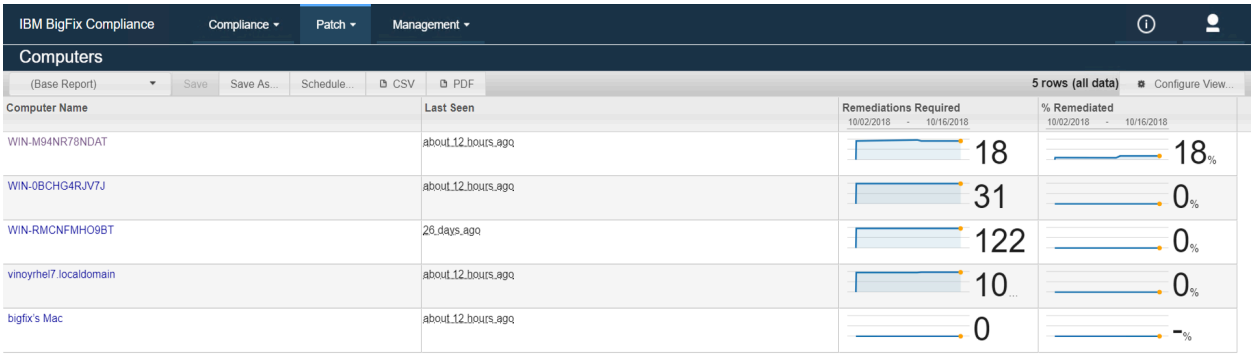
The individual computer contains two sub reports:

Computer Overview

Displays the computer properties, patch data, and the historical aggregate of remediations required and the percentage remediated computers.

Subscribed Patches

Displays the list of patches that are associated with individual computers.



Important: By default, the columns will be sorted in the descending order. You can sort the columns manually by clicking the Relevant Computers and percentage Remediated column titles.

Computer Groups report

This report lists all the computer groups and patch information.

The Computer Groups report displays a list of all computer groups and each computer group's total number of applicable patches, the average number of the days for the patches to be applied, the number of remediations that are still required, and the remediation percentage and the historical aggregate of remediations. You can access the sub reports by clicking the required computer group in the list.

Each computer groups contains three sub reports:

Computer Group Overview

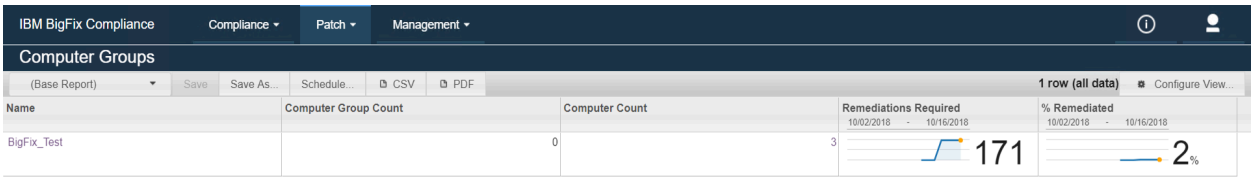
Displays computer group properties, patch data, and the historical aggregate of remediations required and the percentage of the computers that were remediated.

Computers

Displays the list of computers that are associated with the selected computer group.

Patches

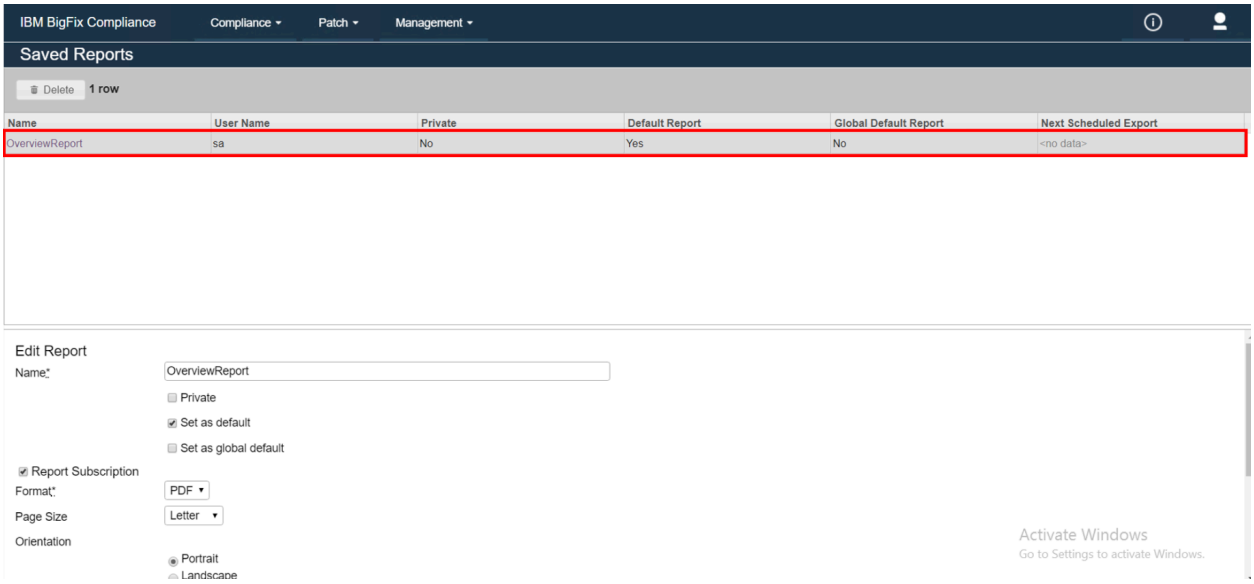
Displays the list of patches that are associated with the computer group.



Important: By default, the columns will be sorted in the descending order. You can sort the columns manually by clicking the Relevant Computers and percentage Remediated column titles.

Saved reports

The saved reports feature retains a specific report format (including the displayed columns and filters that you used to customize the view) for future use, so that you don't have to configure the same settings each time. When you save a report, it becomes available in the **Saved Reports** list. To view the saved reports, open the **Patch** from the menu bar.



Managing reports

You can generate and manage the patch reports by using the following actions in the application.

Save As

You can save a copy of a report under a different name.

Procedure

1. While a report is open, click **Save As**.
2. Enter a name that is different from the current report name..
3. Select **Private** or **Set as default**, **Set as global default** as required.
4. Click **Create**.

The saved report is listed in My Reports section.

Schedule

You can schedule an export process to push a report to the email IDs in the pre-defined timeline.

Procedure

1. Select the required format (PDF or CSV) from the format menu.
2. Select the page size from the menu.
3. Set the orientation to either portrait or landscape.
4. Enter the email ID. Insert commas between multiple email IDs.
5. Enter the start date and start time.
6. Select the export frequency from the menu.
7. Select the language from the menu.
8. Click **Save**.

You must setup the mail settings to schedule an export to the desired email IDs. To setup the mail settings, see Enabling mail settings *(on page 36)*.

Export

You can export the reports in PDF and CSV formats, but a few reports can be exported only in a PDF format.

Procedure

- Click **CSV** to export a report in a `.csv` format.
- Click **PDF** to export a report in a `.pdf` format.

Configure View

This report view can be configured differently for each report. You can select the required columns, time range, filters and options to configure the report view.

Procedure

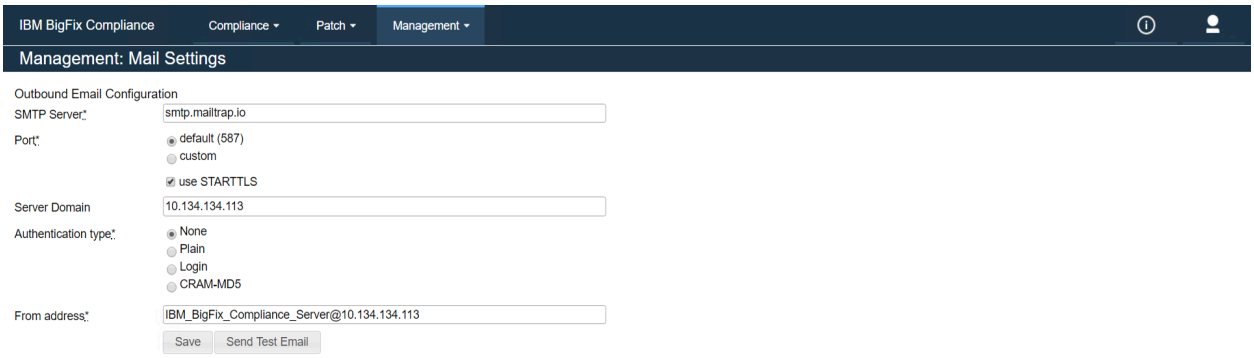
- **Options**: select the **Autosize Columns** check box to auto size the columns in the report.
- **Columns**: select the columns from the list to be featured in the report.
- **Time Range**: enter the time range to pull the data.
- **Filters**: select the filters for pulling specific data.

Enabling mail settings

You must configure outbound email in mail settings to schedule an export to an email recipient. The patch report can be sent to multiple email recipients.

Procedure

1. Click **Management**.
2. Select **Mail Settings** from the menu.
3. In **Outbound Email Configuration**, set the configuration.
4. Enter the details in **SMTP Server** details.
5. Select the port in **Default or Custom**.
6. Select the **use STARTTLS** check box to make the connection secure.
7. In **Server Domain**, enter the server domain.
8. In **Authentication type**, select the authentication type.
9. In **From address**, enter the senders address.
10. Click **Save**.



For information about scheduling an export, see Managing reports *(on page 34)*.

Adding external sites

You can add external sites that are not included in the supported sites list.

You must perform the below actions only when you need to track the patch history of endpoints in patch sites, and not for the list of supported patch sites. Adding patch sites increases the time it takes to complete an ETL import process. You must run the remediation report to add the external sites to supported sites list. After you add the external sites, the site contents are included in the Patch Reporting.

To add external sites:

1. In the BigFix console, subscribe to the sites.
2. Stop the BigFix Compliance service.
3. Create a backup copy of the original file `patch_sites.json` in the directory. The directory is located in `C:\Program Files\BigFix Enterprise\SCA\wlp\usr\servers\server1\apps\tema.war\WEB-INF\domains\pr\config\`.

> **Note:** Save the backup copy in a different directory other than the current directory it resides.

4. Copy the same `patch_sites.json` file into this directory `C:\Program Files\BigFix Enterprise\SCA\wlp\usr\servers\server1\apps\tema.war\WEB-INF\data\config\` and rename it to `custom_patch_sites.json`.
5. Start the BigFix Compliance service.
6. Run the Remediation report from **Management menu > Server Settings**.

BFC Patch Sites

Starting from 2.0.1, the file name has changed in the SCM Reporting site to `patch_sites.2.json`. The code will look for a `custom_patch_sites.json` file, then look for the proper version of `patch_sites.json` in the SCM reporting site for the version of SCA, and then the local `patch_sites.json` file in the application code base.

The Patch Reporting application supports the following sites:

Table 4. Supported Sites

Site name	URL	Notes
Patches for Windows English	http://sync.bigfix.com/cgi-bin/bfgather/bessecurity	No
Patches for Windows (Brazilian Portuguese)	http://sync.bigfix.com/cgi-bin/bfgather/windows-patchesbrazilianportuguese	No
Patches for Windows (Czech)	http://sync.bigfix.com/cgi-bin/bfgather/windows-patchesczech	No
Patches for Windows (NLD)	http://sync.bigfix.com/cgi-bin/bfgather/windows-patchesnld	No

Table 4. Supported Sites (continued)

Site name	URL	Notes
Patches for Windows (Finnish)	http://sync.bigfix.com/cgi-bin/bfgather/windows-patchesfinnish	No
Patches for Windows (French)	http://sync.bigfix.com/cgi-bin/bfgather/windows-patchesfrench	No
Patches for Windows (German)	http://sync.bigfix.com/cgi-bin/bfgather/windows-patchesgerman	No
Patches for Windows (Hungarian)	http://sync.bigfix.com/cgi-bin/bfgather/windows-patcheshungarian	No
Patches for Windows (Italian)	http://sync.bigfix.com/cgi-bin/bfgather/windows-patchesitalian	No
Patches for Windows (Japanese)	http://sync.bigfix.com/cgi-bin/bfgather/windows-patchesjapanese	No
Patches for Windows (Korean)	http://sync.bigfix.com/cgi-bin/bfgather/windows-patcheskorean	No
Patches for Windows (Norwegian)	http://sync.bigfix.com/cgi-bin/bfgather/windows-patchesnorwegian	No

Table 4. Supported Sites (continued)

Site name	URL	Notes
Patches for Windows (Polish)	http://sync.bigfix.com/cgi-bin/bfgather/windows-patchespolish	No
Patches for Windows (Simplified Chinese)	http://sync.bigfix.com/cgi-bin/bfgather/windows-patcheschineses	No
Patches for Windows (Spanish)	http://sync.bigfix.com/cgi-bin/bfgather/windows-patchesspanish	No
Patches for Windows (Swedish)	http://sync.bigfix.com/cgi-bin/bfgather/windows-patchesswedish	No
Patches for Windows (Turkish)	http://sync.bigfix.com/cgi-bin/bfgather/windows-patchesturkish	No
Patches for Windows (CHT)	http://sync.bigfix.com/cgi-bin/bfgather/windows-patchescht	No
Patches for Windows (Russian)	http://sync.bigfix.com/cgi-bin/bfgather/windows-patchesrussian	No
Patches for Windows (Danish)	http://sync.bigfix.com/cgi-bin/bfgather/windows-patchesdanish	No

Table 4. Supported Sites (continued)

Site name	URL	Notes
Patches for Windows (Hebrew)	http://sync.bigfix.com/cgi-bin/bfgather/windows-patcheshebrew	No
Patches for Windows (Greek)	http://sync.bigfix.com/cgi-bin/bfgather/patchesfor-windowsgreek	No
Updates for Windows Applications	http://sync.bigfix.com/cgi-bin/bfgather/updateswindowsapps	No
Windows Point of Sale	http://sync.bigfix.com/cgi-bin/bfgather/windows-pointofsale	No
Patches for RHEL 5 Extended Support	http://sync.bigfix.com/cgi-bin/bfgather/patchesfor-rhel5ESU	Added to all SCA Versions
Patches for RHEL 6 Extended Support	http://sync.bigfix.com/cgi-bin/bfgather/patchesfor-rhel6ESU	Added to all SCA Versions
Patches for RHEL 7 Extended Support	http://sync.bigfix.com/cgi-bin/bfgather/patchesfor-rhel7ESU	Added to all SCA Versions
Patches for RHEL 8 Extended Support	http://sync.bigfix.com/cgi-bin/bfgather/patchesfor-rhel8ESU	Added to all SCA Versions

Table 4. Supported Sites (continued)

Site name	URL	Notes
Patches for RHEL 7	http://sync.bigfix.com/cgi-bin/bfgather/patchesfor-rhel7	No
Patches for RHEL RHSM 7 on System z	http://sync.bigfix.com/cgi-bin/bfgather/patchesfor-rhelrhsm7z	No
Patches for RHEL RHSM 6 on System z	http://sync.bigfix.com/cgi-bin/bfgather/patchesfor-rhelrhsm6z	No
Patches for RHEL 7 PPC64LE	http://sync.bigfix.com/cgi-bin/bfgather/patchesfor-rhelppc64le7	No
Patches for RHEL PPC64BE 7	http://sync.bigfix.com/cgi-bin/bfgather/patchesfor-rhelppc64be7	No
Patches for RHEL 6 Native Tools	http://sync.bigfix.com/cgi-bin/bfgather/patchesfor-rhelppc64be7	No
Patches for RHEL 8 (BFC 2.0)	http://sync.bigfix.com/cgi-bin/bfgather/patchesfor-rhel8	No
Patches for CentOS6 Plug-in R2 (BFC 2.0.1)	http://sync.bigfix.com/cgi-bin/bfgather/patchesfor-centos6pluginr2	Added to all SCA versions

Table 4. Supported Sites (continued)

Site name	URL	Notes
Patches for CentOS7 Plug-in R2 (2.0.1)	http://sync.bigfix.com/cgi-bin/bfgather/patchesfor-centos7pluginr2	Added to all SCA versions
Patches for Mac OS X (2.0.1)	http://sync.bigfix.com/cgi-bin/bfgather/macpatches	Uses non-standard x-fixlet-superseded_id so only supported 2.0.1 and later.
Updates for Mac Applications (2.0.1)	http://sync.bigfix.com/cgi-bin/bfgather/updates-macapps	Uses non-standard x-fixlet-superseded_id so only supported 2.0.1 and later.
Windows 7 ESU (2.01)	http://sync.bigfix.com/cgi-bin/bfgather/win7esu	Added to all SCA versions.
Windows 2008 ESU (2.0.1)	http://sync.bigfix.com/cgi-bin/bfgather/win2008ESU	Added to all SCA versions.

System requirements

Configure your BigFix Patch Reporting deployment environment according to the following requirements.

Table 5. Supported components and system requirements to deploy BigFix Patch Reporting

Disk space requirements with and without the SCA patch domain enabled.

Components	Requirements
Disk space requirements for data base tables (patch domain)	• SCA without patch domain enabled: 100,000 endpoints, 100 subscribed checklists, and 12 computer groups • SCA with patch domain enabled: 100,000 endpoints, 100 subscribed check lists, 30 subscribed patch sites, and 12 computer groups
Disk space for the tem_-analytics database	• Data file size: Initial ETL report SQLServer MDF: 54.7 GB, LDF 108.4 GB, TempDB: 8x1.4 GB each • Data file size: Incremental ETL import after patch enabled SQLServer MDF: 57.9 GB, LDF: 108.5 GB, TempDB: 8x1.4 GB each
JVM heap size 2GB	• 2 GB heapsize in `jvm.options` • 2 GB for SCA 1.10

Table 6. Supported components and system requirements to deploy BigFix Patch Reporting

Windows server versions for SCA Compliance and Patch Domains.

Components	Requirements
Minimum - Windows Server 2008 R2	• SP1, 16 GB RAM 32 GB for best results

Table 6. Supported components and system requirements to deploy BigFix Patch Reporting

Windows server versions for SCA Compliance and Patch Domains.

(continued)

Components	Requirements
Maximum: Windows Server 2016 R2	• SP2, 16 GB RAM 32 GB for best results
MSQL Server 2008 R2	• SP3, 16 GB RAM 32 GB for best results
MSQL Server 2016 R2	• SP3, 16 GB RAM 32 GB for best results

Recommendations:

- The Windows SCA Compliance service runs on the Windows server needs sufficient free memory (RAM) to efficiently complete ETL. The default size for the SCA Compliance Service is 2GB.
- For Windows servers with small amounts of RAM ensure a minimum 3 GB free space at all times during each ETL import process and an extra 1GB for the overhead of Java.
- For Windows server with plenty of RAM, and large deployments, the JVM heap size limit can be increased to 4GB to improve ETL import times. To change the JVM heap size limit, change the setting "-Xmx2048m" to "-Xmx4096m" in the `file JVM.options` file in the directory. The file is located in `C:\Program Files\HCL\SCA\wlp\usr\servers\server1\jvm.options`. In order for the changes to take effect, you must restart the Compliance Service.

Sample use cases

Use cases can help you understand the capabilities of the patch reporting application.

Case 1: How can I view the computers that require more remediations?

Summary: You can view the computers that require the most remediations on the Overview report.

Prerequisites: You must enable the Patch report, and patch data must exist so that the report can be displayed.

Procedure

1. On the header bar, click **Patch**.
2. Select **Overview** from the menu.
3. On the Overview report, you can view the computers that required the most remediations in the "Most Unpatched Computers" section..

Exception: If there are no computers that require the most remediations, the **Most Unpatched Computers** section will be empty.

Case 2: How can I view only the critical patches?

Summary: You can view the critical patches in the Patches report.

Prerequisites: You must enable the Patch report, and patch data must exist so that the report can be displayed.

Procedure

1. On the header bar, click **Patch**.
2. Select **Patches** from the menu.
3. In the Patches report, click **Configure** at the top right side of the console to filter only the critical patches.
4. To add the filters, click **Add**.
5. Three filters are displayed, select **Severity** and **Equals** from the menus of first and second filters respectively.
6. Enter `Critical` in the third filter filed.
7. Click **Submit**.

The Patches Report displays only the critical patches.

Exception: If there are no critical patches, the report is blank.

Case 3: How can I learn about required remediations and status of patches that are applied a computer?

Summary: You can view the patch applied status of the computer in the **Computers** report.

Prerequisites: You must enable the Patch report, and patch data must exist so that the report can be displayed.

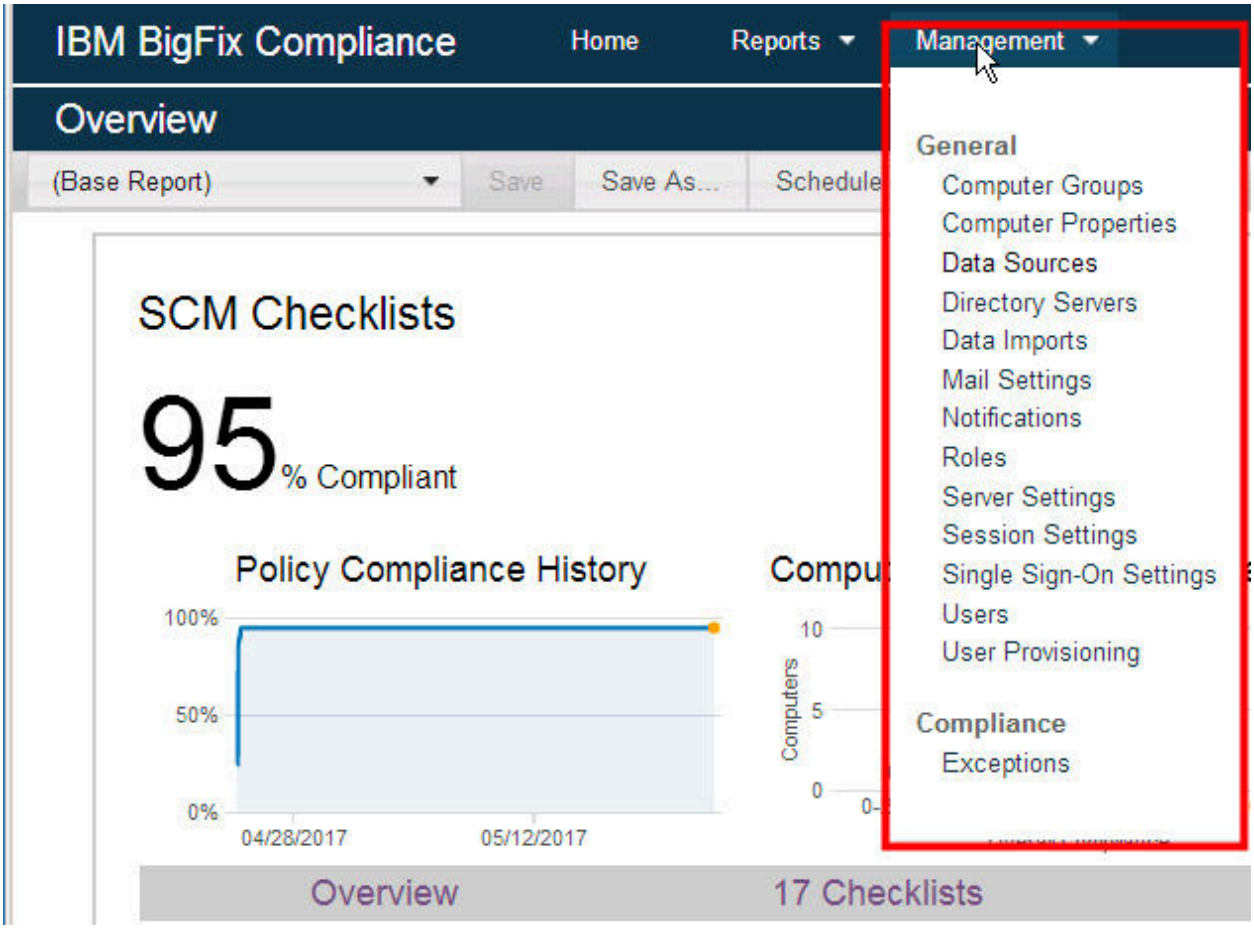
Procedure

1. On the header bar, click **Patch**.
2. Select **Computers** from the drop down.
3. On the **Computers** page, click **Configure** at the top right side of the console.
4. Under **Columns** in the **Patch** section, select the **Remediations Required** and **% Remediated** checkboxes.
5. Click **Submit**.

The Computers report displays the **Remediations Required**, and **% Remediated** columns. You can compare the graphs in these columns to determine the patch applied status.

Chapter 4. Management Tasks

The Management Tasks function within BigFix Compliance Analytics 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, directories, imports, mail settings, roles, server settings, session settings, users, user provisioning, and exceptions.



Click **Management** to select any of the following tasks

- General
  - Computer Groups
  - Computer Properties

    - Datasources
    - Directories
    - Imports
    - Mail Settings
    - Roles
    - Server Settings
    - Session Settings
    - Users
    - User Provisioning
- Security and Compliance
    - Exceptions

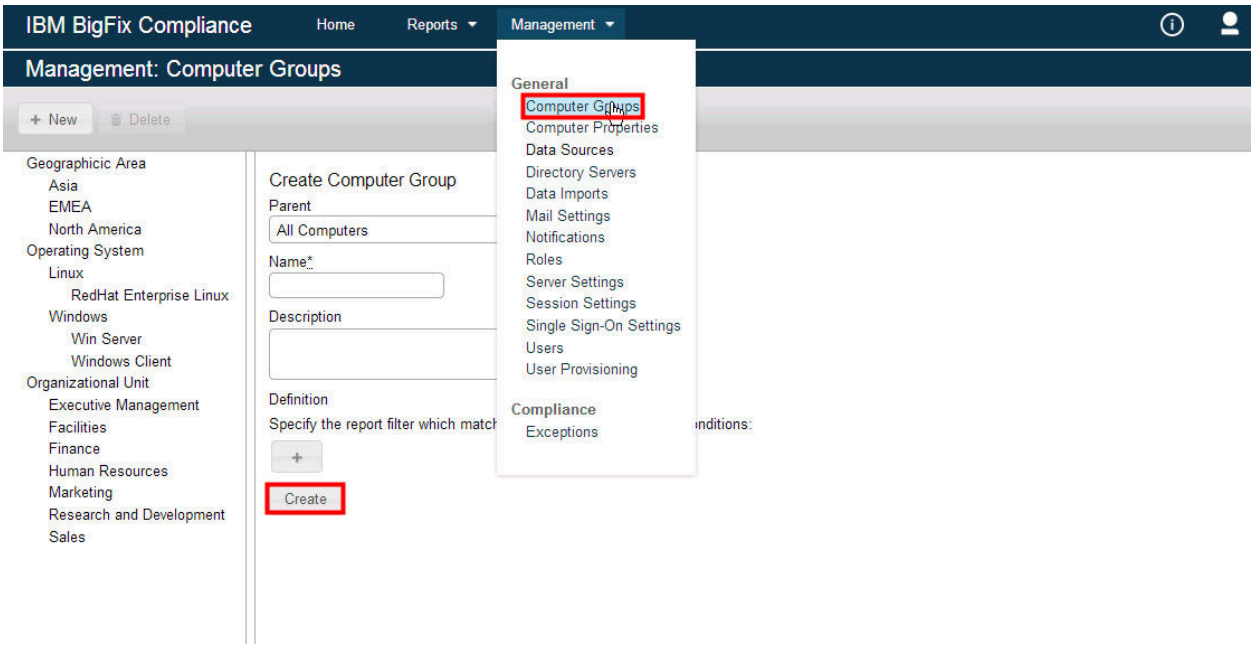
Computer Groups

BigFix Compliance Analytics computer groups help you organize the compliance data that displays in your reports. Specifically, you can filter data to limit what you want to see displayed in your overviews and lists.

All users need to be assigned to a computer group in order to log in to BigFix Compliance Analytics. Logged-in users can see compliance data based on their associated computer group.

To create a computer group, click the **Management** drop-down menu at the top of the console and select **Computer Groups**. Click **New**. Use the dropdown menu to assign your group to a parent. Use the **Definition** field to assign parameters to your group.

When finished, click *Create*.

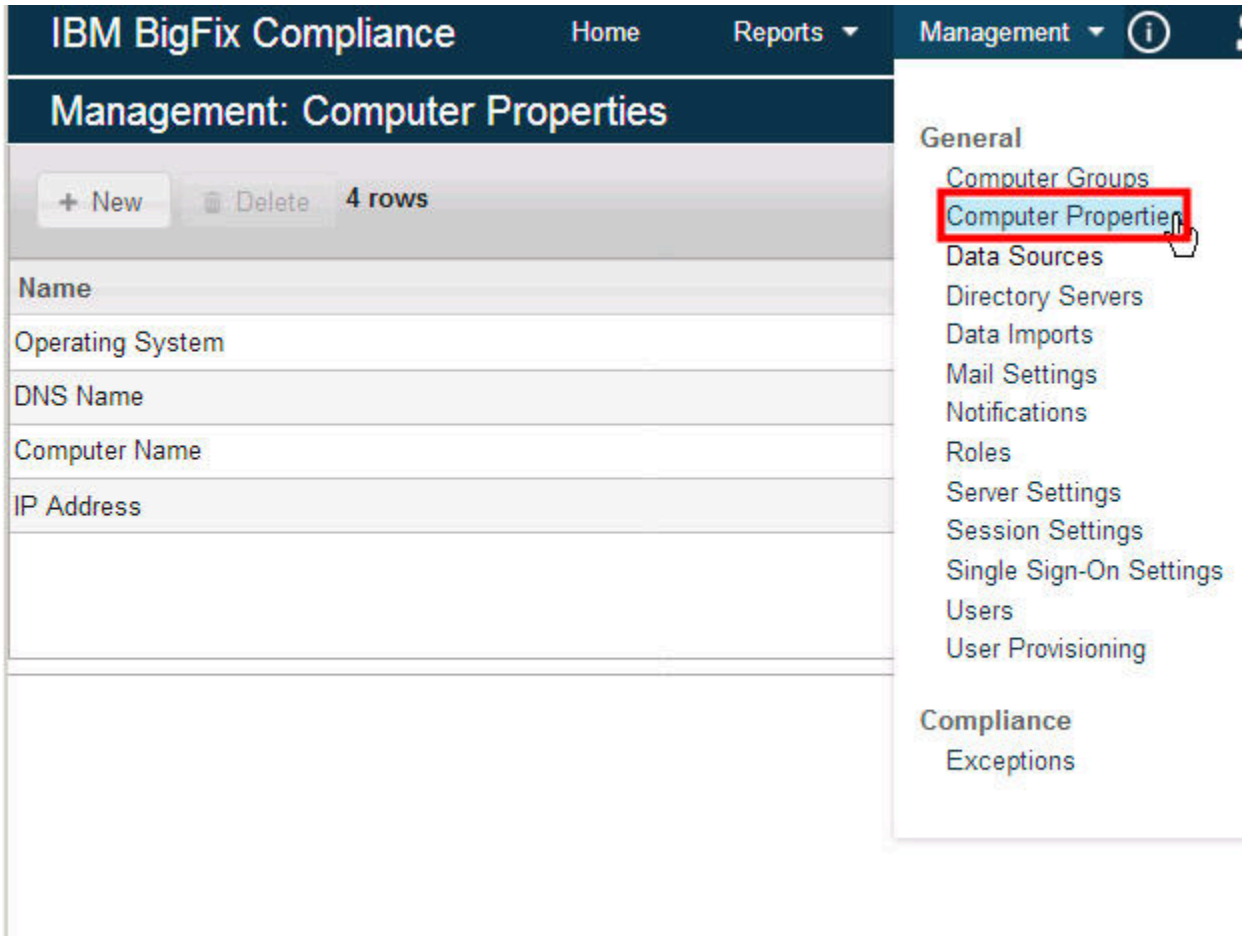


Note: You must perform an import after saving your changes.

You can set the Users account to configure multiple computer groups. To configure multiple groups, see Configuring multiple computer groups *(on page 82)*.

Computer Properties

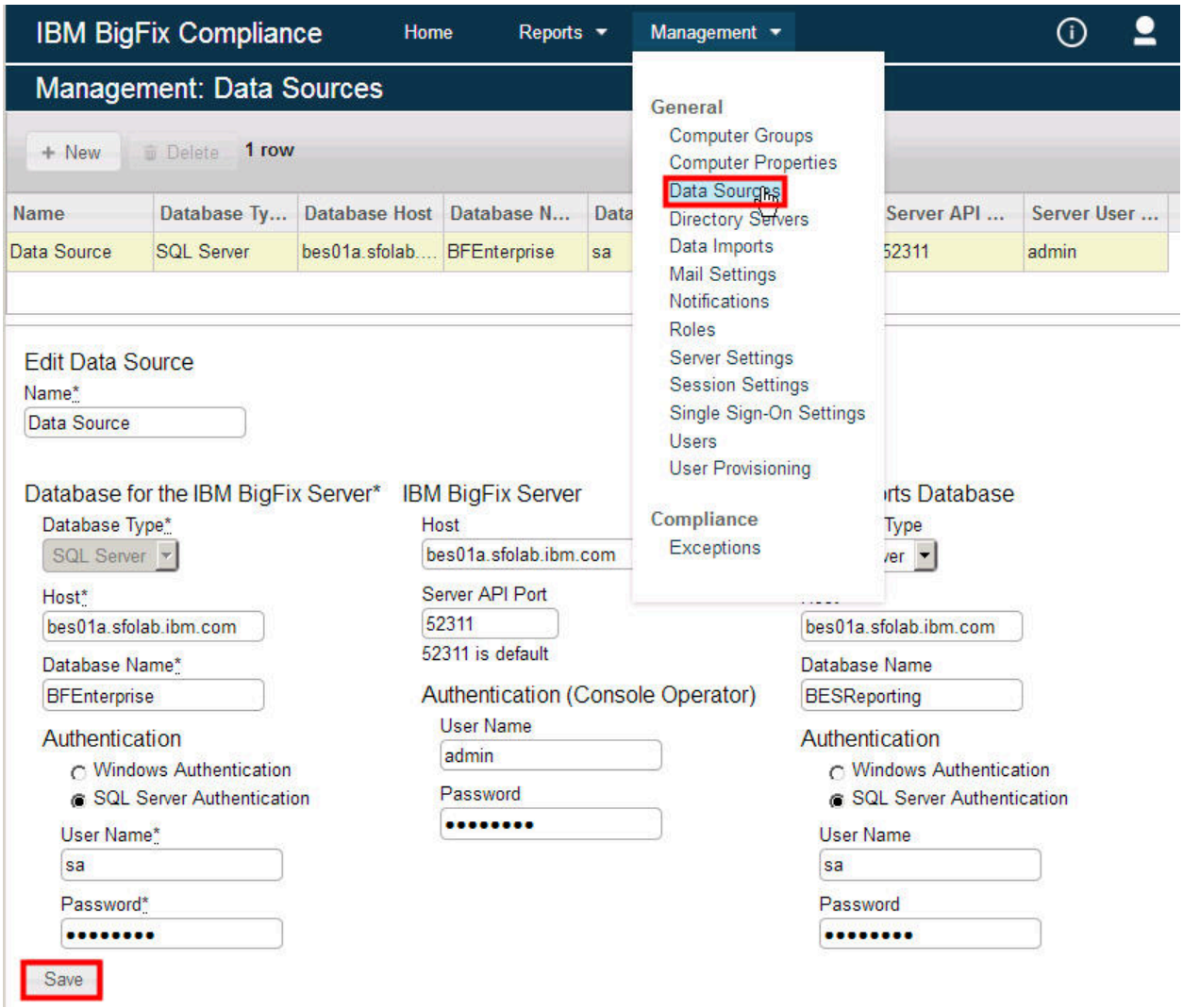
You can create computer properties from the BigFix datasources available for reporting and filtering within the Analytics interface. You can use the default properties in your console, or click *New* to create new properties. These computer properties become the display columns in the computers and results list view for your reports.



Note: You must perform an import after saving your changes.

Data Sources

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



Adding a data source

Add a data source to view information about the database on which your compliance data is based.

When you are adding a data source:

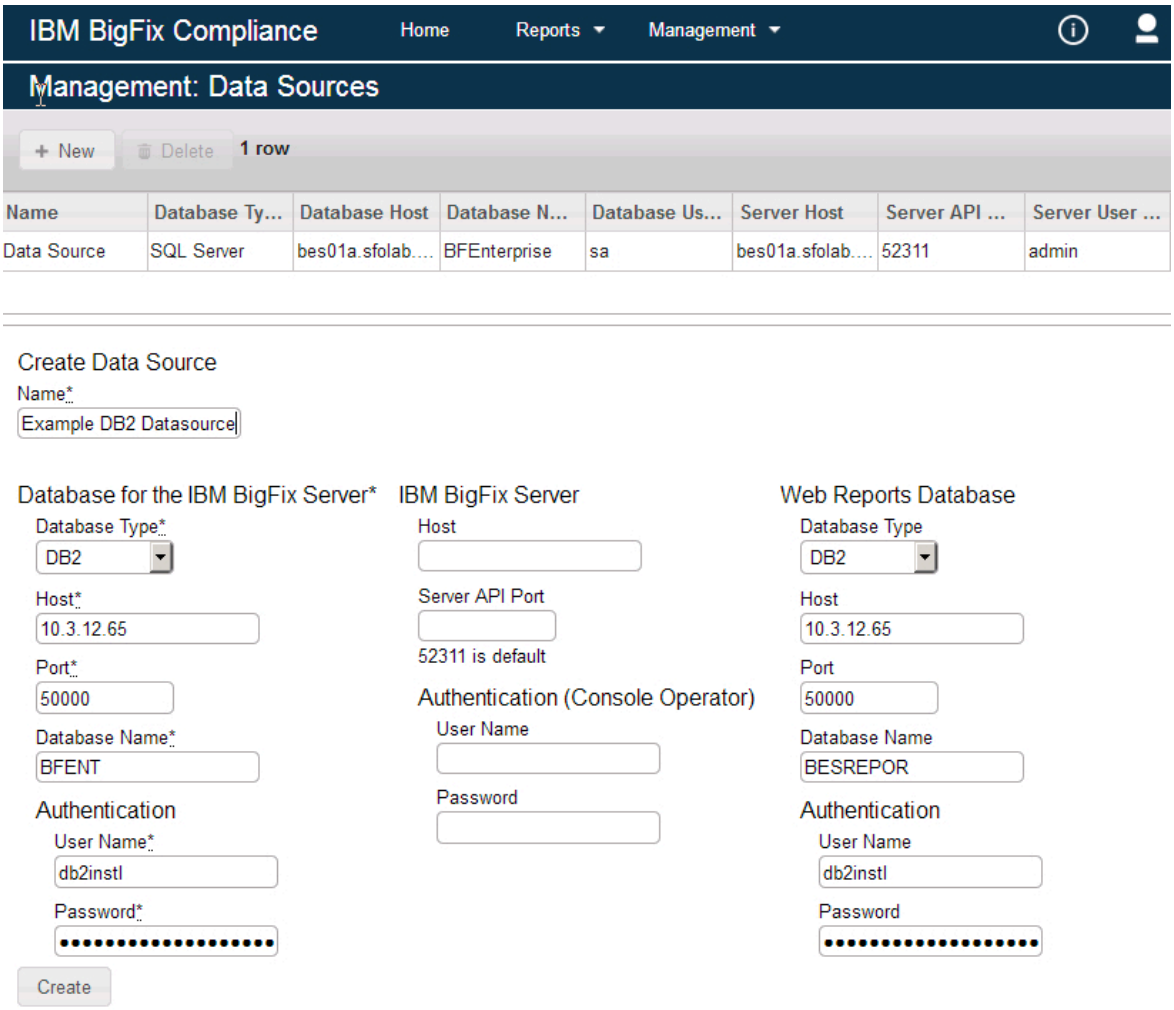
- Do not add a datasource that is a DSA copy of an existing datasource to avoid the display of duplicate data.
- If you restrict user access based on computer groups, you might have to create new computer groups or modify existing ones to ensure correct access restrictions for the new datasource.
- If you added new computer properties, ensure that you provide mappings to those properties in the new datasource.
- In BigFix Compliance Analytics, if you have exceptions that are based on computer groups, ensure that those exceptions and groups are set up correctly for the new datasource.
- In Software Usage Analysis (SUA), if you have contracts that are based on computer groups, ensure that those contracts and groups are set up correctly for the new datasource.
- You must run an import after you add a datasource before computers from that datasource are available in reports.
- When you are running an import, all datasources must be online and reachable or the import fails. This ensures that reports do not show incomplete data or misleading inventory or compliance aggregates.
- Regarding Report data, a user with restricted access by computer group sees only the results or computer report data for their assigned computer group. Examples of results or computer report data are Computers, Computer Groups, Check Results, Exception Results, and Vulnerability Results.

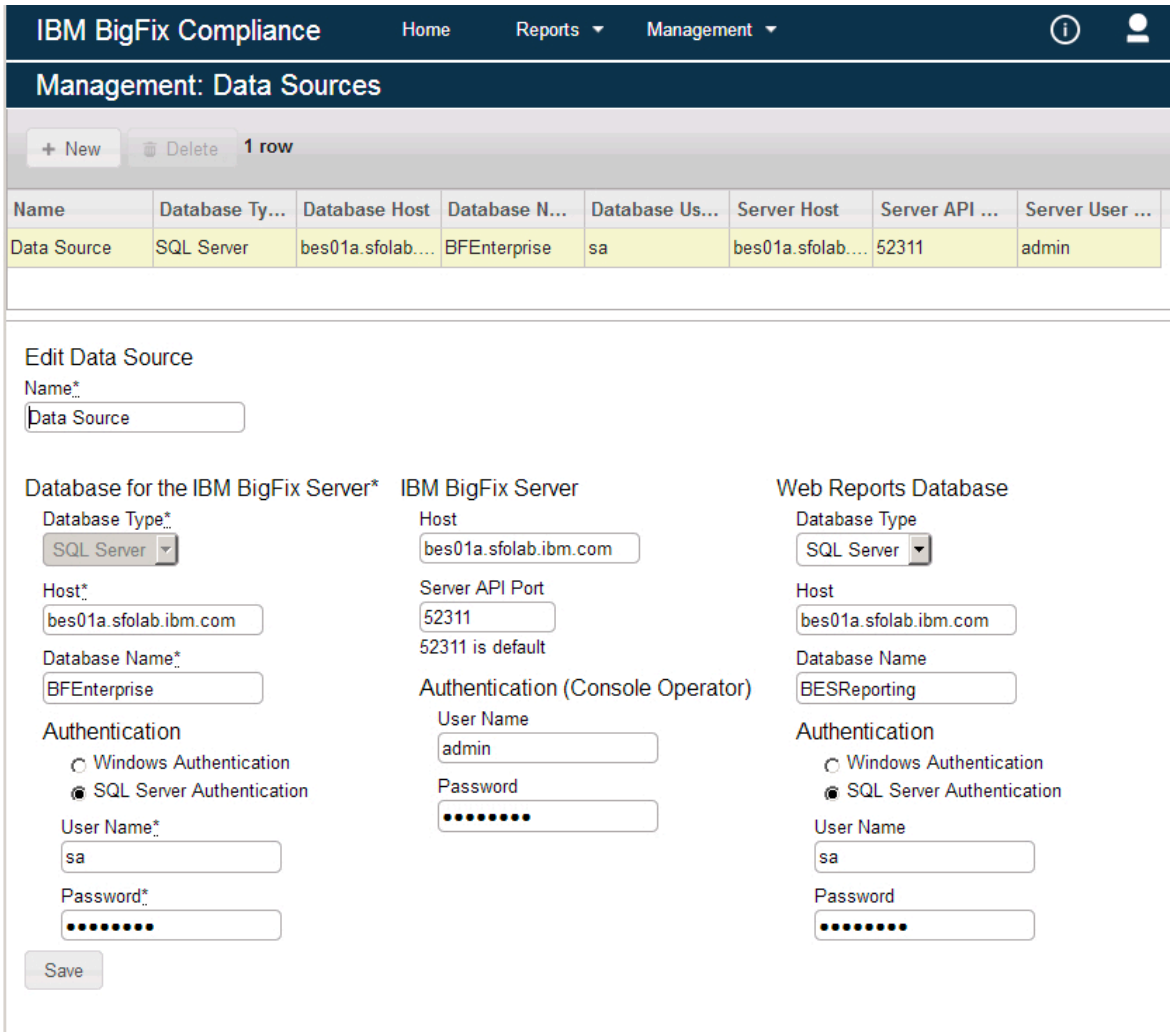
  All users still see all Checklists, Checks, and Vulnerabilities from all datasources, regardless of Computer Group restrictions. Multi-tenancy supports segmentation of computer data based on computer groups and a user's computer group membership. It does not support segmentation of checklists, checks, and venerability checks themselves or of a SUA software catalog.

  You must deploy multiple Compliance servers for the following cases:
  - If you are not able to see the existence of checklists that are created for other customers
  - You have to apply different software catalogs for different customers

1. In the upper right corner, click **Management > Data sources**.
2. In the upper left corner of the horizontal navigation bar, click **New**. A new form opens in the lower pane.
3. Provide the unique name for the new data source.
4. Select the database type from the **Database Type** drop-down list.

Option	Description
Database Type	**Steps**
DB2	a. Specify the host, port, and database name. b. For server authentication, specify a user name and password.
SQL Server	a. Specify the host and database name. b. Select the authentication type. c. For SQL server authentication, specify a user name and password.


IBM BigFix Compliance
Home
Reports
Management
Management: Data Sources
+ New
Delete
1 row
Name
Database Ty...
Database Host
Database N...
Database Us...
Server Host
Server API ...
Server User ...
Data Source
SQL Server
bes01a.sfolab....
BFEnterprise
sa
bes01a.sfolab....
52311
admin
Create Data Source
Name*
Example DB2 Datasource
Database for the IBM BigFix Server*
Database Type*
DB2
Host*
10.3.12.65
Port*
50000
Database Name*
BFENT
Authentication
User Name*
db2instl
Password*
IBM BigFix Server
Host
Server API Port
52311 is default
Authentication (Console Operator)
User Name
Password
Web Reports Database
Database Type
DB2
Host
10.3.12.65
Port
50000
Database Name
BESREPOR
Authentication
User Name
db2instl
Password
Create



5. Provide credentials of the administrative user that you created while installing HCL BigFix (by default, IEMAdmin). The advanced policy functionality is currently used only for PCI content. To enable the advanced policy functionality, you must provide the credentials for a BigFix console operator. It is recommended that this is a master operator, but at the minimum, the console operator must meet the following permissions:
    - Can use REST API
    - Have reader permission for the PCI DSS Reporting site

   If you do not use this feature, you may leave these fields blank.
6. Click **Create**.

Deleting a data source

1. In the upper right corner, click **Management > Datas sources**.
2. In the upper pane, click the data source that you want to delete.
3. In the upper left corner of the navigation bar, click **Delete**.

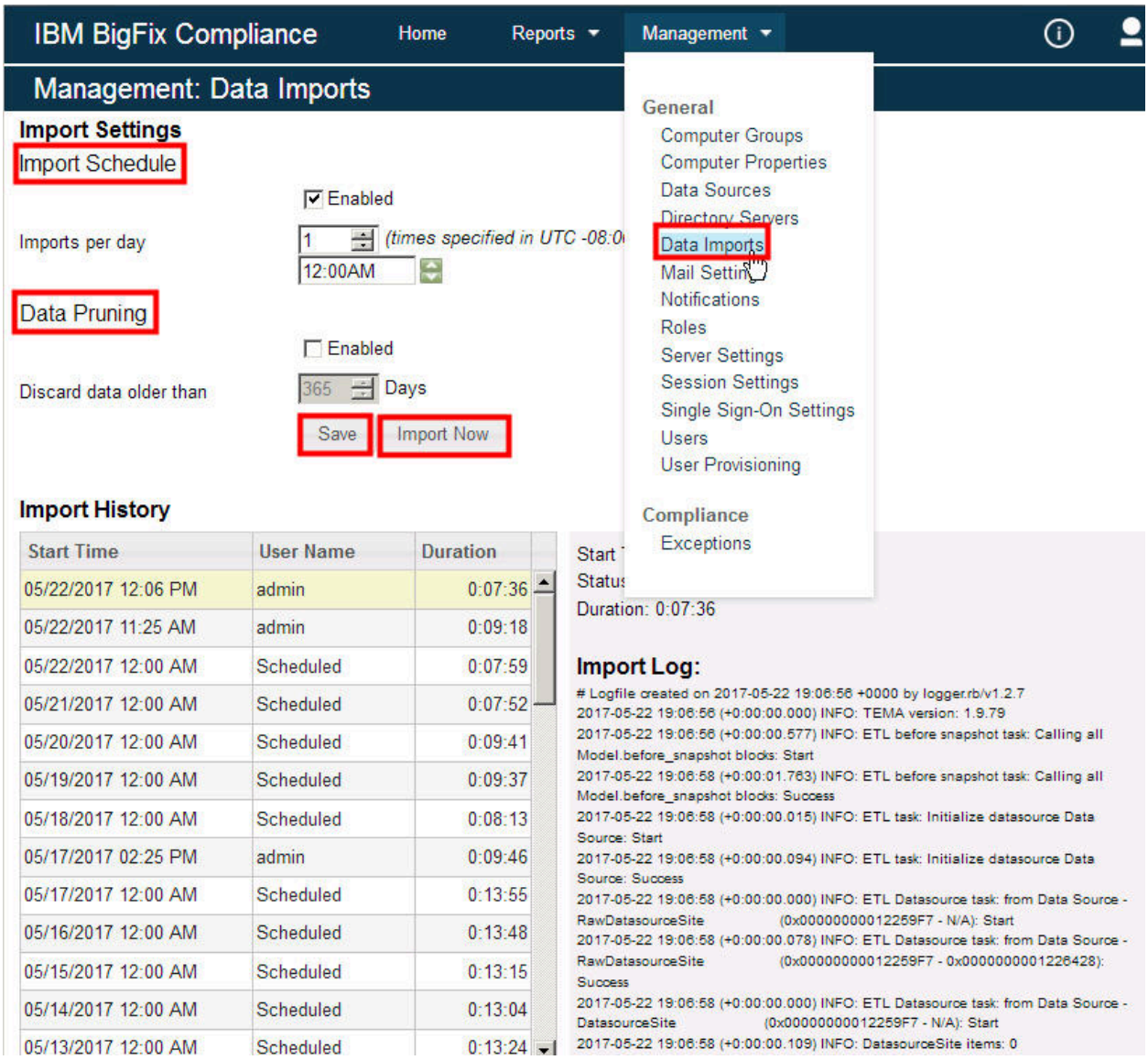
You deleted all the data for computers that belong to this data source.

Data 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.

Run an immediate import by clicking *Import Now*. To schedule a recurring import, first check the import box at the top of the window and set the desired daily start time.

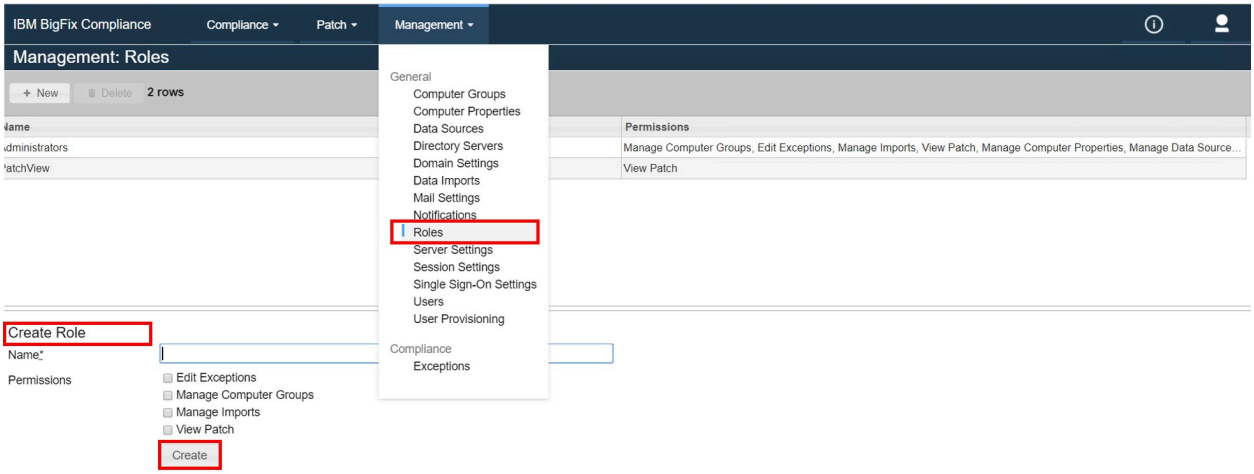
From the Data Imports interface, you can also enable Data Pruning and discard older data. Click Save to confirm the change.



Roles

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

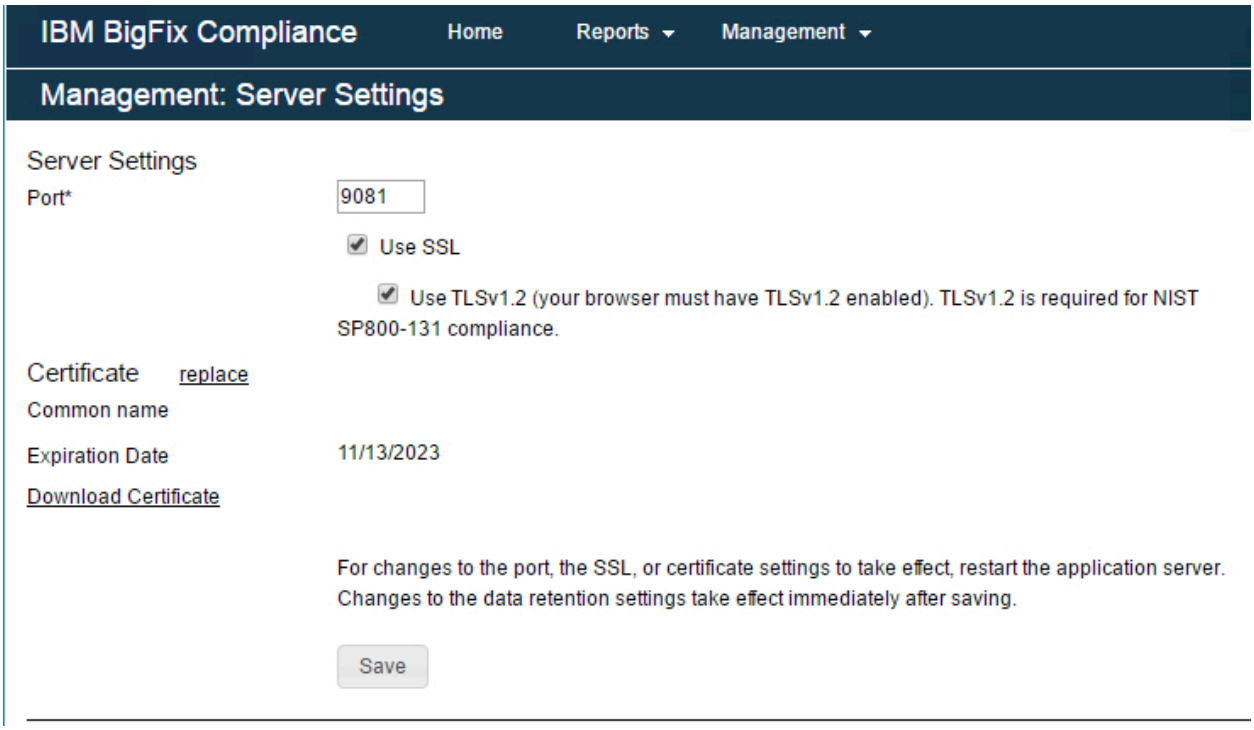
Use the buttons on the top bar to create new roles or delete existing roles.



Important: Administrators can assign permissions to the created role. User will be able to view/edit the reports based on the permissions provided by administrators.

Server Settings

Use the Server Settings interface to configure the HTTP port, SSL, TLS, and enable or disable data retention. Any changes to the port or SSL settings require a service restart.



Enabling TLS 1.2 with SQL Server

Follow the steps to set up TLS 1.2, which is required for NIST SP800-131 compliance.

- The TLS set up requires installing supported versions of MS SQL and the latest patches.
- The minimum required version is MS SQL Server 2012 Service Pack 3.
- Ensure that your browser is TLS 1.2 enabled.
- For BFC V1.10.x and earlier:
  - Open the `jvm.options` file with a text editor and add the following code:

    ```
    -Dcom.ibm.jsse2.overrideDefaultTLS=true
    ```

    File location: `<SCA>\wlp\usr\servers\server1\`

    Note: Ensure that there are no extra/empty space or tab in the code.

  - You must restart the compliance service for the updates to take effect.

- For BFC V2.0.x and later, the code is already added in `jvm.options`.

  File location: `<SCA>\wlp\usr\servers\server1\configDropins\defaults\`

1. Install one of the supported versions of MS SQL server and the latest patches. Minimum requirement is MS SQL Server 2012 Service Pack 3. For more information about the updates that Microsoft is releasing to enable TLS 1.2 support for Microsoft SQL Server setup, see https://support.microsoft.com/en-us/help/3135244/tls-1.2-support-for-microsoft-sql-server
2. Generate your self-signed certificate using Openssl or IIS manager tool (make sure the certificate owner or 'common name' match with your hostname).
    a. OpenSSL > req -x509 -sha256 -nodes -days 365 -newkey rsa:2048 -keyout privateKey.key -out certificate.crt
    b. Make sure you combine your certificate and keys into .pfx
    c. OpenSSL > pkcs12 -export -out sca_server.pfx -inkey privateKey.key -in certificate.crt
    d. Use IIS manager to generate Self-signed certificate and export to .pfx directly. To install the IIS manager, go to Server Manager, click adding features and add Web Server(IIS). For information on generating certificates, see https://aboutssl.org/how-to-create-a-self-signed-certificate-in-iis/
3. Upload the certificate/key into Bigfix Compliance.
4. From the command line, run mmc.exe.
5. Add a certificate snap-in.
    a. Select **File > Add/Remove Snap-in**.
    b. Select the **Certificates** snap-in and click **Add**.
    c. Select **Computer account** and click **Next**.
    d. Ensure that the **Local computer** option is selected and click **Finish**.
    e. Click **OK**.
6. Import the certificate.
    a. In the Console window, go to **Console Root > Certificates**.
    b. Right-click **Certificates** and select **All Tasks > Import**.
    c. From the Welcome Window, click **Next**.
    d. Click **Browse**and select the certificate store that you created.

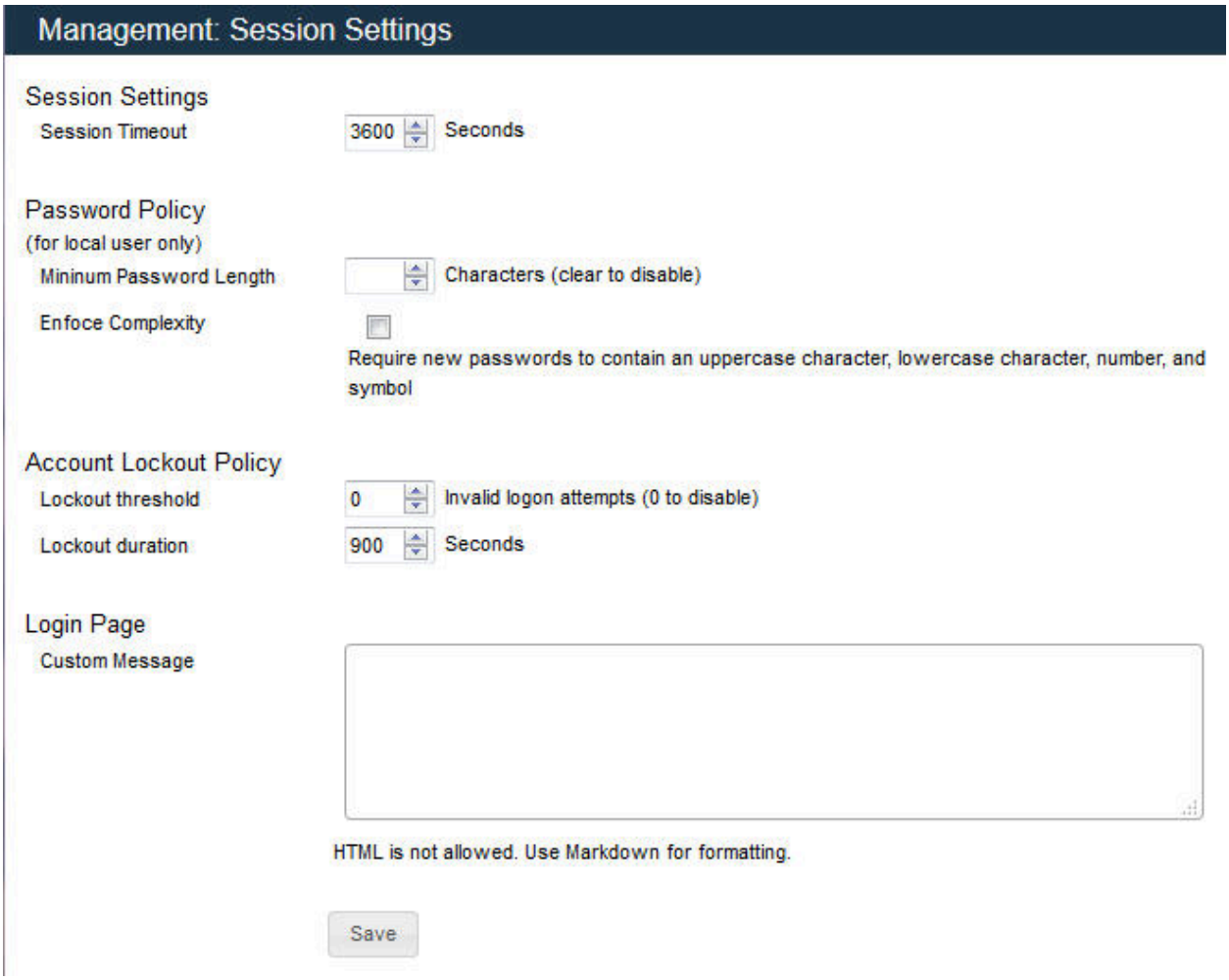
e. Click **Next**.
f. Enter the password for the certificate store and click **Next**.
g. Ensure that **Place all certificates in the following store** is selected and that **Certificate Store** is set to **Personal**.
h. Click **Next** and click **Finish**.

7. Manage the private keys.
   a. Right-click the certificate file and select **All Tasks > Manage Private Keys**.
   b. Click **Add**.
   c. Click **Check Names**, select **MSSQLSERVER** and click **OK** (If **MSSQLSERVER** is not found, choose **SERVICE** instead).
   d. Click **OK** on the **Select Users and Groups** window.
   e. Set permissions for **MSSQLSERVER** on the **Permissions** window and click **OK**. For example, select **Allow for Read** for a Read-only option.
8. Configure the SQL Server to accept the encrypted connections by following the windows sql server documents. For more information, see https://docs.microsoft.com/en-us/previous-versions/sql/sql-server-2012/ms191192(v=sql.110)#EncryptConnection
9. Restart the SQL server and Bigfix Compliance.

Session Settings

You can change your session settings to specify the session time for a logged in user who is inactive for a certain period and to custom the message on the login page using Markdown text.

To make changes in your session setting, go to **Management > Session Settings**.



You can configure the following settings:

Session Settings

Set the session timeout.

Password Policy

This policy is for local users only. You can set the password of length and require users to have more a more complex password.

Account Lockout Policy

Set the number of allowed invalid log on attempts and the duration before the account is locked.

Login Page

You can enter a message. Note that Markdown formatting is supported, but HTML is not allowed.

Make your changes then click **Save**.

Directory Servers

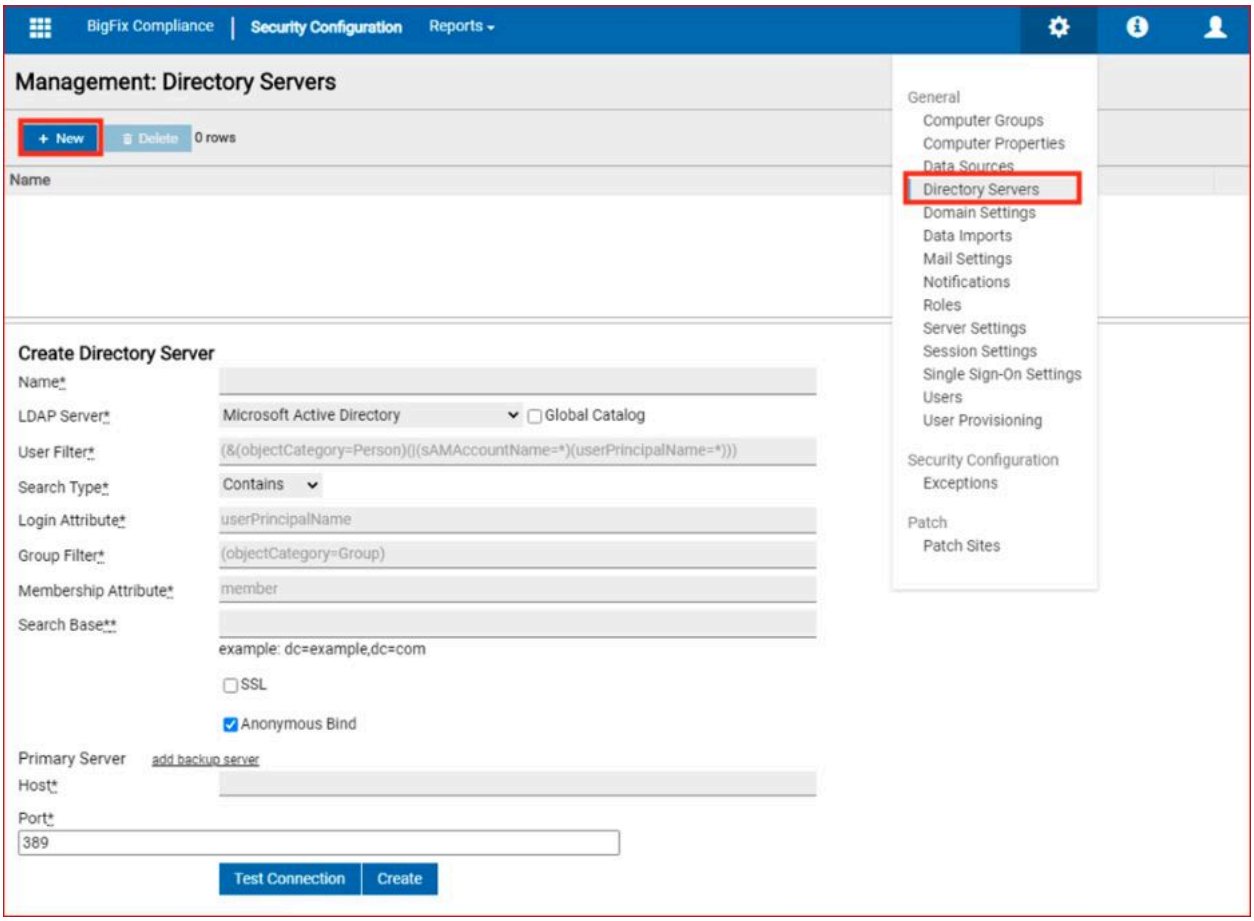
BigFix Compliance Analytics supports authentication with directory servers through Lightweight Directory Access Protocol (LDAP). You can add directory servers to BigFix Compliance Analytics so that the users can log in using credentials based on your existing authentication scheme.

To authenticate BigFix Compliance Analytics users with directory servers, you must do the following:

1. Add a directory server
2. Link a user to the directory server (See Users *(on page 81)* section).

You can also use the User Provisioning feature to automatically create users (with directory server authentication) without doing it individually from the Users menu.

- (Optional) Add a user provisioning rule (See User Provisioning section).



Configuring a directory server that has a load balancer or multiple domain controllers

BigFix Compliance supports authentication through a LDAP server. Learn how to configure the root certificate for the BigFix Compliance server.

Contact the BigFix Support team to obtain the password that is required during configuration.

The LDAP does not work on BigFix Compliance servers when an individual domain controller certificate is updated. Thus, compliance sites stop authenticating the users through LDAP because the updated domain controller is not trusted. Perform the steps in this procedure to configure the directory server. Ensure that you configure a directory

server after each application upgrade, because the certificates that you add according to this procedure are not preserved.

If your LDAP server uses a load balancer or multiple domain controllers that dynamically change the list of hosts, and the connection between LDAP and the BigFix Compliance server is secure, perform advanced configuration of the BigFix Compliance server.

Perform the following steps to configure the root certificate for the BigFix Compliance server:

1. Contact LDAP server administration and obtain a root certificate for LDAP, which contains one or more certificates (full chain of trust). The following example shows a root certificate:

```
-----BEGIN CERTIFICATE-----
MIIHZjCCBk6gAwIBAgISKESJLWXAAAACTANBgkqhkiG9w0BAQUFADBNMRMwEQYK
CRWmyVBwPWQBBUNdilPKJRQwpeYKCZImiZPyLGQBGRYEQ354jTEgGG7GA1UEAiU5
.
.
.
MTAzMzQxWjBZMRMwEQYKCZImiZPJVGQBGRYDbmV0MRkwFwYKCZImiZPyLGQBGRYJ
bnNyb290ZGV2MScwJQYDVQQDEx5DaXRXAEludGVybmFsIERldmljZSBDQSAwMyBM
-----END CERTIFICATE-----
```

   Note: Ensure that root certificate file is in `PEM` format.

2. Copy the root certificate file to the following directory: `C:\Program Files\BigFix Enterprise\SCA\jre\lib`.
3. Using command prompt, run the following command:

```
C:\Program Files\BigFix Enterprise\SCA\jre\bin\keytool -import
 -trustcacerts -file <certificate_file_name>
-alias certAliasName -keystore cacerts -storepass <password>
```

Where <*password*> is provided by the BigFix Support.

4. Restart BigFix Compliance.

Adding a directory server

To use LDAP, you must first configure a connection to your directory server.

You must have the Administrators role (Manage Directory Servers permission) to perform this task.

1. From the navigation bar, click to **Management > Directory Servers**.
2. Click **New** to create a LDAP connection.
3. Enter a name for the new directory service.
4. In the LDAP server list, select the type of your LDAP server. If your LDAP server values are different from the defaults, select **Other** and enter the values of filters and attributes of your LDAP server. If you select Microsoft Active Directory **Global Catalog**, the Search Base field is optional.

   Important: The default values might need to be modified in particular for OpenLDAP servers due to various implementations of OpenLDAP.

5. Type the name of Search Base. This parameter defines the location in the directory from which the LDAP search begins.
6. Select the **SSL** check box, if your directory servers use Secure Socket Layer protocol (SSL).
7. Clear **Anonymous bind** and provide a name and a password for the user whose credentials are to be used for connecting to the directory server, if your server requires authentication.

   Tip: If you selected Microsoft Active Directory, provide the user name as Active Directory logon name or User Principal Name, for example `username@domain.com`. Do not specify the user name in the following way: `DOMAIN/username`.

8. Provide the host name or IP address of your primary LDAP server in the **Host** text field,
9. Accept the default port value or provide a new one.
10. **Optional:** To add a backup server:
    a. Click **add backup server**.
    b. Provide its host name or IP address and the port number.
11. Select the **Security Protocol** from the drop-down.

    Note: The available Security Protocols in SCA are TLS 1.0, 1.1, and 1.2, but we recommend to use TLS 1.2.

12. Click **Test Connection** to verify whether all of the provided entries are valid.
    A confirmation pop-up window opens.
13. Click **Create**. A confirmation message is displayed in the middle of the page.

You configured a connection to your LDAP server.

Editing a directory server

1. On the **Directory Servers** page, click the name of the directory server whose configuration you want to modify.
2. In the lower area of the window, enter the new parameters.
3. Click **Save**.

Deleting a directory server

1. On the **Directory Servers** page, click the name of the directory server whose configuration you want to delete.
2. In the upper left area of the window, click **Delete**.

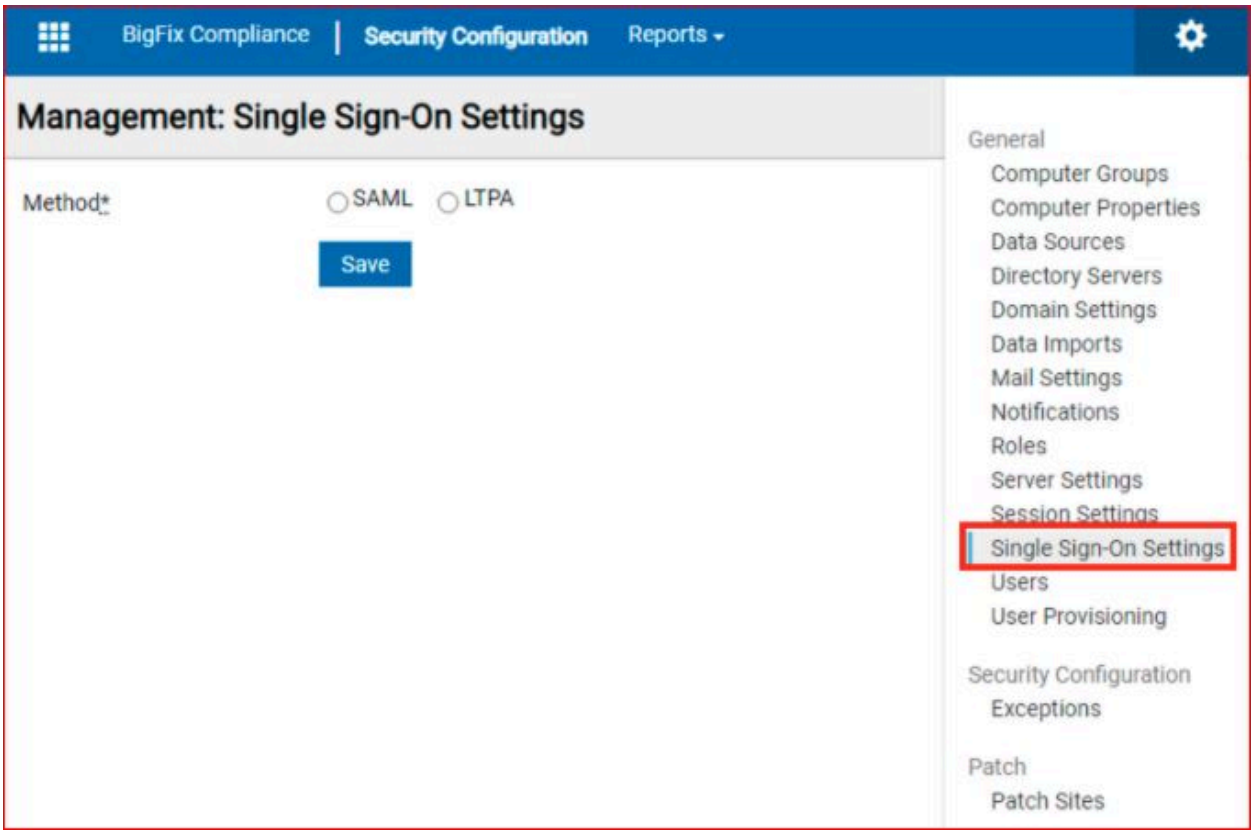
Single Sign-On Settings

Authenticating users with Single Sign-On

BigFix Compliance supports Single Sign-On (SSO) for user authentication through:

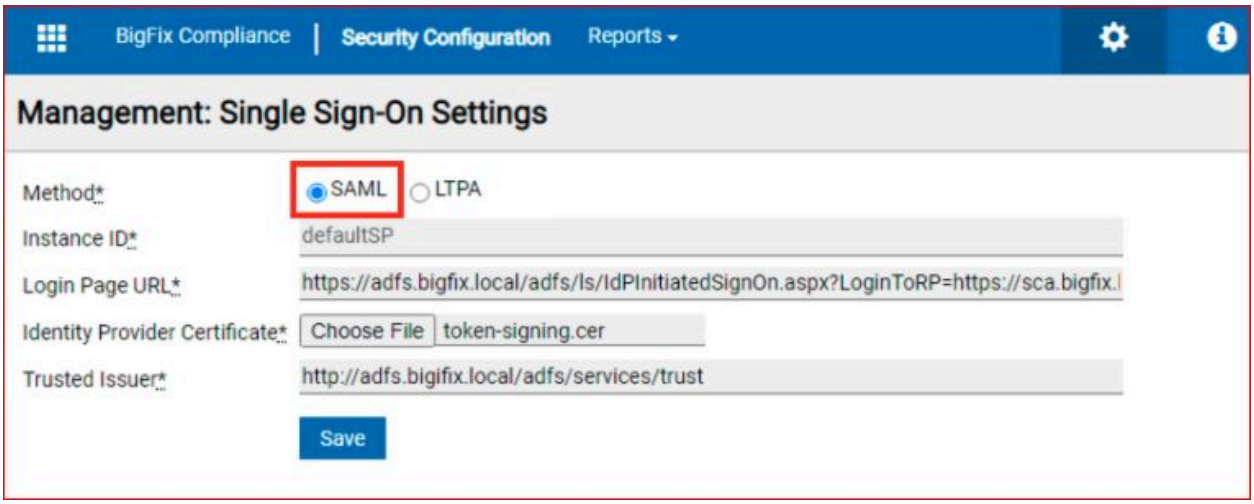
- Security Assertion Markup Language (SAML)
- Lightweight Third-Party Authentication (LTPA)

To open Single Sign-On Settings page, navigate to settings gear icon and click **Single Sign-On Settings** from the list.



Configuring SAML Single Sign-On

Follow the steps below to set up SAML Single Sign-On for your system with Active Directory Federation Services (ADFS).



Before you begin

- Get the following information from the identity provider (IdP):
  - Login URL
  - Token-Signing Certificate
  - Trusted Issuer
- Backup on the following `.xml` files:
  - <Install Dir>\wlp\usr\servers\server1\server.xml
  - <Install Dir>\wlp\usr\servers\server1\app\tema.war\web.xml
- When enabling Single Sign-On in Server Settings, you must have at least one Single Sign-On user created. Before enabling Single Sign-On, you need to do the following:
  - Create Single Sign-On users from **Management > Users**Management > Users. The operator must create at least one user with Administrators role and Single Sign-On as Authentication Method.
  - Consider changing the authentication method of existing users to Single Sign-On.
  - Create User Provisioning rules as necessary (optional)

Note: The user name format for user provisioning must be a User-Principal-Name (or a SAM-Account-Name, without domain). User provisioning on Single Sign-On is associated with what is indicated on the directory server.

1. Login to BigFix Compliance as an administrator (with FQDN URL).
2. Create a SSO user with administrator rights in the BigFix Compliance server.

    a. Go to **Management > Users**. Click **Create User**.

    b. Enter a user name. The format of the user name is related to the Name ID format of the claim rules on relaying party trust on ADFS. Ensure that the user name format follows the LDAP attribute format.

    User-Principal-Name

    The user name format is `<user>@<domain name>`.

    Example: `user01@bigfix.local`

    SAM-Account-Name

    The user name format is `<user>` without domain part.

    Example: `user01`

    E-Mail Address

    The user name is the email address in the profile of the user.

    Example: `user01@bigfix.local`

    c. Check Administrators role.

    Note: At least one Single Sign-On user needs to have Administrators role.

    d. Specify **Computer Groups**, as necessary (not applicable for administrator).

    e. Select **Single Sign-On** as the Authentication Method.

    f. Enter the **email address** and **contact information** (optional).

    g. Click **Create**.
3. Follow these steps if you plan to use user provisioning.

a. Add your directory server by creating an entry in **Management > Directory Servers**. (See Directory Servers *(on page 64)* section).
b. Configure the user provisioning rule in **Management > User Provisioning**. When Single Sign-On is enabled, the authentication method of all the provisioned users is Single Sign-On. (See User Provisioning section)

4. Create a SAML configuration entry.

   a. Click **New**.

   b. Select **SAML** as the Single Sign-On method.

   c. Enter the values for the following field(s).
      - **Login Page URL**: Enter the log in page URL. `https://<ADFS_hostname>/adfs/ls/IdPInitiatedSignOn.aspx?LoginToRP=https://<SCA_hostname>:9081/ibm/saml20/defaultSP`
      - **Identity Provider Certificate**: Browse to select the identity provider certificate. This certificate refers to the Token-Signing certificate exported from ADFS in DER/Base64 encoded X.509.
      - **Trusted Issuer**: Enter the trusted issuer. `http://<ADFS_hostname>/adfs/services/trust`

   d. Click **Save**.

   e. Restart BigFix Compliance service.

5. Download the metadata of the service provider and configure the service provider details on the identity provider. Download the service provider metadata file, `spMetadata.xml` from the link.

   a. Log in to BigFix Compliance and go to **Management > Single Sign-On Settings**.

   b. Click the Download SP Metadata link to download the service provider metadata file, `spMetadata.xml`.

Note: When the SAML SSO entry is created, only the **Delete** button and the **Download SP Metadata** link are enabled. If the download link is not enabled, try the following:

i. Open the folder `C:\Program Files\IBM\SCA\wlp\usr\servers\server1\apps\tema.war\WEB-INF\config\` or the BigFix Compliance installation path.
ii. Copy the `options.cfg.sample` file and save it as `options.cfg` into the folder.
iii. Open the `options.cfg.` file and locate the line: `#platform.sso.saml.metadata.link.ssl.verify=false`.
iv. Remove # from the code and save the file.
v. Restart the Compliance service.
vi. Log in again and check if the download link is enabled.

After the `spMetadata.xml` is downloaded, configure Relying Party Trusts in ADFS Management with the metadata file.

i. In ADFS Management, navigate to **Relying Party Trusts**, click **Add Relying Party Trust**.
ii. Click **Start** and select **Import data about the relying party from a file**.
iii. Click **Browse** and specify the `spMetadata.xml` file and click **Next**.
iv. Specify a display name (for example Compliance) and click **Next**.
v. Click **Next** all the way and **Close**.
vi. In Edit Claim Rules window, click **Add Rule** and click **Next**.
vii. Enter a claim rule name such as Name ID.
viii. Select **Active Directory** as attribute store.
ix. Select **User-Principal-Name** as LDAP Attribute and **Name ID** as Outgoing Claim Type.
x. Click **Finish**.

Once ADFS is configured, continue to enable SSO in BigFix Compliance, on **Management > Single Sign-On** page:

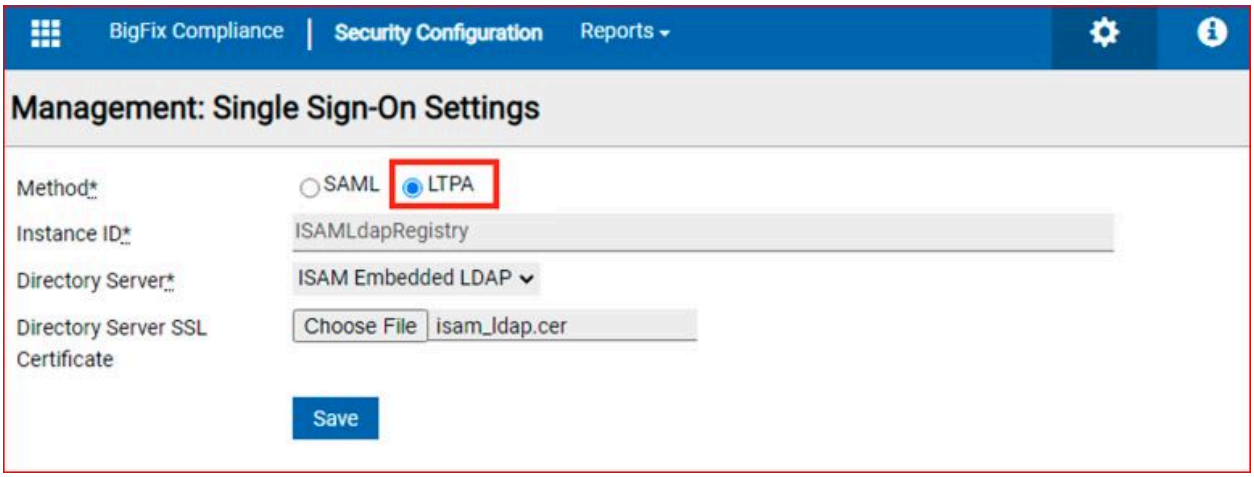
c. Click **Enable**.

d. Restart BigFix Compliance service.

After the service is restarted, BigFix Compliance login page will redirect to the login page of the identity provider. Enter your credentials. Once authentication is successful, it will be redirected to BigFix Compliance landing page (Security Configuration Overview page).

Configuring LTPA Single Sign-On for your system

Follow these steps to set up Lightweight Third-Party Authentication (LTPA) SSO for your system with IBM Security Access Manager for Web (ISAM).



Before you begin

Note: After the Single Sign-On is enabled, only Single Sign-On users can log in to BigFix Compliance Analytics. To avoid log-in access issues, all existing users, except the local Administrator user, should convert to Single Sign-On users.

When enabling Single Sign-On in Server Settings, you must have existing Single Sign-On users. Before enabling Single Sign-On, you need to do the following:

- Identify ISAM server, Directory Server and Compliance Server
- Backup on the following `.xml` files:
  - `<Install Dir>/wlp/usr/servers/server1/server.xml`
  - `<Install Dir>/wlp/usr/servers/server1/app/tema.war/web.xml`
- Create Single Sign-On users from **Management > Users**. The operator must create at least one single sign-on user with Administrators role.
- Create User Provisioning rules.

Note: The user name format for user provisioning must be a User-Principal-Name (or a SAM-Account-Name, without domain). User provisioning on single sign-on is associated with what is indicated on the directory server.

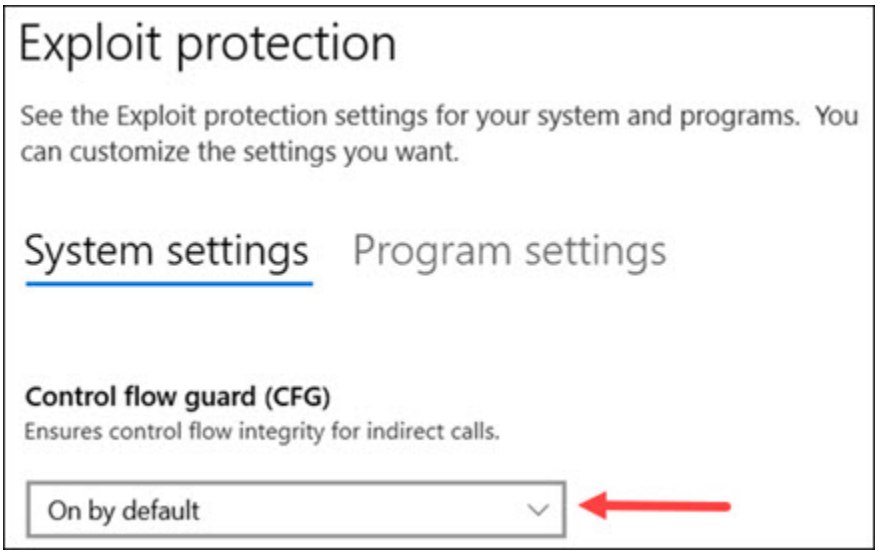
1. Login to BigFix Compliance and go to **Management > Directory Servers**.
2. Create a Directory Server entry for single sign-on authentication. (See Adding a directory server *(on page 67)* section for how to add a Directory Server).
3. Go to **Management > Users** to create an Single Sign-On user.
   a. Go to **Management > Users**. Click **Create User**.
   b. Enter a user name that is registered in the directory server.
   c. Check **Administrators** role (at least one single sign-on user needs to have Administrators role).
   d. Specify Computer Groups, as necessary. (not applicable for administrator).
   e. Select Single Sign-On as the Authentication Method.
   f. Enter the email address and contact information (optional).
   g. Click **Create**.
4. Create an LTPA configuration entry.
   a. Go to **Management > > Single Sign-On Settings**.
   b. Select **LTPA** as the Single Sign-On method.
   c. Select the directory server that was created in Step 2.
   d. If the directory server is configured with SSL option, click **Browse** and upload the directory server's certificate.
   e. Click **Save**.
5. Restart Compliance service.

6. Download LTPA Keys from Compliance.
    a. Login back to Single Sign-On Settings page.
    b. Click **Download LPTA Keys** link and save `ltpa.keys`.
7. Configure reverse proxy / virtual junction on ISAM with Compliance's server certificate and LTPA keys (See https://help.hcltechsw.com/bigfix/10.0/inventory/Inventory/security/t_configuring_sso_isam.html for details).
8. Enable Single Sign-On in Compliance.
    a. Login back to Single Sign-On Settings page.
    b. Click Enable.
9. Restart Compliance service.
10. Access Compliance by ISAM's virtual host/url (such as https://<virtual_host>/sca)

Adding Exception to Exploit Protection Control Flow Guard in Windows 2019

This topic describes how to add exception to the Control flow guard (CFG) to prevent the BigFix Compliance and Inventory services from crashing.

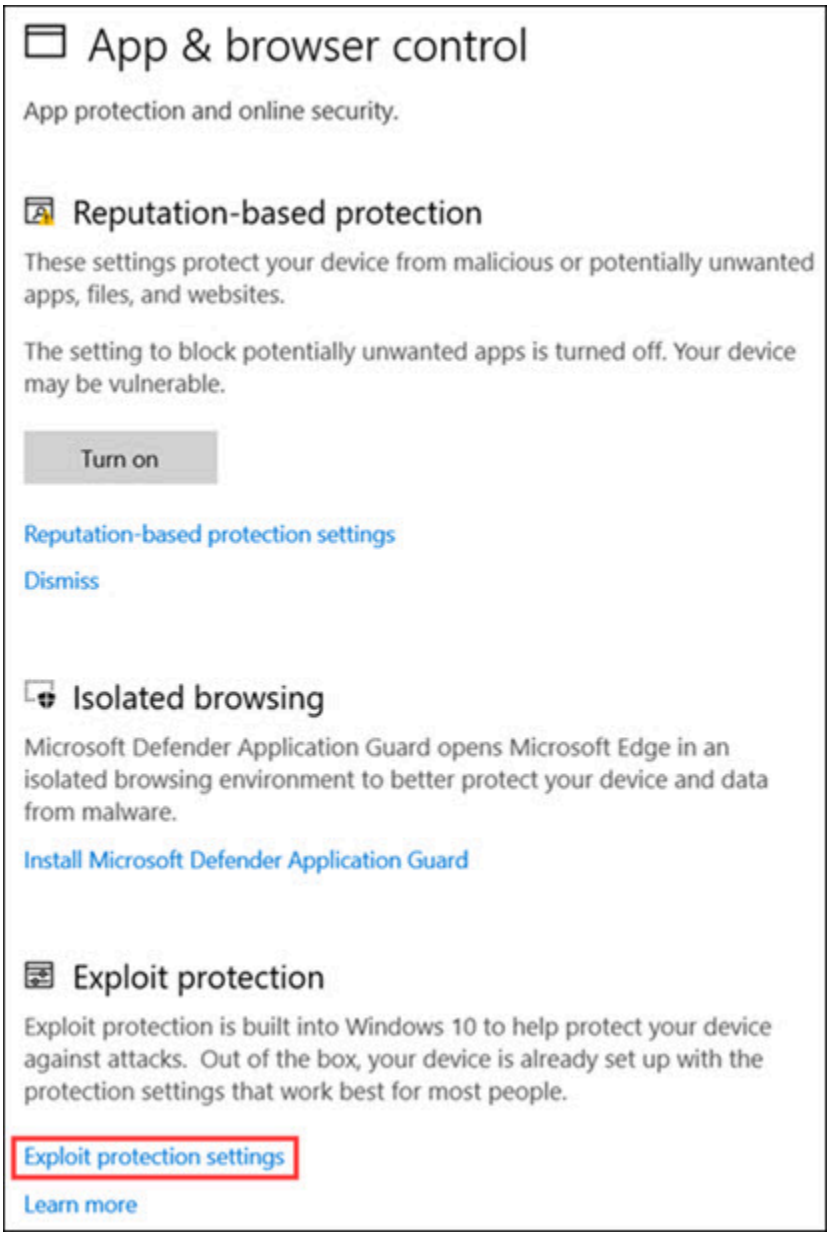
By default, the CFG for BigFix Compliance and Inventory `javaw.exe` file is set to **Use default (On)** when you update BigFix servers to Windows 2019. When CFG is explicitly set to **On by default**, the Security Assertion Markup Language (SAML) is enabled, and the first authentication to ADFS or SSO causes the BigFix Compliance and Inventory services to crash. Also, there are no error logs recorded in the `tema.log` file related to the crash. To prevent this, you must add custom setting for `javaw.exe`.



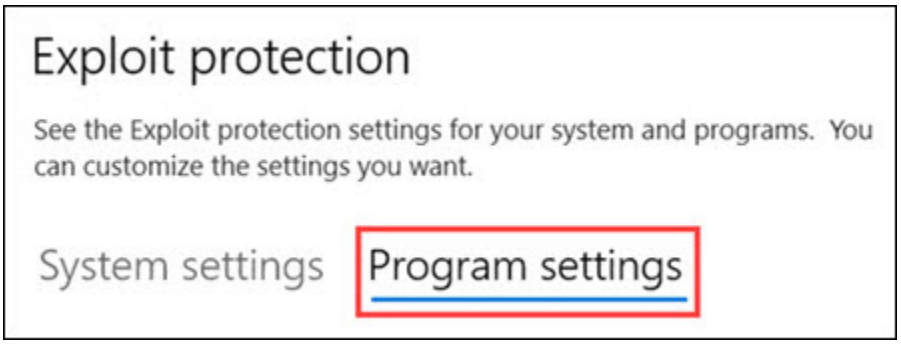
Note: CFG set to **On by default**, which results in crashing BigFix Compliance and Inventory services.

Perform the following steps to turn off the CFG:

1. Go to **Settings > Update & security > Windows security > App & browser control** and click **Exploit protection settings**.

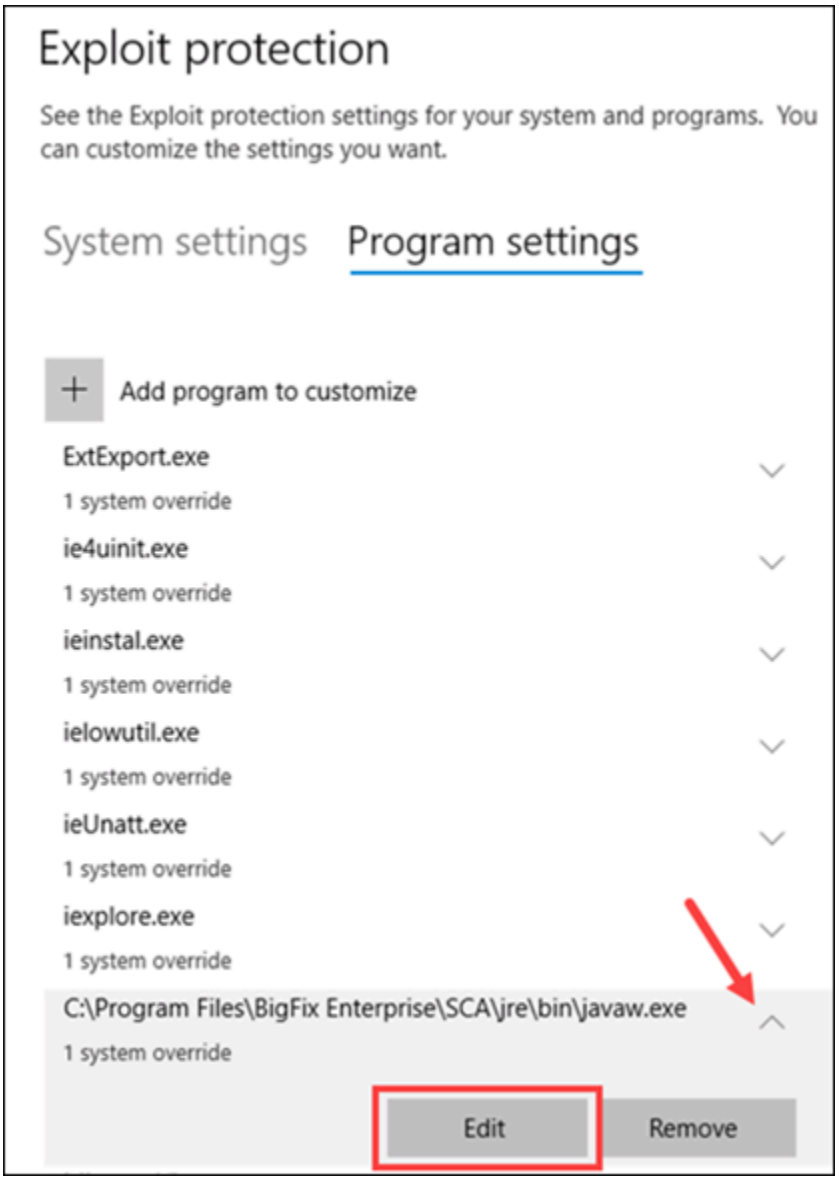


2. Click **Program settings**.

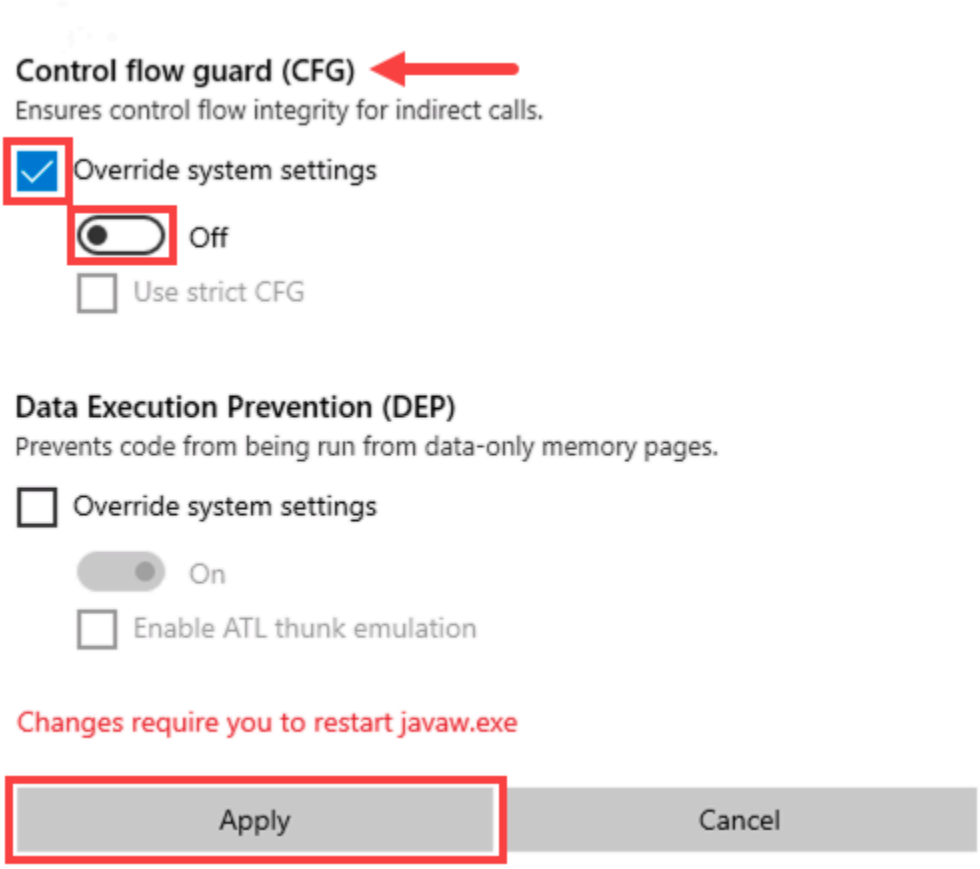


3. In the **Program settings** tab, navigate to `javaw.exe` and from the drop-down click **Edit**.

Note: By default, the `javaw.exe` file is located in the `<SCA>\jre\bin\` folder.



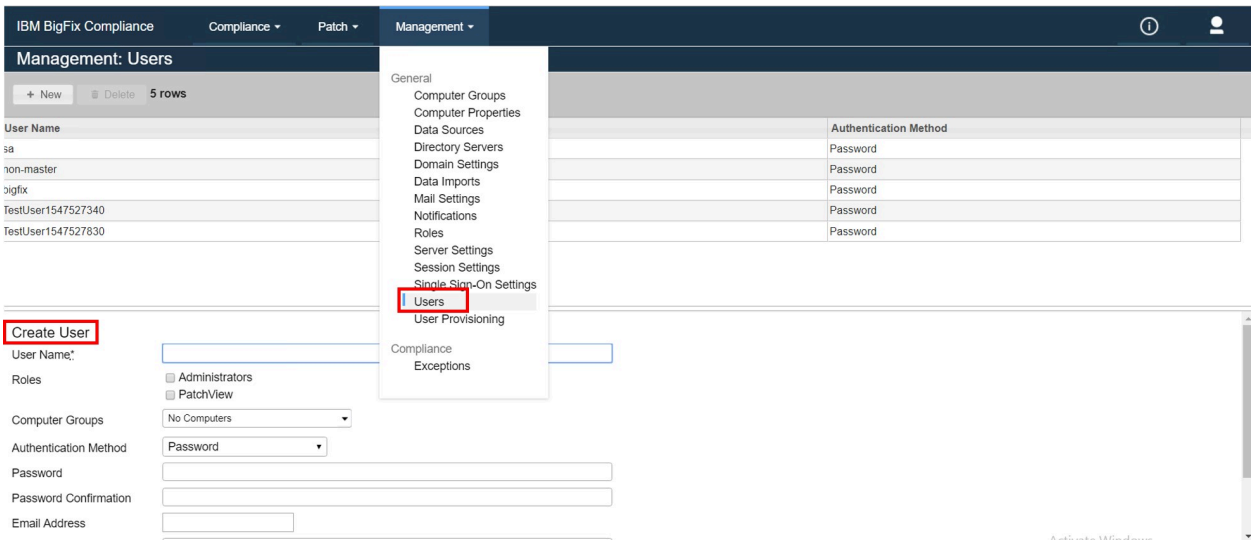
4. In **Control flow guard (CFG)** settings, check **Override system settings** and set the toggle switch to **Off**.
5. Click **Apply**.



Important: Restart the BigFix Compliance service to implement the changes.

Users

From the Users interface, 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.



Important: Administrators must select relevant roles for the user. User will be able to view/edit the reports based on the selected role.

Configuring multiple computer groups

You must have Administrator privileges or use the Manage Computers Group role to configure user accounts to include multiple computer groups.

This feature enables non-Administrator users to view ranges for computer group compliance data by granting the user access to multiple computer group during user creation or user account updates.

1. Log in to Security Compliance and Analytics as an Administrator or using the Manage Computer Groups role.
2. From the navigation menu, click **Management**. Select **User** from the dropdown menu.
3. From the **Managers: Users** window, create a new user.
    a. Enter the details for the following fields:
    b. From the Computer Groups dropdown menu, select the computer groups that the new user will be associated with.

c. Enter then confirm a password.
d. Enter the email address.

4. From the top navigation menu, click **Reports**. Click **Import Now**.

To confirm if the multiple group was configured correctly, login to the new user account that has more than one computer group associated with it.

Configuring LDAP

HCL BigFix for BigFix Compliance Analytics 1.9 supports authentication through the Lightweight Directory Access Protocol (LDAP) server. You can add LDAP associations to HCL BigFix Analytics so you and other users can log in using credentials based on your existing authentication scheme.

To use LDAP for authentication of HCL BigFix Analytics users, you must do the following steps:

- Add an LDAP server directory
- Link a user to the created directory

You can also use the user provisioning feature to authenticate LDAP users without creating individual users in the application.

Adding LDAP servers

To use LDAP for authentication of HCL BigFix Analytics users, you must add a working LDAP directory.

You must be an Administrator to do this task.

1. Log in to the TEMA application server.
2. Go to **Management > Directory Servers**.
3. To create an LDAP connection, click **New**.
4. Enter a name for the new directory.

5. Select an LDAP Server for authentication from a list and enter the name of a Search Base
6. If the values of your LDAP server are different from the default, select **Other** from the LDAP Server list.
7. Enter values of filters and attributes of your LDAP server.
8. Enter a name and a password for the authenticated user.
9. If your LDAP server uses Secure Socket Layer protocol, select the **SSL** check box. If you require no user credential, select the **Anonymous Bind** check box.
10. In the Host field, provide the host name on which the LDAP server is installed.
11. Enter the Port.
12. To verify whether all of the provided entries are valid, click **Test Connection**.
13. Click **Create**. You configured a system link to an authentication system.
14. To add a backup LDAP server, in the Primary Server tab, click the **Add backup server** link.
    a. Enter the host and IP of the backup LDAP server.
    b. Click **Test Connection** to verify whether all of the provided entries are valid.
    c. Click **Save** to confirm the changes.
15. Optional: To edit the directory, select its name. Click **Save** to confirm the changes.
16. Optional: To delete the created directory, select its name. In the upper left of the window, click **Delete**.

Linking users to directories

To complete an authentication process through LDAP, you must create a user that would link to the created directory.

You must be an Administrator to do this task.

1. Log in to the TEMA application server.
2. Go to **Management > Users**.
3. To create a user, click **New**.
4. In the **Username** field, enter the name of an existing user of an LDAP server.
5. From the list, select a Computer Group that the user would be assigned to.
6. From the Authentication Method list, select the name of an LDAP directory.

7. Click **Create**.
8. 8. Optional: To delete the created user, click its name. Then in the upper left of the window, click **Delete**.

To confirm authentication, log in to the BigFix Analytics server with the credentials.

Authenticating LDAP through user provisioning

You can configure the LDAP group permission to authenticate LDAP users without creating users individually in SCA.

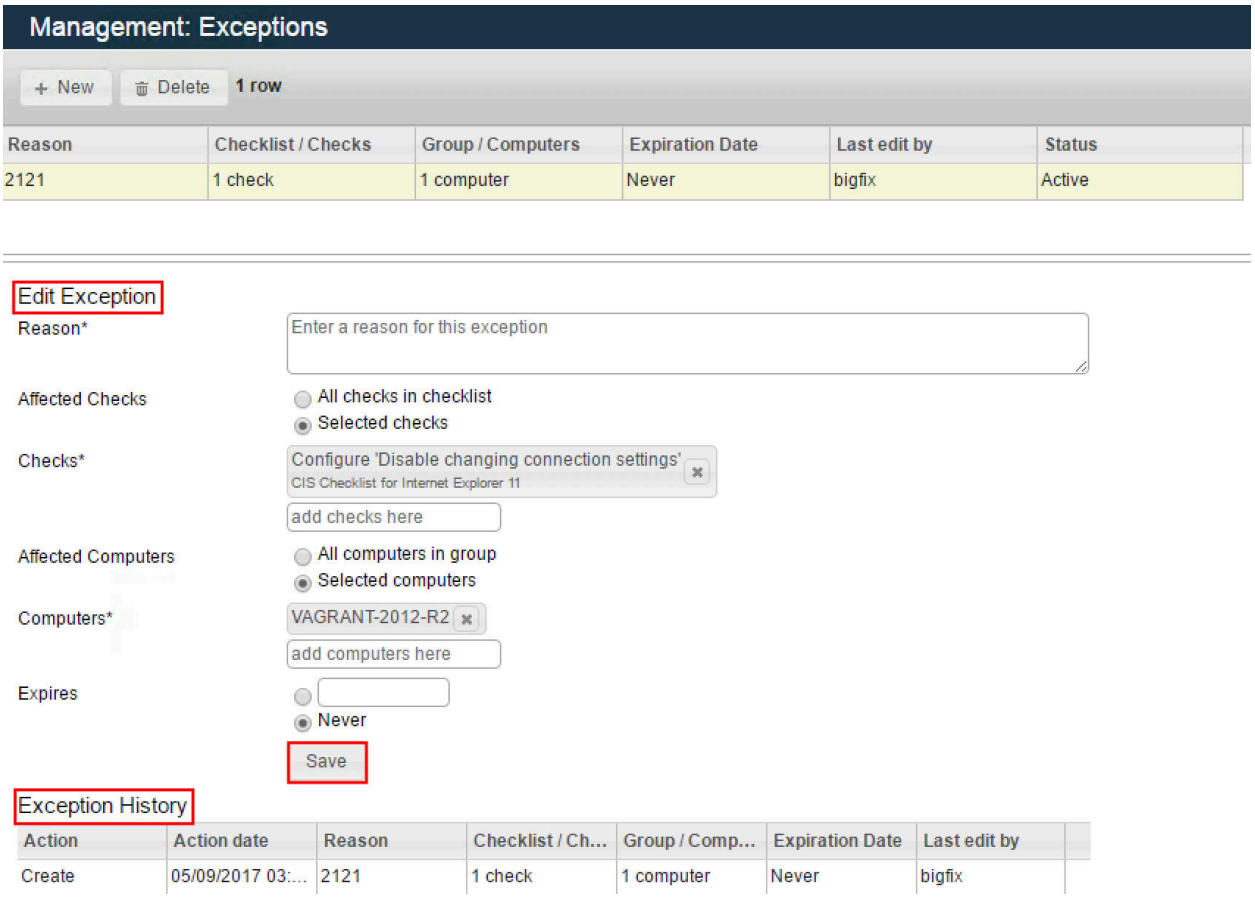
You must configure at least one directory with a working LDAP group in the LDAP server.

1. Log in to the TEMA application server.
2. Go to **Management > User Provisioning**.
3. To create a user, click **New**.
4. In the **Group Names** field, type the name of an existing group of an LDAP server.
5. From the list, select a Computer Group that the TEMA would grant for authentication.
6. From the **Roles** field, click one or more roles that the group users granted for access permission.
7. From the **Computer Group** field, select a computer group that the group users would be assigned to.
8. Click **Create**.

To confirm authentication, log in to the BigFix Analytics server with user within the LDAP group you created.

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.



Policy Management

View external content, create policies, and publish content from **Policy Management**.

The **Policy Management** section has two tabs.

Policy Library tab

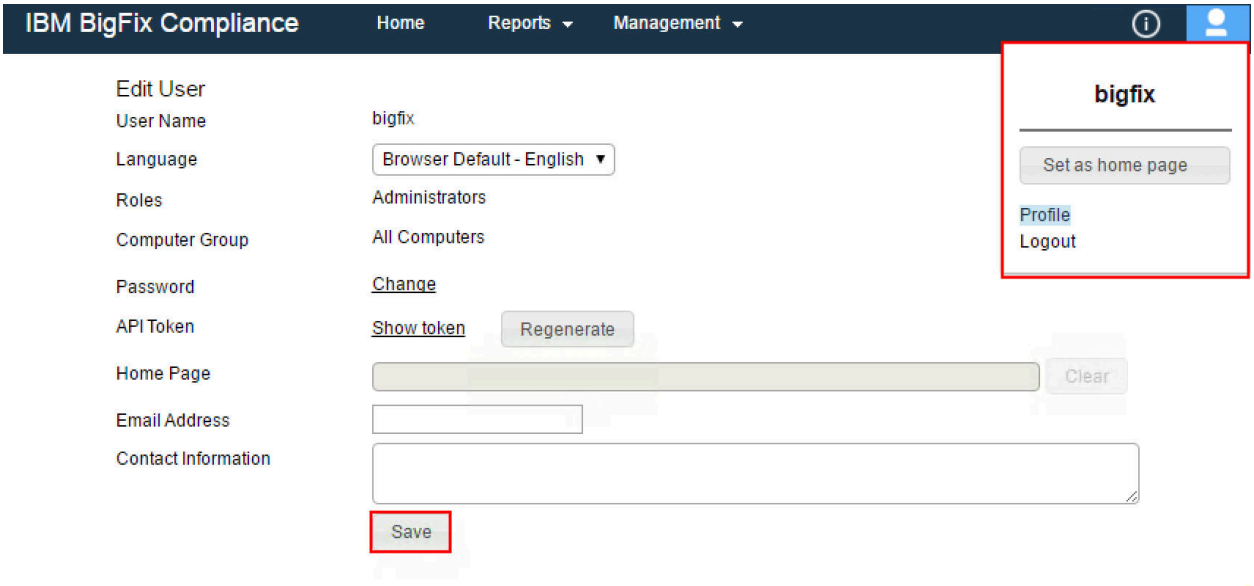
Access all external content to which you are subscribed. You can search and filter by content, operating system, and checklists. You can sort by check, checklist name, the most recent. Select the checklist and click **Add to workspace** to place your selections in the **Workspace** tab.

Workspace tab

From this tab, you can view and publish content that were selected from the **Policy Library** tab. After clicking **Publish**, the checklist site and analysis are created. Once you click **Save**, all content are created in the BigFix server.

Account Preferences

Use the Account Preferences interface to change passwords, contact information, or API tokens. Click the *Account* drop-down menu from the top of the window.



Chapter 5. Configuring report definitions using REST API

Administrators can use REST API to create, update, and delete saved report view definitions across TEMA instances.

Overview of REST API report definitions

The operations of the BigFix Compliance Analytics REST API protocol is defined as HTTP methods on certain REST resources.

Table 7. Target REST Operations

Target REST operation URI	HTTP methods	Purpose of the operation
`api/reports`	POST	Create a saved report item.
`api/reports`	PUT	Update a saved report item by ID.
`api/reports`	GET	Retrieve all saved report items.
`/api/reports/<id>`	GET	Retrieve a saved report item by ID.
`api/reports`	DELETE	Delete a saved report item by ID.

Path parameters

The `path` parameter specifies the report name that is used when configuring the report definitions.

Table 8. Path parameters of Security Compliance and Analytics reports

Report name	Path parameter
Overview	`/scm`

Table 8. Path parameters of Security Compliance and Analytics reports

(continued)

Report name	Path parameter
Checklists	`/scm/checklists`
Checks	`/scm/checks`
Vulnerabilities	`/scm/vulnerabilities`
Computers	`/scm/computers`
Computer Groups	`/scm/computer_groups`
Check results	`/scm/check_results`
Exception Results	`/scm/exception_results`
Vulnerability Results	`/scm/vulnerability_results`

Query parameters

Table 9. Query parameters

Parameter	Description
`token`	The API token for the target user.
`ID`	The saved report ID. This parameter is not used for input.
`user_id`	The user ID of the report owner in TEMA. This parameter is not used for input.
`pagestate_id`	The page state ID that is specific to the report. This parameter is not used for input.
`name`	The name of the saved report.

Table 9. Query parameters

(continued)

Parameter	Description
`path`	The path that specifies the report (for example Overview, Computer Groups, and others).
`private`	The value is True for private and False for public.
`state`	
`column`	The columns in a saved report.
`column_order`	The order of the columns as specified by `<column name" : <number>`. The order of the column number starts from the left, with the smallest column number. The value of the number must be integers, such as 0, 1, 2, 3, and so on.
`criteria`	The conditions found in **Configure View > Filter**.
`grid_options`	The Autosize Columns options in **Configure View**.
`autosize_columns`	This parameter is present when Autosize Columns is on
`order`	
`asc`	The parameter that is true for ascending order; False for descending order
`col`	The parameter for the column to be sorted. The value is null for none.
`time_range`	
`type`	
`all`	The parameter for `all` types

Table 9. Query parameters

(continued)

Parameter	Description
`relative`	The parameter for the last *X* day/week/month/year
`absolute`	The parameter for a specific date range
`units`	"days", "weeks", "months", "years"
`value`	The value for the last X units
`min`	Starting datetime (range)
`max`	Ending datetime (range)
`column_widths`	The column widths that are specified by `<column name> : <width>`

Create a saved report

Use Rest API to create a saved report across Compliance instances.

Use the POST operation on the `api/reports` element to create a saved report.

Table 10. Operation details

Operation details	Description
Operation	`POST/api/reports`
Purpose	Create a saved report item.
HTTP method	`POST`

Table 10. Operation details

(continued)

Operation details	Description
Request `content type`	`Application/json`
Normal HTTP response codes	`200 OK` + JSON data for single saved report definition that is created by POST

Error response codes

The following list includes the operation details for error response codes.

`500 + "Error: Name is already taken"`

When a duplicate post is made. The report is unique by name, user, and report category.

`500 + "Error: The property '#/' did not contain a required property of 'name' in schema f967028a-a442-59a2-ac38-8b596bcf8d2a#"}"`

When the header is missing `content-type: application/json`.

`401 Unauthorized + {"error":"There is no match for the provided user name and password"}`

When no token is provided.

`404 Not found`

When using unnecessary ID (`POST/api/reports/<id>`

`500 Internal Server Error ('Sorry something went wrong...')` + error in the TEMA log

When the JSON format is invalid.

`401 Unauthorized + {"error":"You are not assigned a Computer Group. You will not be able to access the system until you are assigned a valid Computer Group. Contact your administrator for assistance."}`

When the token for the user has no computer assigned.

`404 + {"error":"Sequel::RecordNotFound"}`

When the ID is invalid.

`404 + {"error":"Sequel::RecordNotFound"}`

When accessing the private report of another user.

`500 + {"error":"There was a problem with your request."}500 + {"error":"The property '#/path' value \"aaa\" did not match the regex '^(/[^/]+)+$' in schema f967028a-a442-59a2-ac38-8b596bcf8d2a#"}`

When specifying path parameters that do not exist, such as `/scm/test`, `aaa`, and others.

`500 + {"error":"The property '#/state/column_order/id' of type String did not match the following type: integer in schema afc10b8d-2caf-50e7-a82e-a083dc10ee61#"}`

When there is a parameter type mismatch such as previously specifying a string for an integer. You must delete then recreate the saved report with API, or save the report again from the UI.

`"criteria":{ "and":["aaa","bbb"] } 500 + {"error":"Argument must be a Hash, Array, or Criterion"}`

When the criteria specification is invalid.

Note: When an invalid column is selected, such as columns from a different report, the created saved report returns the default columns but without any data, or the specified column name is saved but ignored.

Update a saved report

Use Rest API to update a saved report across Compliance instances.

Use the PUT operation on the `api/reports` element to update a saved report by ID.

Table 11. Operation details

Operation details	Description
Operation	`PUT/api/reports`
Purpose	Update a saved report item.
HTTP method	`PUT`
Request `content type`	`Application/json`
Normal HTTP response codes	`200 OK` + JSON data for single saved report definition that is updated by PUT

Error HTTP response codes

The following list includes the operation details for HTTP error response codes.

`500 - "Error: The property '#/' did not contain a required property of 'name' in schema f967028a-a442-59a2-ac38-8b596bcf8d2a#"`

When the header is missing `content-type: application/json`.

`500 + {"Error":"the before_save hook failed"}`

PUT with non-owner's token.

`401 Unauthorized + {"error":"There is no match for the provided user name and password"}`

When no token is provided.

`404 Not Found`

When the ID is missing.

`500 Internal Server Error ('Sorry something went wrong...')` + error in the TEMA log

When the JSON format is invalid.

`401 Unauthorized + {"error":"You are not assigned a Computer Group. You will not be able to access the system until you are assigned a valid Computer Group. Contact your administrator for assistance."}`

When the token for the user has no computer assigned.

`404 + {"error":"Sequel::RecordNotFound"}`

When the ID (#) is invalid.

`404 + {"error":"Sequel::RecordNotFound"}`

When accessing the private report of another user.

`500 + {"error":"There was a problem with your request."}500 + {"error":"The property '#/path' value \"aaa\" did not match the regex '^(/[^/]+)+$' in schema f967028a-a442-59a2-ac38-8b596bcf8d2a#"}`

When specifying path parameters that do not exist, such as `/scm/test`, `aaa`, and others.

`500 + {"error":"The property '#/state/column_order/id' of type String did not match the following type: integer in schema afc10b8d-2caf-50e7-a82e-a083dc10ee61#"}`

When there is a parameter type mismatch such as previously specifying a string for an integer. You must delete then recreate the saved report with API, or save the report again from the UI.

`"criteria":{ "and":["aaa","bbb"] } 500 + {"error":"Argument must be a Hash, Array, or Criterion"}`

When the criteria specification is invalid.

Note: When an invalid column is selected, such as columns from a different report, the created saved report returns the default columns but without any data, or the specified column name is saved but ignored.

Retrieve all saved report items

Use Rest API to retrieve all saved report items across Compliance instances.

Use the GET operation on the `api/reports` element to create a saved report by the report ID.

Table 12. Operation details

Operation details	Description
Operation	`GET/api/reports/<report id>`
Purpose	Retrieves all saved report items.
HTTP method	`GET`
Request `content type`	`Application/json`
Normal HTTP response codes	`200 OK` + JSON data (total count + array of saved report definitions)

Error HTTP response codes

The following list includes the operation details for HTTP error response codes.

`401 Unauthorized + {"error":"You are not assigned a Computer Group. You will not be able to access the system until you are assigned a valid Computer Group. Contact your administrator for assistance."}`

When the token for the user has no computer assigned.

`401 Unauthorized + {"error":"There is no match for the provided user name and password"}`

When no token is provided.

`404 + {"error":"Sequel::RecordNotFound"}`

When the ID (#) is invalid.

`404 + {"error":"Sequel::RecordNotFound"}`

When accessing the private report of another user.

```
500 + {"error":"There was a problem with your request."}500 +
{"error":"The property '#/path' value \"aaa\" did not match the regex '^(/
[^/]+)+$' in schema f967028a-a442-59a2-ac38-8b596bcf8d2a#"}
```

When specifying path parameters that do not exist, such as `/scm/test`, `aaa`, and others.

```
500 + {"error":"The property '#/state/column_order/id' of type String did
not match the following type: integer in schema afc10b8d-2caf-50e7-a82e-
a083dc10ee61#"}
```

When there is a parameter type mismatch such as previously specifying a string for an integer. You must delete then recreate the saved report with API, or save the report again from the UI.

```
"criteria":{ "and":["aaa","bbb"] } 500 + {"error":"Argument must be a
Hash, Array, or Criterion"}
```

When the criteria specification is invalid.

Note: When an invalid column is selected, such as columns from a different report, the created saved report returns the default columns but without any data, or the specified column name is saved but ignored.

Retrieve saved reports by report ID

Use Rest API to retrieve a saved report by ID across Compliance instances.

Use the GET operation on the `api/reports` element to create a saved report by the report ID.

Table 13. Operation details

Operation details	Description
Operation	`GET/api/reports/<report id>`
Purpose	Retrieves all saved report items using the report ID.
HTTP method	`GET`
Request `content type`	`Application/json`
Normal HTTP response codes	`200 OK` + JSON data for single saved report definition that is specified by ID.

Error HTTP response codes

The following list includes the operation details for HTTP error response codes

`401 Unauthorized + {"error":"You are not assigned a Computer Group. You will not be able to access the system until you are assigned a valid Computer Group. Contact your administrator for assistance."}`

When the token for the user has no computer assigned.

`401 Unauthorized + {"error":"There is no match for the provided user name and password"}`

When no token is provided.

`404 + {"error":"Sequel::RecordNotFound"}`

When the ID (#) is invalid.

`404 + {"error":"Sequel::RecordNotFound"}`

When accessing the private report of another user.

`500 + {"error":"There was a problem with your request."}500 + {"error":"The property '#/path' value \"aaa\" did not match the regex '^(/[^/]+)+$' in schema f967028a-a442-59a2-ac38-8b596bcf8d2a#"}`

When specifying path parameters that do not exist, such as `/scm/test`, `aaa`, and others.

`500 + {"error":"The property '#/state/column_order/id' of type String did not match the following type: integer in schema afc10b8d-2caf-50e7-a82e-a083dc10ee61#"}`

When there is a parameter type mismatch such as previously specifying a string for an integer. You must delete then recreate the saved report with API, or save the report again from the UI.

`"criteria":{ "and":["aaa","bbb"] } 500 + {"error":"Argument must be a Hash, Array, or Criterion"}`

When the criteria specification is invalid.

Note: When an invalid column is selected, such as columns from a different report, the created saved report returns the default columns but without any data, or the specified column name is saved but ignored.

Delete a saved report item by ID

Use Rest API to update a saved report item by ID across Compliance instances.

Use the DELETE operation on the `api/reports/<id>` element to Delete a saved report by id.

Table 14. Operation details

Operation details	Description
Operation	`DELETE/api/reports/<id>`
Purpose	Deletes a saved report item.
HTTP method	`DELETE`
Request `content type`	`Application/json`

Table 14. Operation details

(continued)

Operation details	Description
Normal HTTP response codes	`204 No Content`

Error HTTP response codes

The following list includes the operation details for HTTP error response codes.

`403 Forbidden + {"Error":"Access Blocked"}`

DELETE with the token of the non-owner, even if with administrative privilege.

`404 Not Found`

When the ID is missing.

`401 Unauthorized + {"error":"There is no match for the provided user name and password"}`

When no token is provided.

`401 Unauthorized + {"error":"You are not assigned a Computer Group. You will not be able to access the system until you are assigned a valid Computer Group. Contact your administrator for assistance."}`

When the token for the user has no computer assigned.

`404 + {"error":"Sequel::RecordNotFound"}`

When the ID is invalid.

`404 + {"error":"Sequel::RecordNotFound"}`

When accessing the private report of another user.

`500 + {"error":"There was a problem with your request."}500 + {"error":"The property '#/path' value \"aaa\" did not match the regex '^(/[^/]+)+$' in schema f967028a-a442-59a2-ac38-8b596bcf8d2a#"}`

When specifying path parameters that do not exist, such as `/scm/test`, `aaa`, and others.

`500 + {"error":"The property '#/state/column_order/id' of type String did not match the following type: integer in schema afc10b8d-2caf-50e7-a82e-a083dc10ee61#"}`

When there is a parameter type mismatch such as previously specifying a string for an integer. You must delete then recreate the saved report with API, or save the report again from the UI.

`"criteria":{ "and":["aaa","bbb"] } 500 + {"error":"Argument must be a Hash, Array, or Criterion"}`

When the criteria specification is invalid.

Note: When an invalid column is selected, such as columns from a different report, the created saved report returns the default columns but without any data, or the specified column name is saved but ignored.

Chapter 6. Disaster Recovery for BigFix Compliance Analytics

Use the standard cold standby method of creating a backup and restoring the system in your disaster recovery plan for BigFix Compliance Analytics.

Similar to the HCL BigFix disaster plan, BigFix Compliance Analytics uses a standard backup/restore method that is called the Cold Standby method. This method does periodic backups of the application server and database files, usually done nightly. If there is a problem, the database and application server files can be restored to the HCL BigFix Application Server computer or another computer. The system is also restored.

Table 15. Pros and cons of using the cold standby method

Pros	Cons
• Simple and allows for multiple backups over time. • Does not require any additional hardware. Hot or cold standby computer is optional.	• All information since the last backup is lost in the event of a failure. • Restoring the system from the backup might have significant downtime.

The disaster recovery plan covers steps for the following procedures:

1. Backup procedure
2. Recovery procedure
3. Recovery verification procedure

Creating a backup of the application server

Create backups of the files and folders that the application server uses.

Establish a maintenance plan for nightly backups for the TEM_Analytics databases using SQL Server Enterprise Manager. Multiple backup copies give greater recovery flexibility. Consider backing up to a remote system to allow for higher fault tolerance.

For recovery purposes, create backups of the following files and folders that the application server uses:

- `[TEMA Application folder]\config` -- Configuration (HTTPS, Port number, database connection information, and others)
- `[TEMA Application folder]\log` -- Archived Import, error, and access logs

Recovering the backup application server

Restore the backup of your BigFix Compliance Analytics application server.

1. Install the same version of SQL Server that was previously used in either a previous application server computer or a new computer.

   Note: If you used Mixed Mode Authentication on the previous application server, you must enable it for your new SQL installation.

2. Restore the TEM_Analytics databases from backup.
3. Install the application server. Use the same version of the application installation binary as was previously used.
4. At the end of installation, skip the launch web configuration step. Instead, go to NT Services Manager and stop 'Tivoli Endpoint Manager Analytics' service.
5. Restore/Replace the backed up configuration and log files and folders. Create the directory structure as needed.
6. Go to **NT Services Manager** and start the **Tivoli Endpoint Manager Analytics** service.

   Ensure that the new application server computer can access the following datasources: BFEnterprise and BESReporting. For NT Auth to access the TEM_Analytics and BFEnterprise databases, ensure that the service user has the necessary DB/File access rights).

Verifying the success of the recovery procedure

Check the historical log and run an import action to verify that the Compliance Application is successfully restored.

Do the following steps to ensure that the Compliance Application Server is successfully restored.

1. Go to Compliance web interface and login with Administrator rights to verify that the login works properly.
2. Go to **Management > Import** and verify the historical log shown in the page frame.

Appendix A. Example Reports - Compliance

View examples of the various BigFix Compliance Analytics reports.

The following table lists examples of reports that you can generate in BigFix Compliance Analytics.

Table 16. Examples of BigFix Compliance Analytics reports

Name of Report	Location	Field or Graph Names	Other functions	Export Format
Checklist List *(on page 107)*	From the console, click **Reports > Checklists**	**Name**, **Compliance**	**Save As** and **Schedule**	.CSV and .PDF
Checklist Overview *(on page 108)*	From the console, click **Reports > Checklists**. Click any of the checklists that are displayed.	Compliance History, Computers by Compliance Quartile, Check Results History	**Save As**, **Schedule**, and **Configure View**.	.PDF
Checks List *(on page 110)*	From the console, click **Reports > Checks**	Name, Desired Values, Compliance	**Save As**, **Schedule**, and **Configure View**.	.CSV and .PDF,
Check Overview *(on page 109)*	From the console, click **Reports > Checks**	Compliance History, Check Results History, overall compli-	**Save As**, **Schedule**, and **Configure View**.	.PDF

Table 16. Examples of BigFix Compliance Analytics reports

(continued)

Name of Report	Location	Field or Graph Names	Other functions	Export Format
		ance percentage		
Computers List *(on page 109)*	From the console, click **Reports > Computers**	Computer Name, Last Seen, Vulnerability history, and Overall compliance	**Save As**, **Schedule**, and **Configure View**.	.CSV and PDF
Computer Overview *(on page 110)*	From the console, click **Reports > Overview**	Compliance history, Computers by Compliance Quartile, and Check results history	**Save As**, **Schedule**, and **Configure View**.	.PDF
Computer Groups List *(on page 111)*	From the console, click **Reports > Computer Groups**	Name, Children (subgroups), Vulnerability history, and Compliance in a list format	**Save As**, **Schedule**, and **Configure View**.	.CSV and .PDF
Computer Group Overview *(on page 112)*	From the console, click **Reports > Computer Groups**. Click any com-	Compliance history, computers by compliance quartile, check results history, and vul-	**Save As**, **Schedule**, and **Configure View**.	.PDF

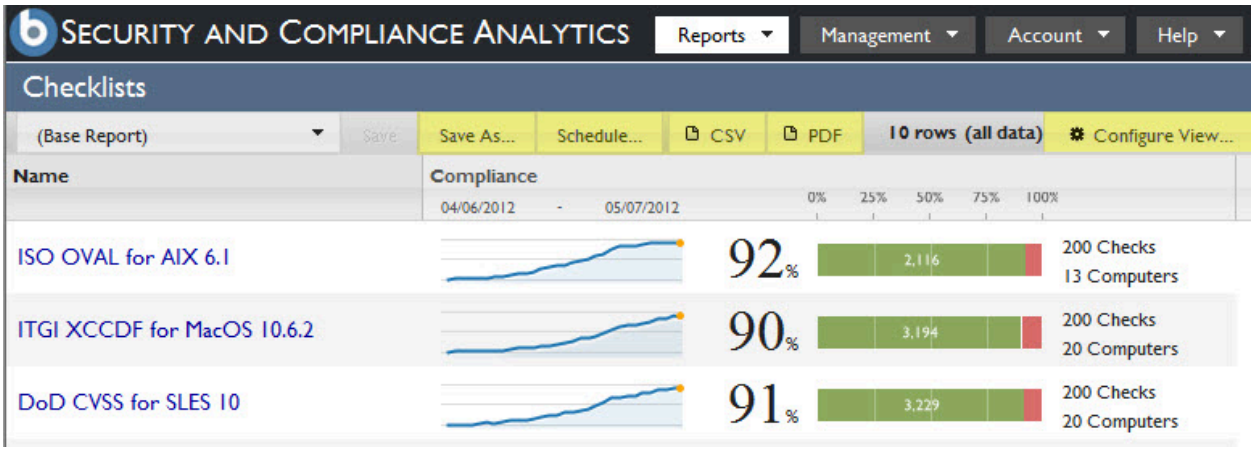
Table 16. Examples of BigFix Compliance Analytics reports

(continued)

Name of Report	Location	Field or Graph Names	Other functions	Export Format
	puter group in the list.	nerability history		
Check Results List *(on page 113)*	From the console, click **Reports > Check Results**	Checklist, check name, computer name, the date results were last seen, and level of compliance	**Save As**, **Schedule**, and **Configure View**.	.CSV and .PDF
Vulnerabilities *(on page 113)*	From the console, click **Reports > Vulnerabilities** or **Reports > Vulnerability Results**	CVE ID and Vulnerability History	**Save As**, **Schedule**, and **Configure View**.	.CSV and .PDF

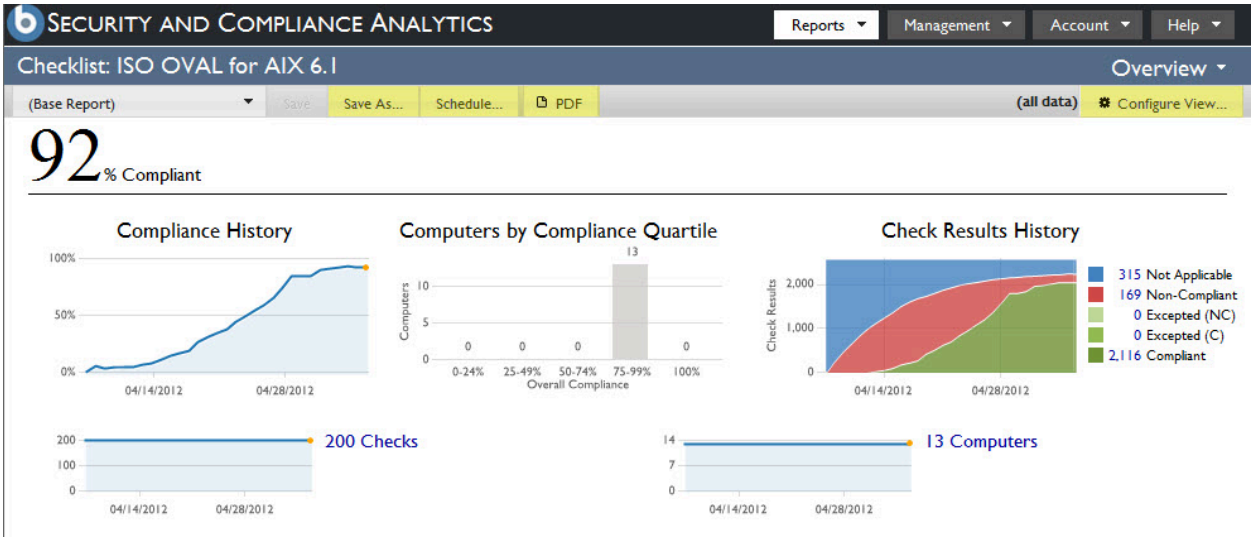
Checklist List Report

To access the Checklist List Report, click the Reports drop-down menu at the top of the console and select Checklists. This report displays data through name and compliance percentage fields. Use the links across the top to Save As, Schedule, export to .csv or .pdf, and Configure View.



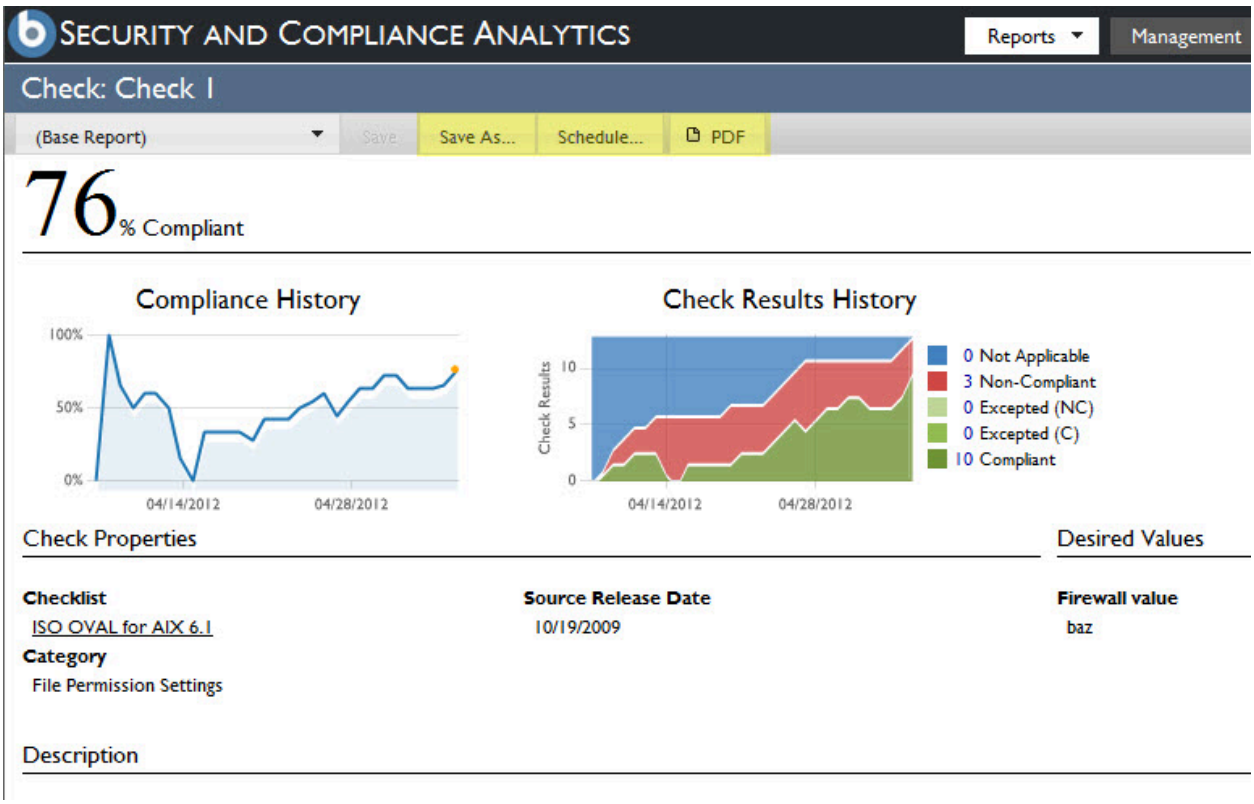
Checklist Overview Report

To access the Checklists Overview Report, click the Reports dropdown menu at the top of the console and select Checklists. The Checklist Overview Report is a drilldown of the Checklists List report. To access this view, click any checklist displayed. The Overview presents a graphic representation of compliance history, computers by compliance quartile, and check results history with an overall compliance percentage shown in the top left corner of the console. Use the links across the top to Save As, Schedule, export to .pdf, and Configure View.



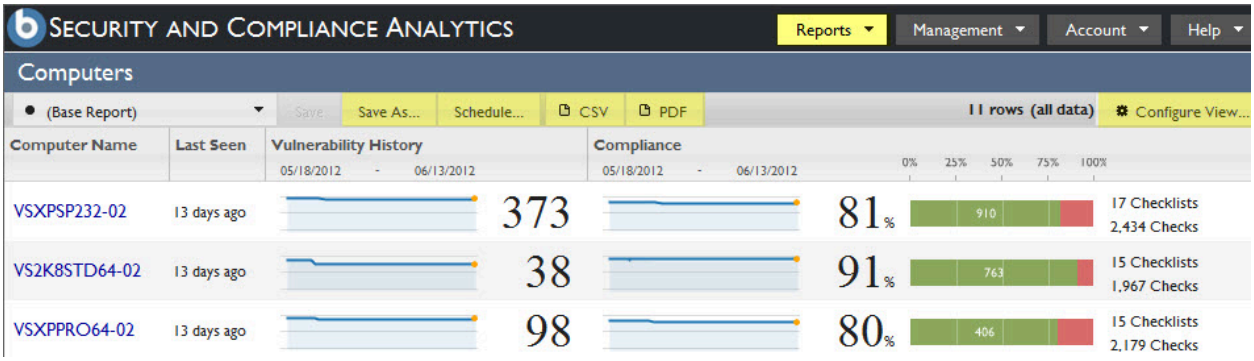
Check Overview Report

To access the Checks "Overview" Report, click the Reports dropdown menu at the top of the console and select Checks. This report is a drilldown of the Checks "List" report. To access this view, click any check in the list. The Checks Overview report presents a graphic representation of Compliance and Check Results history with an overall compliance percentage shown in the top left corner of the console. Use the links across the top to Save As, Schedule, export to .pdf, and Configure View.



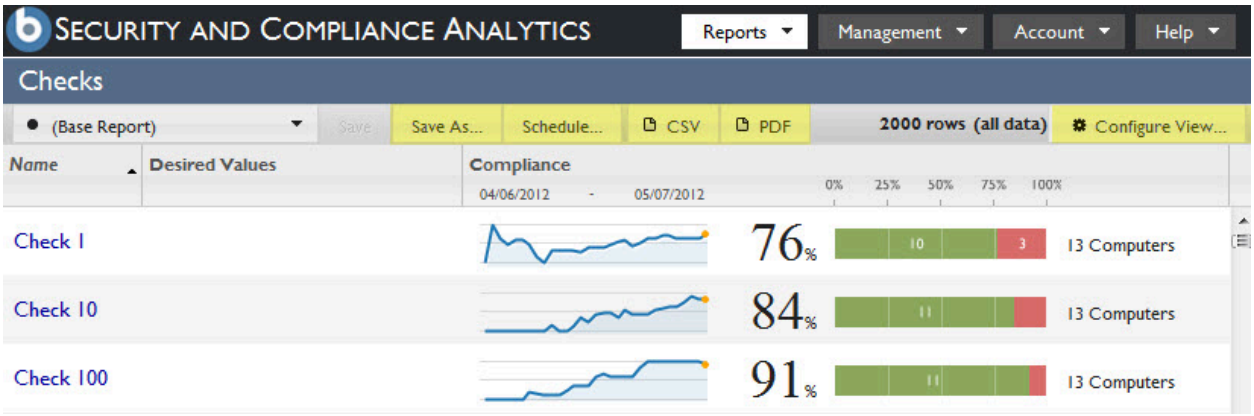
Computers List Report

To access the Computers List Report, click the Reports dropdown menu at the top of the console and select Computers. This report includes fields for computer name, last seen, vulnerability history, and overall compliance. Use the links across the top to Save As, Schedule, export to .csv or .pdf, and Configure View.



Checks List Report

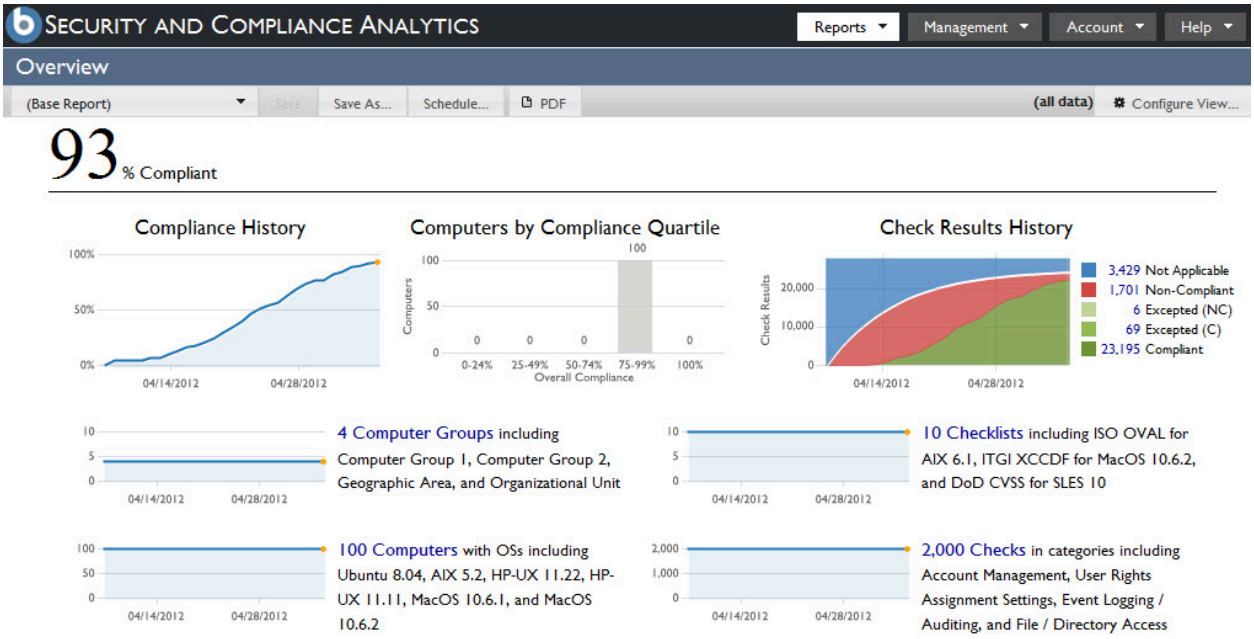
To access the Checks List Report, click the Reports dropdown menu at the top of the console and select Checks. The Checks List report includes fields name, desired values, and compliance. Use the links across the top to Save As, Schedule, export to .csv and .pdf, and Configure View.



Computer Overview Report

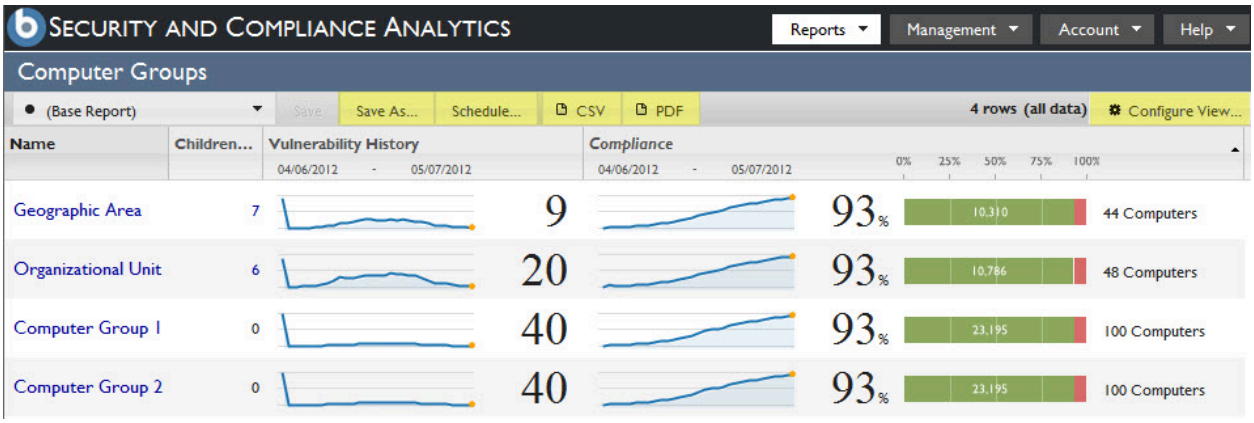
To access the Computer Overview Report, click the Reports dropdown menu at the top of the console and select Overview. This report includes a graphic representation of your

compliance history, check results history, and vulnerability. Use the links across the top to Save As, Schedule, export to .pdf, and Configure View.



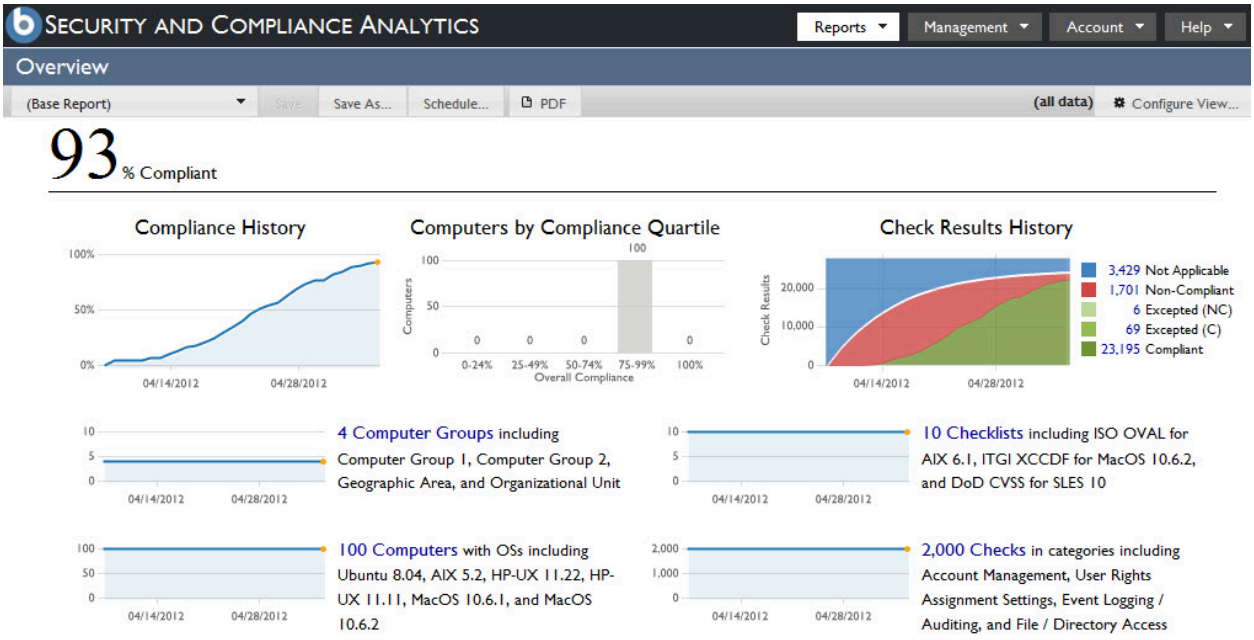
Computer Groups List Report

To access the Computer Groups List Report, click the Reports dropdown menu at the top of the console and select Computer Groups. This report includes fields for name, sub-groups (children), vulnerability history, and compliance in a list format. Use the links across the top to Save As, Schedule, Configure View, or to export the report as .csv or .pdf.



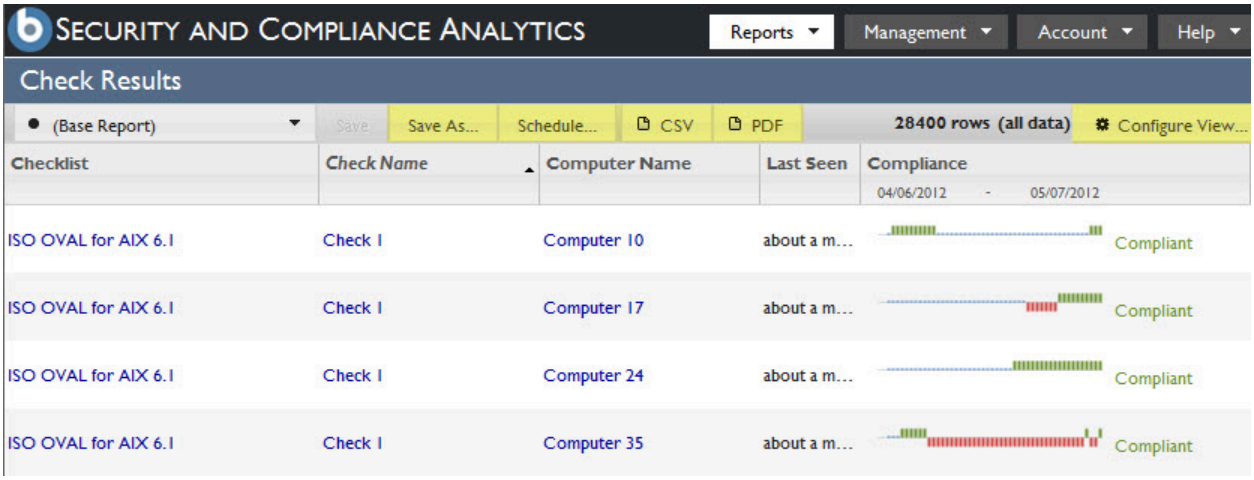
Computer Group Overview Report

To access the Computer Group Overview Report, click the Reports dropdown menu at the top of the console and select Computer Groups. This report is a drilldown of the Computer Groups List Report, and can be accessed by clicking any computer group in the list on the initial screen. This graphic representation of computer groups shows compliance history, computers by compliance quartile, check results history, and vulnerability history. Use the links across the top to Save As, Schedule, export to .pdf, or Configure View.



Check Results List Report

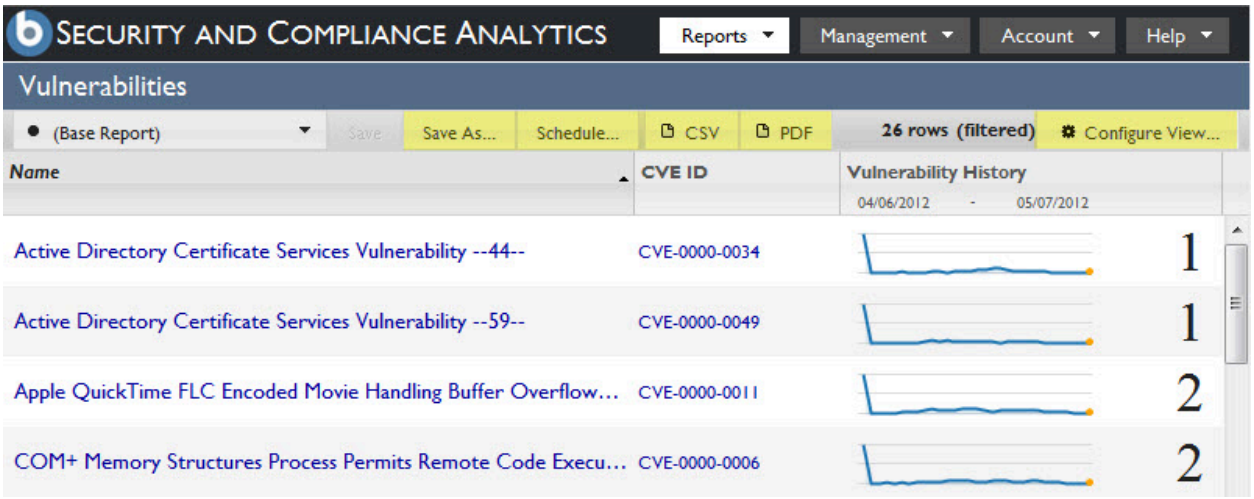
To access the Check Results List Report, click the Reports dropdown menu at the top of the console and select Check Results. This report includes fields for checklist, check name, computer name, the date results were last seen, and level of compliance. Use the links across the top to Save As, Schedule, Configure View, or to export the report as .csv or .pdf.



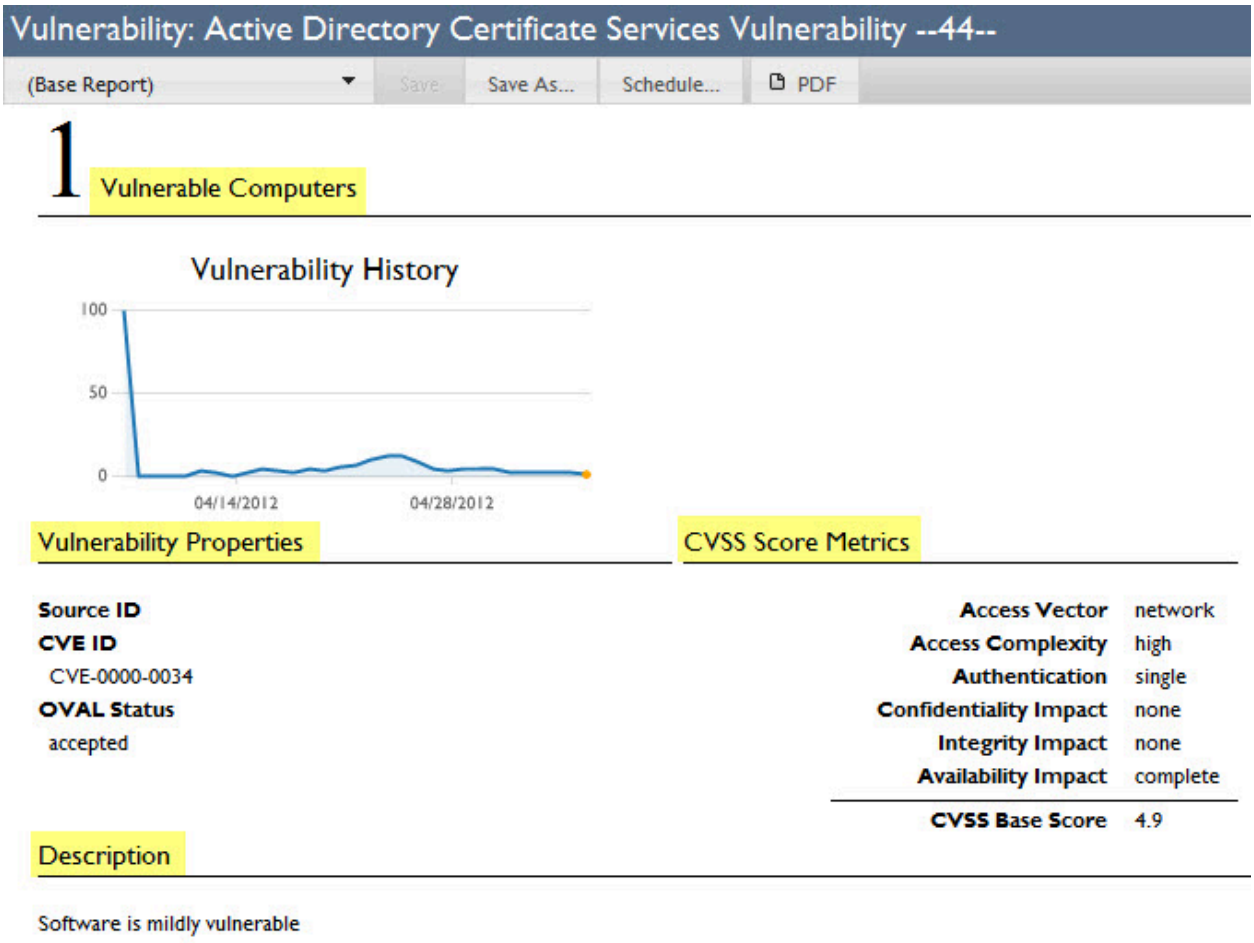
Vulnerabilities Report

To access the Vulnerabilities Report, click the Reports dropdown menu at the top of the console and select either Vulnerabilties or Vulnerability Results. The Vulnerabilities Report organizes data through name, CVE ID and Vulnerability History fields.

By default, the Vulnerabilities list shows vulnerability checks on your deployment to which at least one or more computers are vulnerable. To modify how the vulnerabilities in your deployment presents, click the Configure View button at the top fo the console and use the Filter submenu. Use the links across the top to Save As, Schedule, Configure View, or to export the report as .csv or .pdf.



To access the Vulnerability Overview report, click any name in the Vulnerabilities List report. This report presents a graphic representation of vulnerability history, as well as vulnerability properties, CVSS score metrics, and a description of the vulnerability.



Note: If there is no report about vulnerabilities, the Overview page does not display the Vulnerability Overview.

Appendix B. Example reports - Patch reports

View examples of the various BigFix Compliance Patch reports.

The following table lists examples of reports that you can generate in BigFix Patch Reports. To manage the example reports that follow, see Managing reports *(on page 34)*.

Table 17. Examples of BigFix Compliance Patch reports:

Report name	Location	Field or graph names	Other functions	Export format
Overview *(on page 118)*	From the console, click **Patch > Overview**	Remediations Required, % Remediated, Computers with Most Remediations Required, and Recent Patches	**Save As**, **Schedule**, and **Configure**	`.pdf`
Patches list *(on page 119)*	From the console, click **Patch > Patches**	Name, Severity, Category, Source, Source ID, Days Since Released, Superseded, Relevant Computers, and % Remediated	**Save As**, **Schedule**, and **Configure View**.	`.csv` and `.pdf`
Patch Details *(on page 119)*	From the console, click **Patch > Patches**. Click any	Patch Properties, Related Vulnerabilities, and Description	**Save As**, **Schedule**, and **Configure View**.	`.pdf`

Table 17. Examples of BigFix Compliance Patch reports:

(continued)

Report name	Location	Field or graph names	Other functions	Export format
	displayed patch. Select the sub reports from the top right side of the console by opening the **Overview** menu.			
Computers list *(on page 119)*	From the console, click **Patch > Computers**	Computer Name, Last Seen, Total Patches, Remediations Required and, % Remediated	**Save As**, **Schedule**, and **Configure View**.	`.csv` and `.pdf`
Computers Details	From the console, click **Patch > Computers**. Click a listed computer. Select the sub reports from the top-right side of the console by opening	Computer Properties, Patch Data, Remediations Required and, % Remediated	**Save As**, **Schedule**, and **Configure View**	`.pdf`

Table 17. Examples of BigFix Compliance Patch reports:

(continued)

Report name	Location	Field or graph names	Other functions	Export format
	the **Overview** menu.			
Computer Groups list *(on page 120)*	From the console, click **Patch > Computer Groups**	Name, Computer Count, Remediations Required, and % Remediated	**Save As**, **Schedule**, and **Configure View**.	`.csv` and `.pdf`
Computer Groups Details *(on page 121)*	From the console, click **Patch > Computer Groups**. Click a listed computer group. Select the sub reports from the top-right side of the console by opening the **Overview** menu.	Computer Group Properties, Patch Data, Remediations Required and, % Remediated	**Save As**, **Schedule**, and **Configure View**	`.pdf`

Overview

To access the Overview report, open the **Patch** menu at the top of the console and select **Overview**. The Patches Overview report presents a graphic representation of the required

remediations and the overall remediated computers percentage. It also displays the list of computers that requires the most remediations and a list of recent patches.

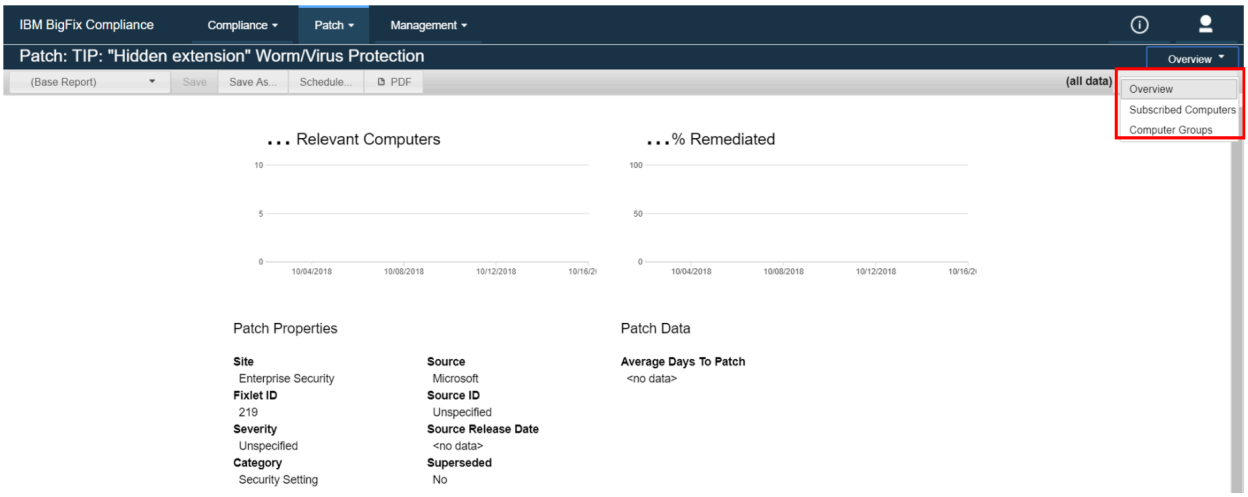
Patches list

To access the Patches List report, open the **Patch** menu at the top of the console and select **Patches**. This report displays complete patch information in a grid format. To view individual patch details, see Patch Details *(on page 119)*.

Patch Details

Patch Details is a sub report of the Patches List

You can access the Patch Details report by clicking a patch in the Patches list. The overview details of the individual patch are displayed, and you can access the sub reports of the individual patch by opening the **Overview** menu at the top right side of the console. The sub reports display the subscribed computers and the computer groups details that are associated with the selected patch.



Computers list

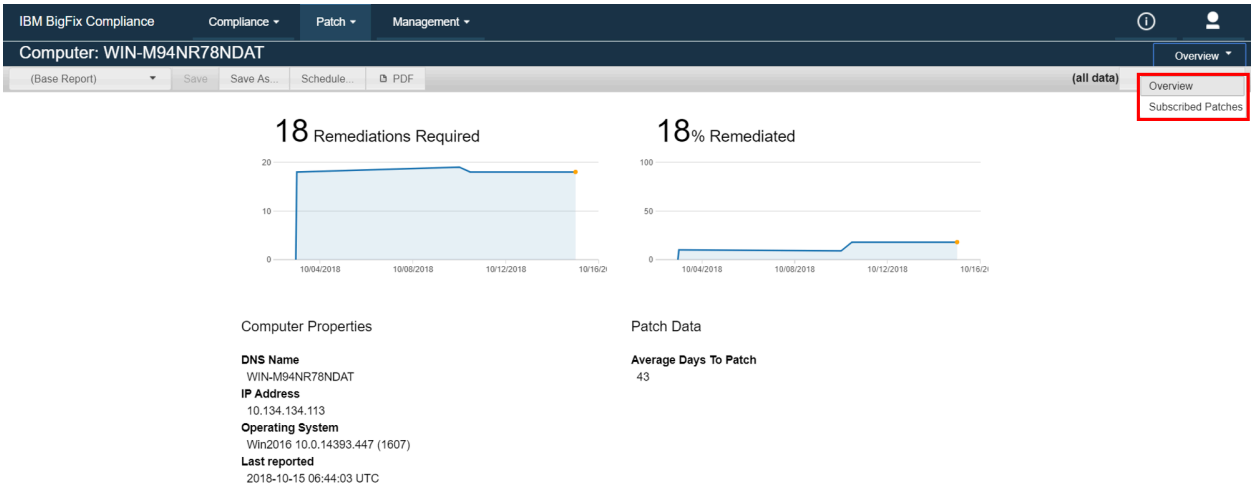
The Computers list report presents patch information about computers.

To access the Computers list report, open the **Patch** menu at the top of the console and select **Computers**. This report includes patch information about individual computers. To view individual computer details, see Computers Details *(on page 120)*.

Computers Details

Computer Details is a sub-report of the **Computers** list.

You can access the report by clicking the computer on the **Computers** list. The overview details of the individual computer are displayed, and you can access the sub-reports of the individual Computer by opening the **Overview** menu at the top right side of the console. The sub reports display the subscribed patches that are associated with the selected computer.



Computer Groups list

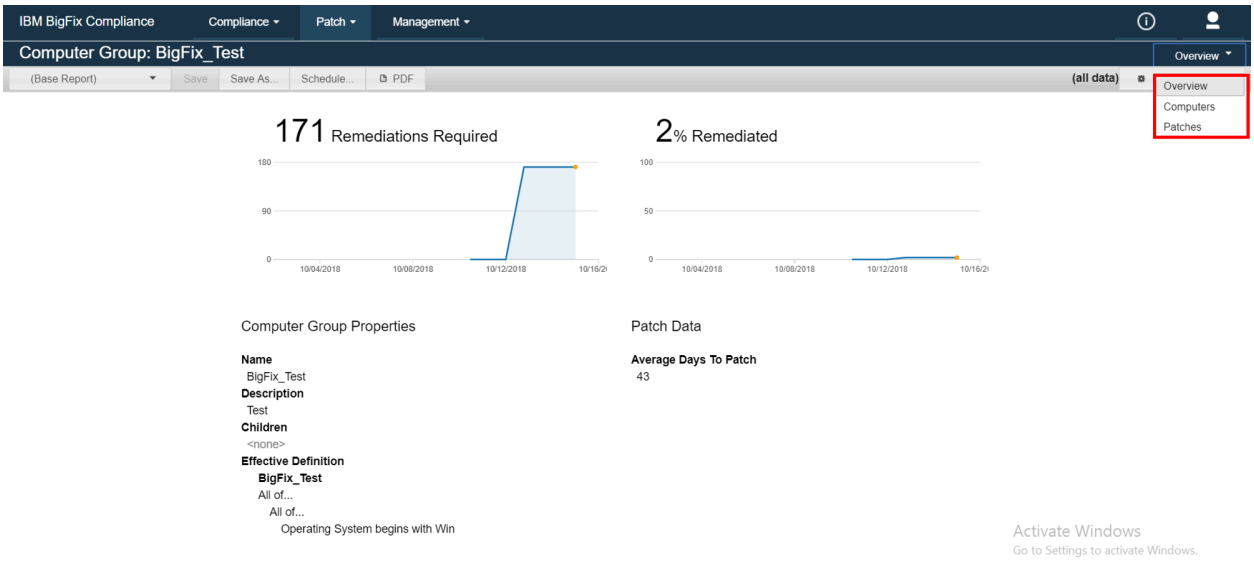
The Computer Groups list report shows the patch details of computers that have been associated as a group.

To access the Computer Groups list report, open the **Patch** menu at the top of the console, and select **Computer Groups**. This report includes the patch details of computer groups. To view the computer group details, see Computer Groups Details *(on page 121)*.

Computer Groups Details

Computer Groups Details is a sub report of the Computer Groups list.

You can access the computer group details by clicking a computer group in the **Computer Groups** list. The overview provides information about the selected computer group, and you can access the sub-reports of the computer group by opening the **Overview** menu at the top right side of the console. The sub reports display the computers and patches that are associated with the selected computer group.



Appendix C. Support

For more information about this product, see the following resources:

- Knowledge Center
- BigFix Support Center
- BigFix Support Portal
- BigFix Developer
- BigFix Wiki
- HCL BigFix Forum

Notices

This information was developed for products and services offered in the US.

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

HCL 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:

HCL
330 Potrero Ave.
Sunnyvale, CA 94085
USA
Attention: Office of the General Counsel

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

HCL
330 Potrero Ave.
Sunnyvale, CA 94085
USA
Attention: Office of the General Counsel

HCL TECHNOLOGIES LTD. 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 jurisdictions 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. HCL 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-HCL websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this HCL product and use of those websites is at your own risk.

HCL may use or distribute any of the information you provide 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:

HCL
330 Potrero Ave.
Sunnyvale, CA 94085
USA
Attention: Office of the General Counsel

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 HCL under terms of the HCL Customer Agreement, HCL International Program License Agreement or any equivalent agreement between us.

The performance data discussed herein is presented as derived under specific operating conditions. Actual results may vary.

Information concerning non-HCL products was obtained from the suppliers of those products, their published announcements or other publicly available sources. HCL has not tested those products and cannot confirm the accuracy of performance, compatibility or

any other claims related to non-HCL products. Questions on the capabilities of non-HCL products should be addressed to the suppliers of those products.

Statements regarding HCL's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to actual people or business enterprises is entirely coincidental.

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 HCL, 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. HCL, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided "AS IS," without warranty of any kind. HCL shall not be liable for any damages arising out of your use of the sample programs.

Each copy or any portion of these sample programs or any derivative work must include a copyright notice as follows:
© (your company name) (year).
Portions of this code are derived from HCL Ltd. Sample Programs.

Trademarks

HCL Technologies Ltd. and HCL Technologies Ltd. logo, and hcl.com are trademarks or registered trademarks of HCL Technologies Ltd., registered in many jurisdictions worldwide.

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 product and service names might be trademarks of HCL or other companies.

Terms and conditions for product documentation

Permissions for the use of these publications are granted subject to the following terms and conditions.

Applicability

These terms and conditions are in addition to any terms of use for the HCL website.

Personal use

You may reproduce these publications for your personal, noncommercial use provided that all proprietary notices are preserved. You may not distribute, display or make derivative work of these publications, or any portion thereof, without the express consent of HCL.

Commercial use

You may reproduce, distribute and display these publications solely within your enterprise provided that all proprietary notices are preserved. You may not make derivative works of these publications, or reproduce, distribute or display these publications or any portion thereof outside your enterprise, without the express consent of HCL.

Rights

Except as expressly granted in this permission, no other permissions, licenses or rights are granted, either express or implied, to the publications or any information, data, software or other intellectual property contained therein.

HCL reserves the right to withdraw the permissions granted herein whenever, in its discretion, the use of the publications is detrimental to its interest or, as determined by HCL, the above instructions are not being properly followed.

You may not download, export or re-export this information except in full compliance with all applicable laws and regulations, including all United States export laws and regulations.

HCL MAKES NO GUARANTEE ABOUT THE CONTENT OF THESE PUBLICATIONS. THE PUBLICATIONS ARE PROVIDED "AS-IS" AND WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE.