BigFix Compliance

Analytics User Guide

Special notice

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

Edition notice

This edition applies to BigFix version 11 and to all subsequent releases and modifications until otherwise indicated in new editions.

Contents

Chapter 1. Introduction

BigFix Compliance Analytics is a component of BigFix Compliance, that includes technical controls and tools that are based on industry practices and standards for endpoint and server security configuration.

The compliance statuses of all endpoints against deployed policies are continually collected, aggregated, and reported using a powerful Compliance Analytics engine, database and user interface in BigFix Compliance. Various compliance reports, showing both current status and historical trend for the entire deployment or individual endpoint, provide comprehensive analytics to meet the various needs of security, IT operation, or compliance teams. With BigFix Compliance Analytics, you can track the effectiveness of the compliance efforts and quickly identify security exposures and risks.

BigFix Compliance Analytics provides consistent report across three security domains:

- Security Configuration Reporting *(on page 53)*
- Patch Reporting *(on page 67)*
- Vulnerability Reporting *(on page 79)*

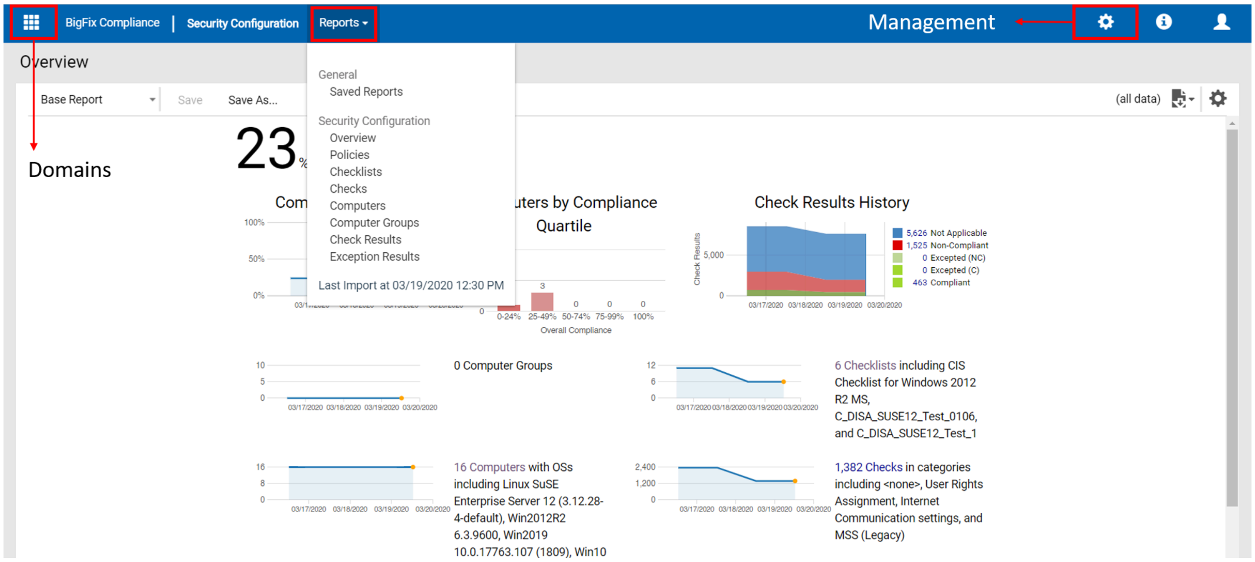
Chapter 2. General Usage Concepts

Primary Menus

This topic gives you an overview of the primary menus in BigFix Compliance Analytics.

Domains: By clicking **Domains** icon on the header you can switch between the **Security Configuration**, **Patch** and **Vulnerability** domains.

Reports: After you select a domain, the **Reports** dropdown lists out domain specific reports. For example, In the below screenshot, the **Security Configuration** domain is selected using **Domains**, under the **Reports** dropdown, General reports, and the reports related to only **Security Configuration** domain is listed.



0 Computer Groups

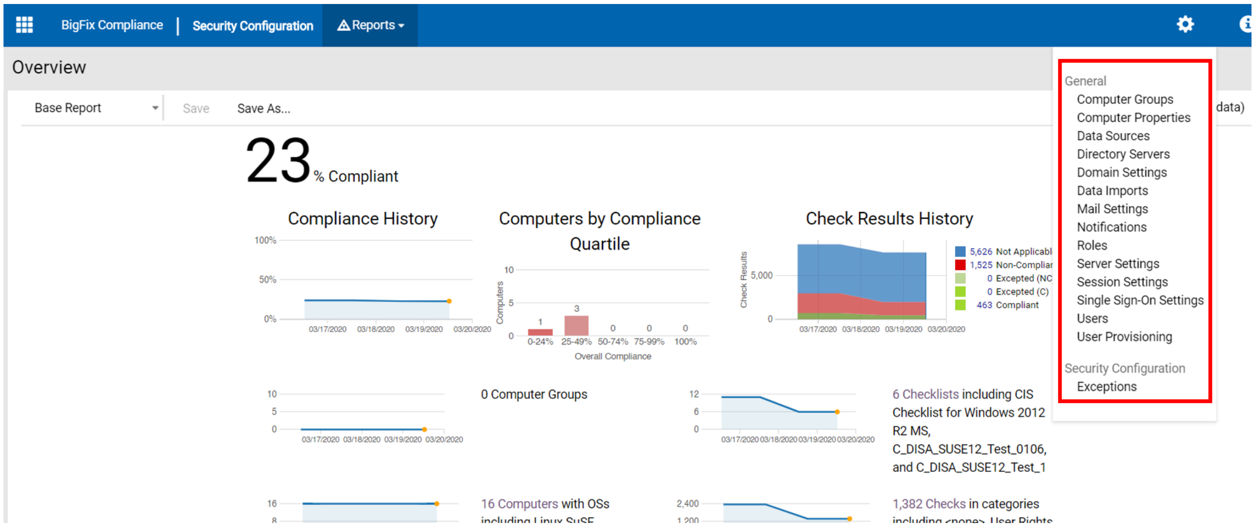
6 Checklists including CIS Checklist for Windows 2012 R2 MS, C_DISA_SUSE12_Test_0106, and C_DISA_SUSE12_Test_1

16 Computers with OSs including Linux SuSE Enterprise Server 12 (3.12.28-4-default), Win2012R2 6.3.9600, Win2019 10.0.17763.107 (1809), Win10

1,382 Checks in categories including <none>, User Rights Assignment, Internet Communication settings, and MSS (Legacy)

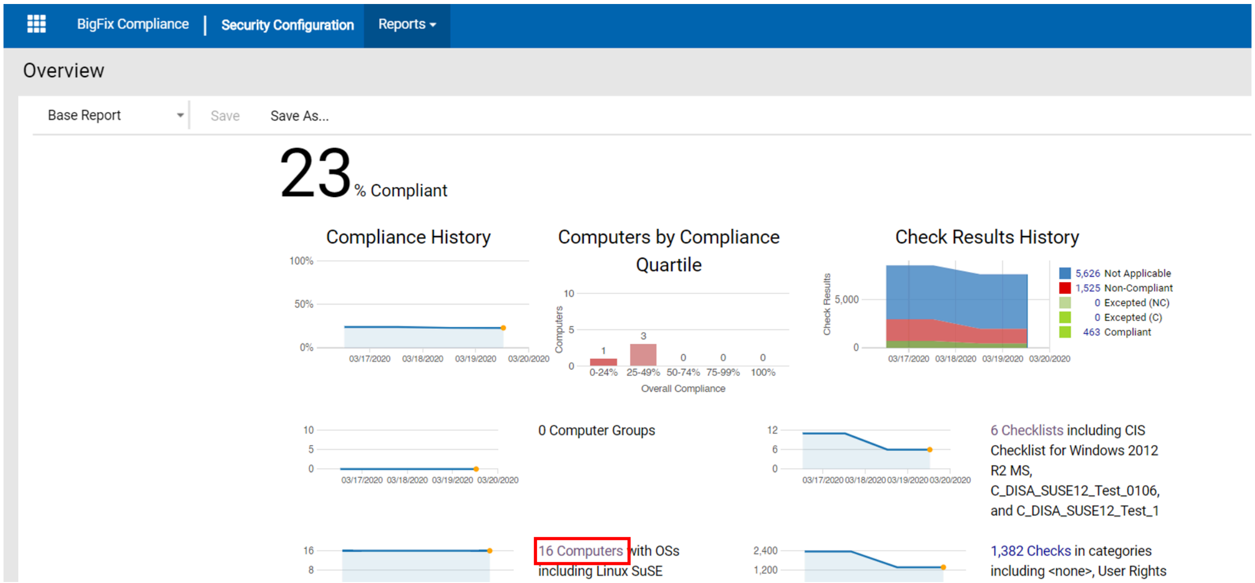
Management Gear Icon: You can perform management tasks within BigFix Compliance Analytics to control various aspects of compliance deployment. From the **Management Gear Icon** dropdown list, users with appropriate permissions can manage general tasks like Computer Groups, Computer Properties, Data Sources, and domain specific management like Exceptions.

Note: Users with appropriate permissions can manage these common management tasks and domain specific tasks to control compliance deployment.



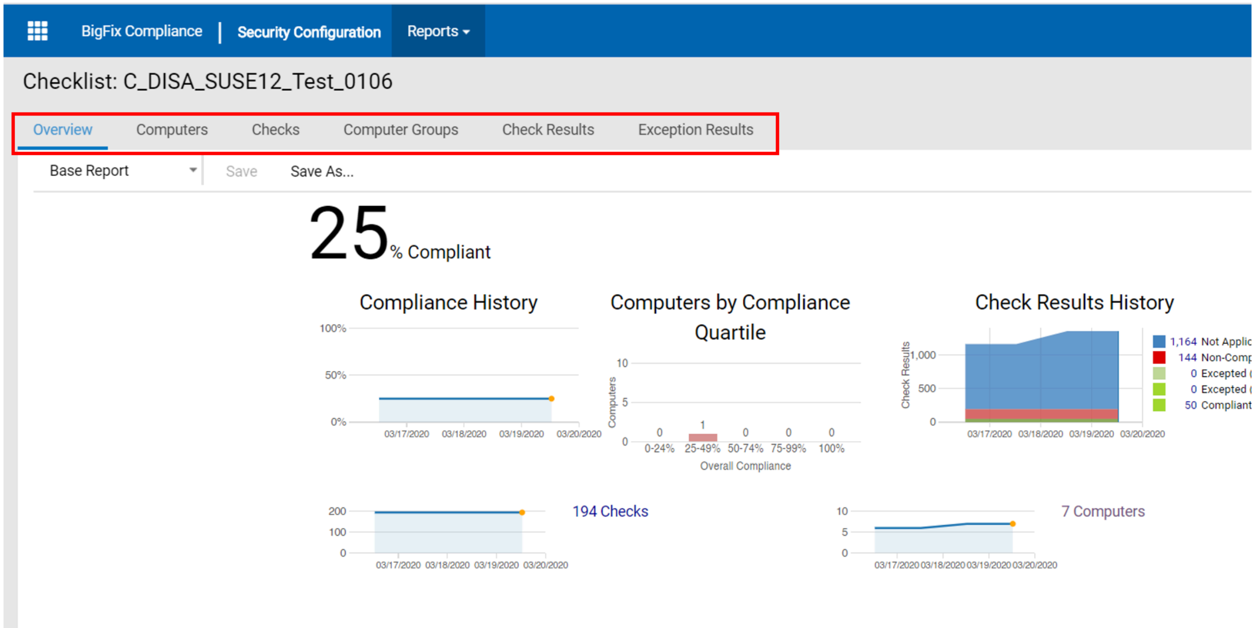
Linked Navigation

You can use linked text to navigate through report types. For example, click *16 Computers* on the Overview report to display the related Computers report.



Sub-Report Navigation

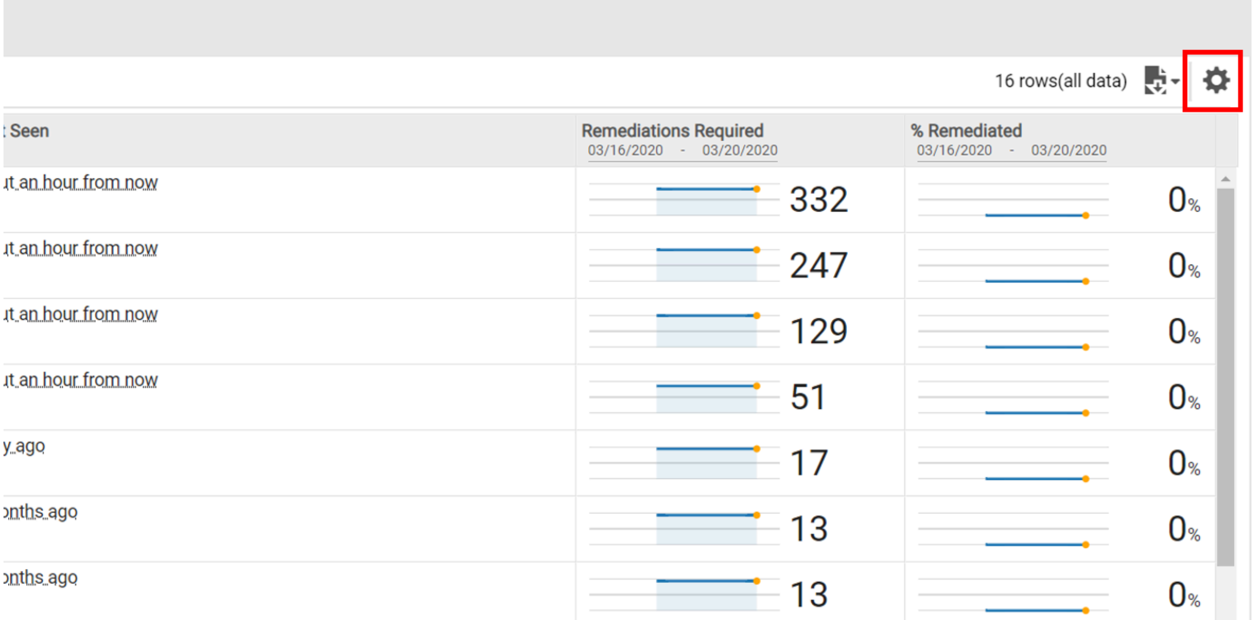
You can also explore reports within a given scope from the sub-report navigation menu. To view all checks, all computers, or all exceptions appropriate for a given checklist, click each tab to view the results.



Customizing Grid Views

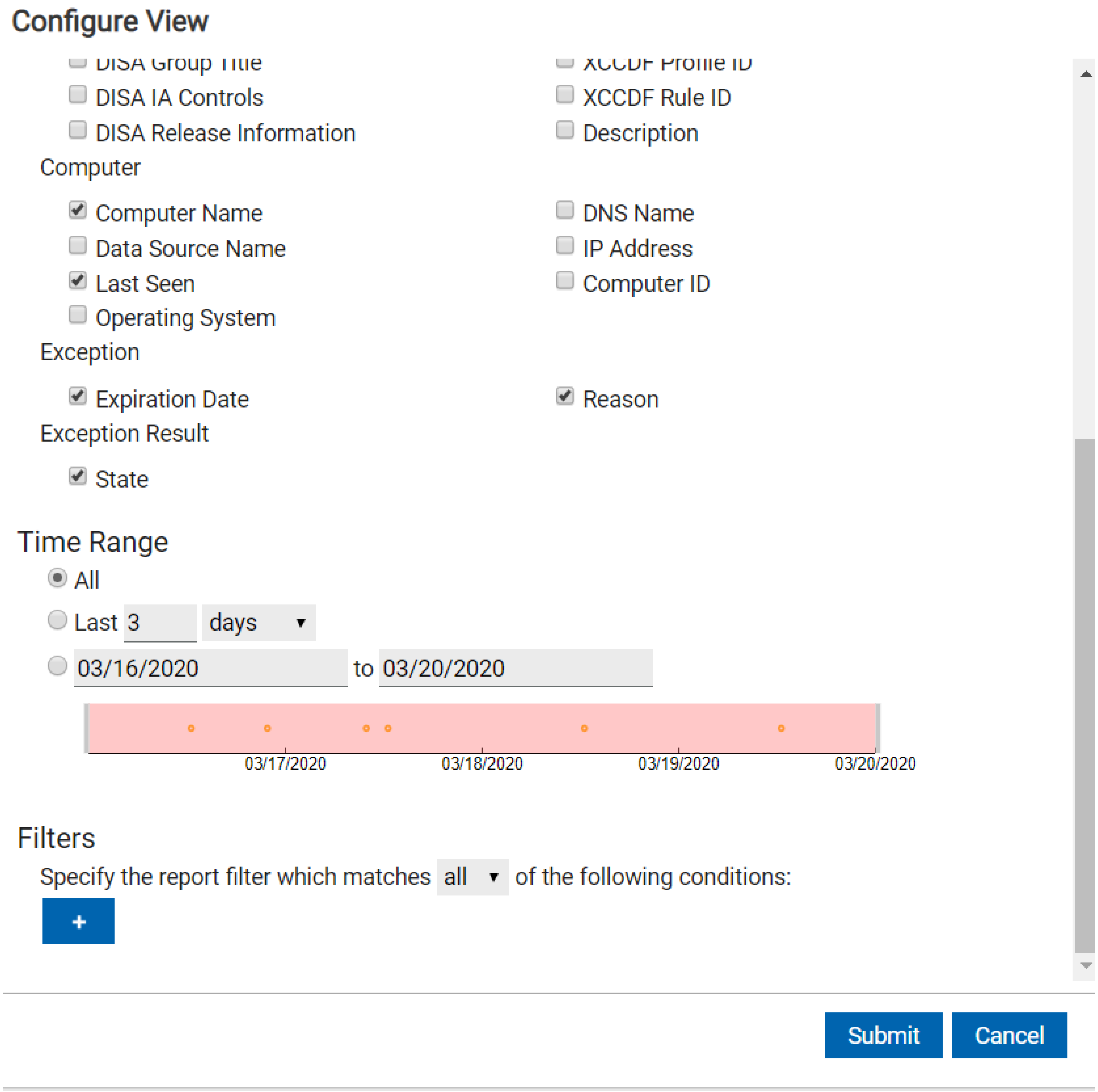
This task helps you to customize the grid views.

To customize the grid views of each report, such as deleting the columns from the grid view or adding additional columns, click **Configure View Gear Icon** to create custom grid views.


16 rows(all data)

: Seen	Remediations Required 03/16/2020 - 03/20/2020	% Remediated 03/16/2020 - 03/20/2020
ıt an hour from now	332	0%
ıt an hour from now	247	0%
ıt an hour from now	129	0%
ıt an hour from now	51	0%
y ago	17	0%
onths ago	13	0%
onths ago	13	0%

You can select different checkboxes to configure the grid view.



Configure View

□ DISA Group Title
□ DISA IA Controls
□ DISA Release Information

□ XCCDF Profile ID
□ XCCDF Rule ID
□ Description

Computer

☑ Computer Name
□ Data Source Name
☑ Last Seen
□ Operating System

□ DNS Name
□ IP Address
□ Computer ID

Exception

☑ Expiration Date

☑ Reason

Exception Result

☑ State

Time Range

● All
○ Last 3 days
○ 03/16/2020 to 03/20/2020

Filters

Specify the report filter which matches all of the following conditions:

Procedure

- **Options**: By disabling the Autosize Columns, the report no longer autosizes to the width of the viewport, instead should be manually adjusted to the desired width.
- **Columns**: select the columns from the list to be featured in the report.
- **Time Range**: The timestamps of data to be included in the report. Graphs are adjusted to the new range. In addition, any static data values reflects the end date of the new time range.
- **Filters**: Allows filtering the displayed data based on the criteria specified. For example, setting a filter of “Name contains ‘foo’” causes the grid to only display rows with the substring “foo” in the name.

Saved Reports

This topic gives you the insights on saving the report and viewing the saved reports.

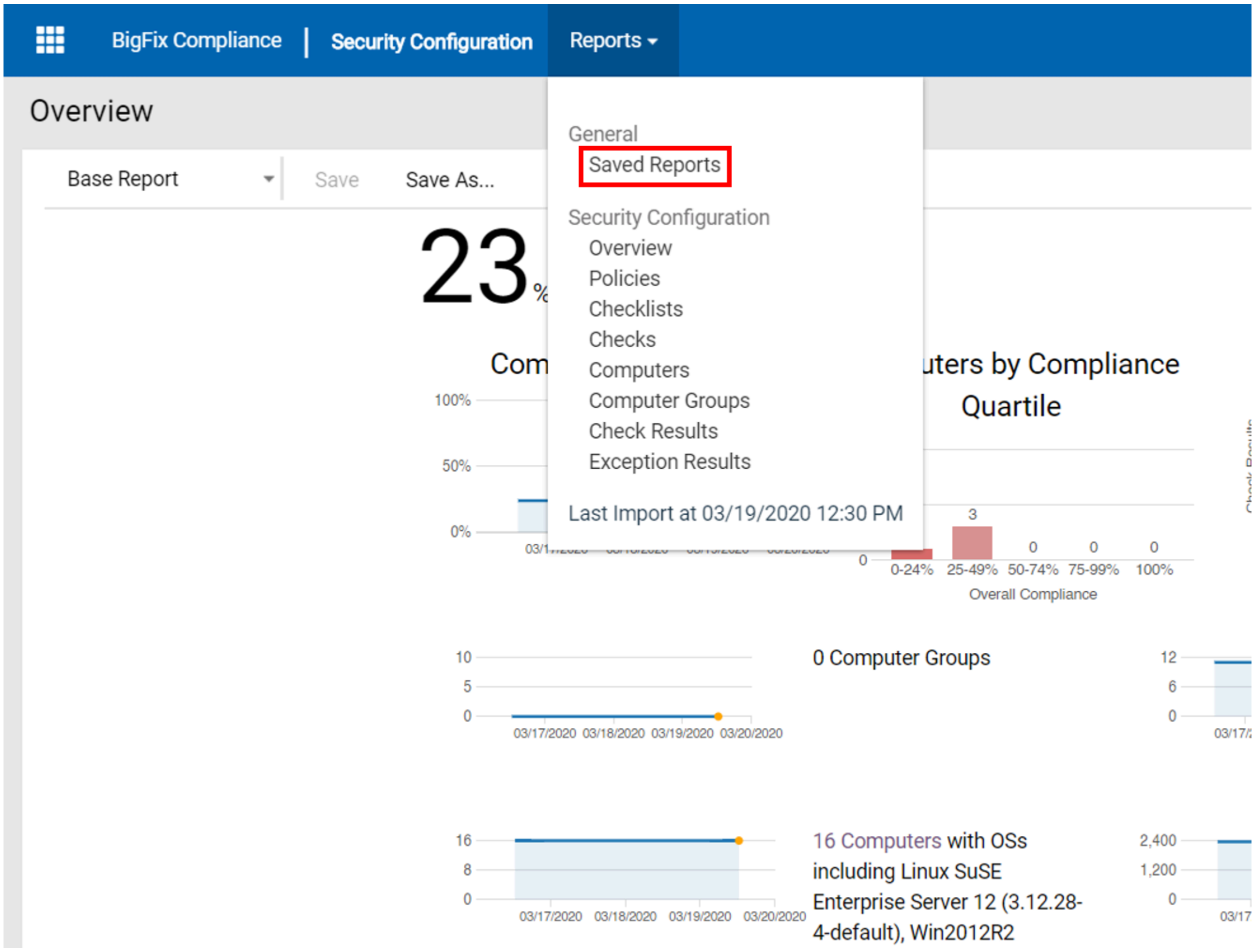
Saving Reports

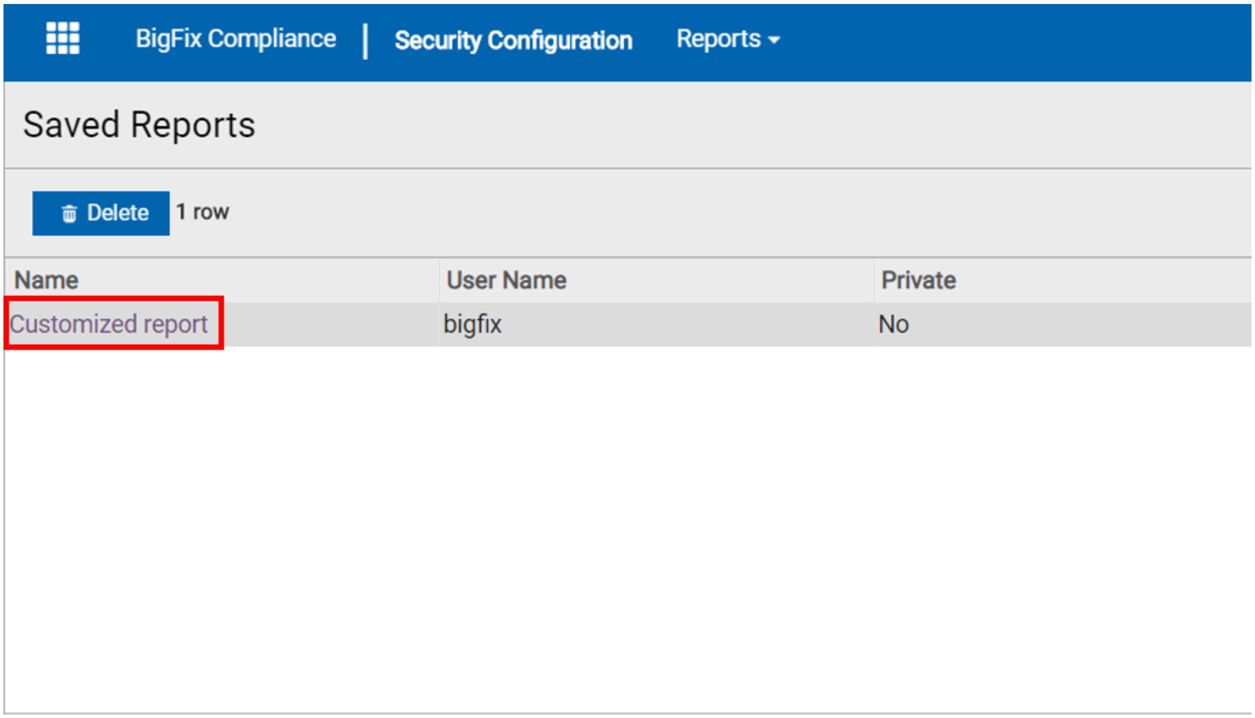
You can save any report view preferences to use it in future. Open any report view that you want to use in future. Click **Save as**, and enter the report name, and click **Create** to save the report view.

To edit the report, see Configuring a report resource as the default view *(on page 13)*.

Viewing Saved Reports

When you save a report view, it will be available as a link in the Saved Reports menu. Selecting a saved report from the menu regenerates the saved customized report. Click **Saved Reports** in the **Reports** menu. Click the report link to regenerate the saved report view.





Saved Reports

1 row

Name	User Name	Private
Customized report	bigfix	No

Configuring a report resource as the default view

This task will guide you to set a default report view.

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

The users can set the default view based on their permission levels:

- Standard users can set the report view to private or default.
- Administrators can set the report view to private, default, or global default.

Private

This option makes the report private, and only the user who saved the report can access the report. Even an administrator will not be able to access the saved report.

Set as default

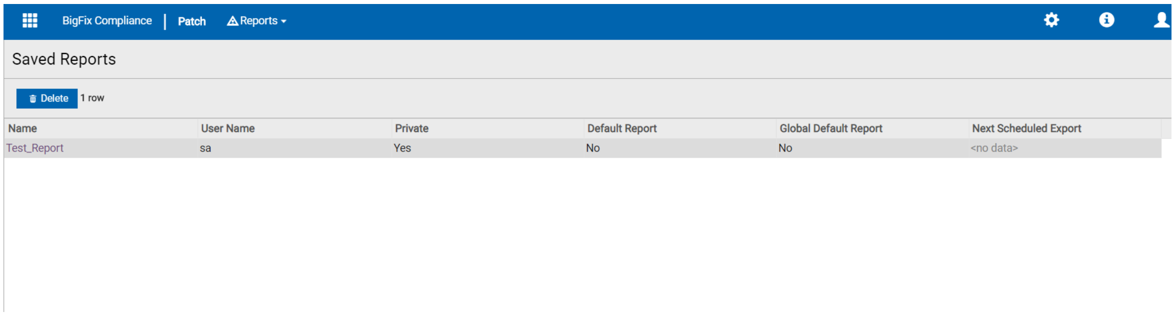
This option saves the report in a default view. Both the user and administrator can view the saved report in a default view.

Set as global default

This option saves the report in the global default view, and all the users will view the report in the saved global default view.

Note: Only administrators can set the report views to global default, but if a standard user already sets the report view to default, the administrator cannot overwrite the settings.

1. Go to **Reports > Saved Reports** and select the report.

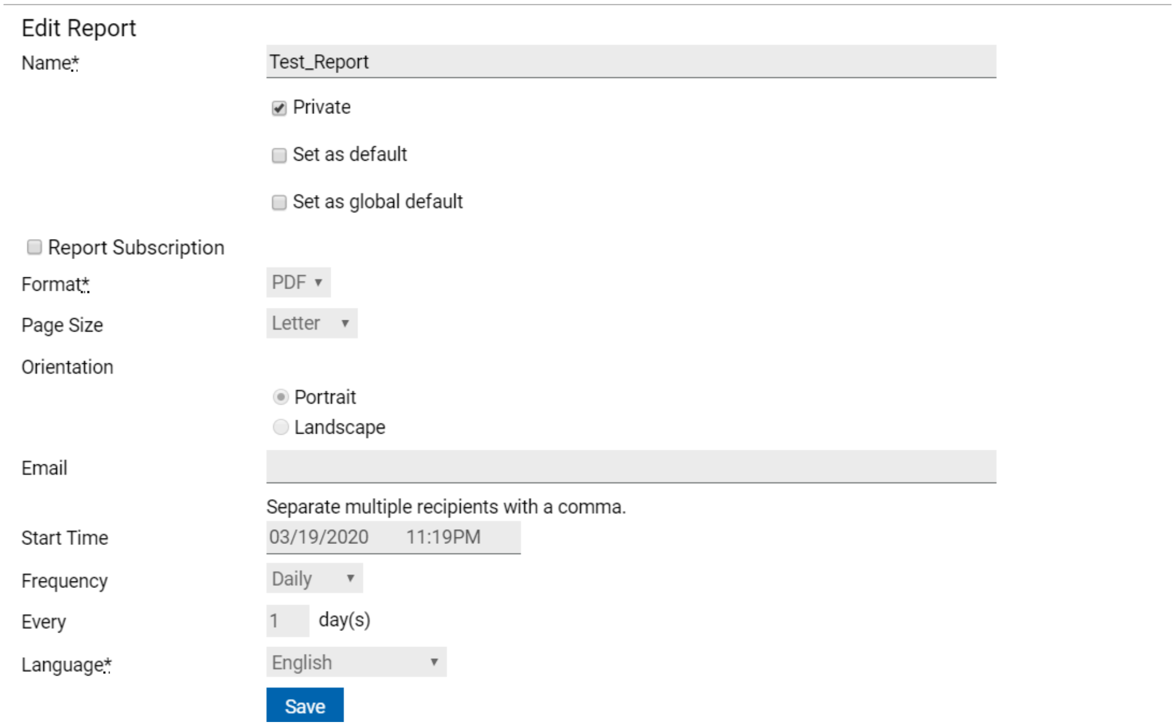


Saved Reports

1 row

Name	User Name	Private	Default Report	Global Default Report	Next Scheduled Export
Test_Report	sa	Yes	No	No	<no data>

2. From the **Edit Report** panel, set the report view.
   - Private
   - Set as default
   - Set as global default



Edit Report

Name*: Test_Report

☑ Private

☐ Set as default

☐ Set as global default

☐ Report Subscription

Format*: PDF

Page Size: Letter

Orientation: ● Portrait ○ Landscape

Email:

Separate multiple recipients with a comma.

Start Time: 03/19/2020 11:19PM

Frequency: Daily

Every: 1 day(s)

Language*: English

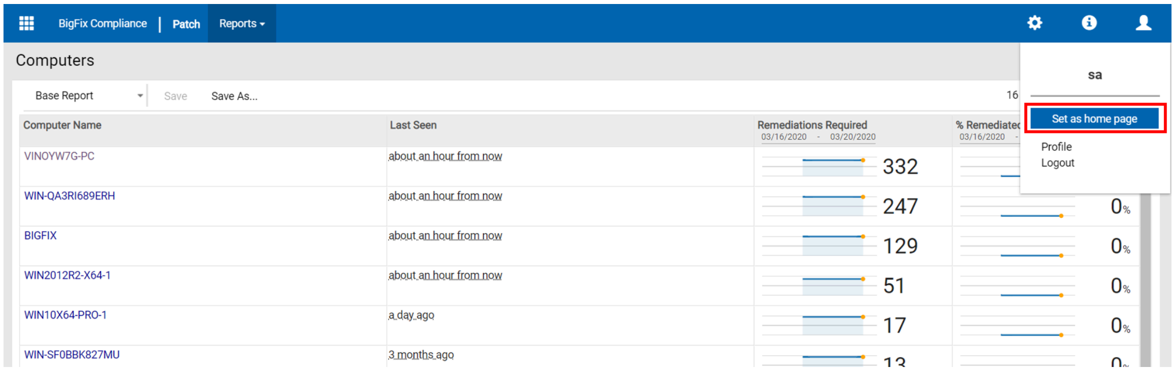
3. Set the report properties.
4. Click **Save**.

Configuring a report resource as the home page

This task helps you to set any page or report, including saved reports, as your 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**.

Note: When a page is currently set as the home page, the option is disabled.



Computers

Computer Name	Last Seen	Remediations Required 03/16/2020 - 03/20/2020	% Remediated 03/16/2020 -
VINOYW7G-PC	about an hour from now	332	
WIN-QA3RI689ERH	about an hour from now	247	0%
BIGFIX	about an hour from now	129	0%
WIN2012R2-X64-1	about an hour from now	51	0%
WIN10X64-PRO-1	a day ago	17	0%
WIN-SF0BBK827MU	3 months ago	13	0%

When you login to BigFix Compliance Analytics application, the report you made as home page will be displayed.

Scheduling

You can use this section to manage the reports.

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, CSV, XLSX`) 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.

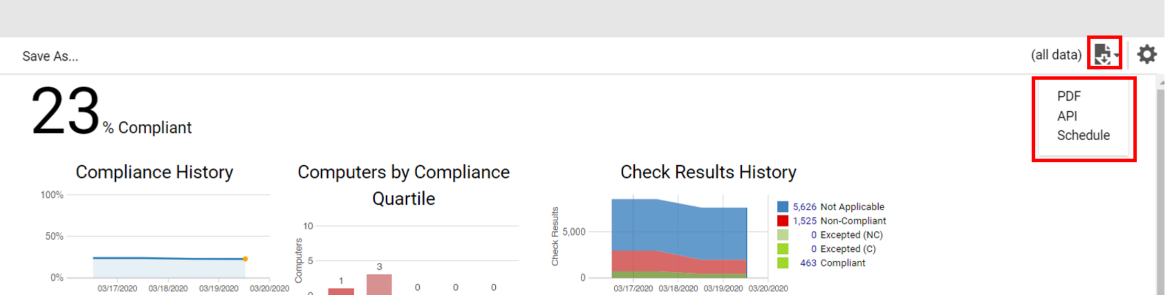
Note: When scheduling PDF or XLSX reports, the number of rows in PDF format is limited to 65,536 and in XLSX format to 30,000 respectively.

Exporting Reports

This task will guide you to export reports in multiple formats.

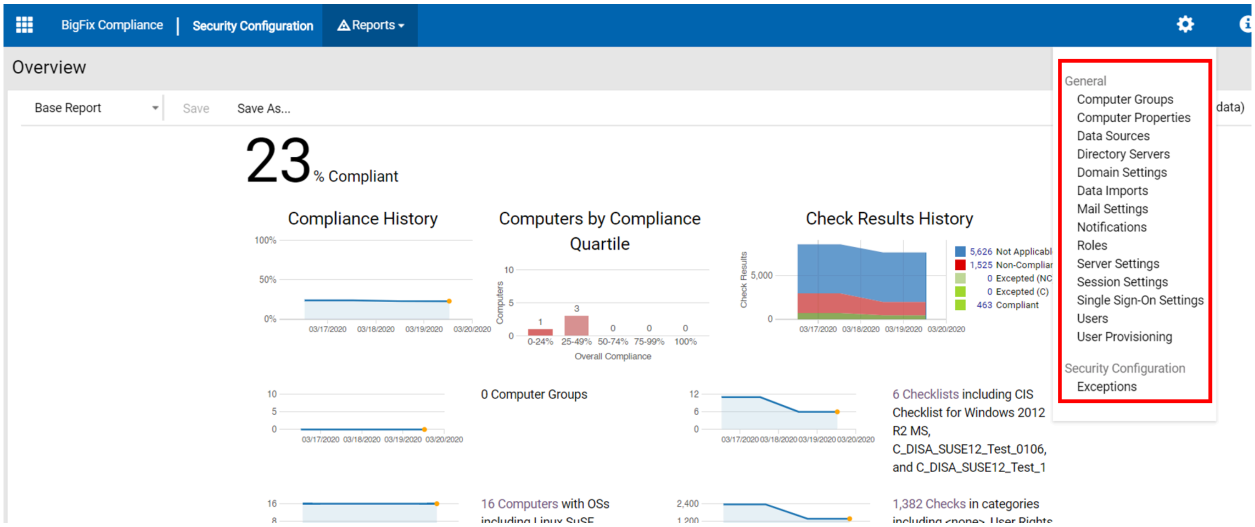
You can export the reports in `.csv` or `.pdf` or `API` file format to your local computer by clicking the **Export Options Icon** and then select **CSV** or **PDF** or **API** link to export the report in a corresponding format.

Note: Some reports cannot be exported in `.csv` format.



Chapter 3. Management Tasks

The following management tasks can be performed if you have appropriate permissions.



- Computer Groups *(on page 17)*
- Computer Properties *(on page 19)*
- Data Sources *(on page 19)*
- Directory Servers *(on page 29)*
- Domain Settings *(on page 20)*
- Data Imports *(on page 22)*
- Mail Settings *(on page 25)*
- Notifications *(on page 26)*
- Roles *(on page 26)*
- Server Settings *(on page 27)*
- Single Sign-On Settings *(on page 32)*
- Session Settings *(on page 31)*
- Users *(on page 50)*
- System Options *(on page 42)*
- User Provisioning *(on page 51)*

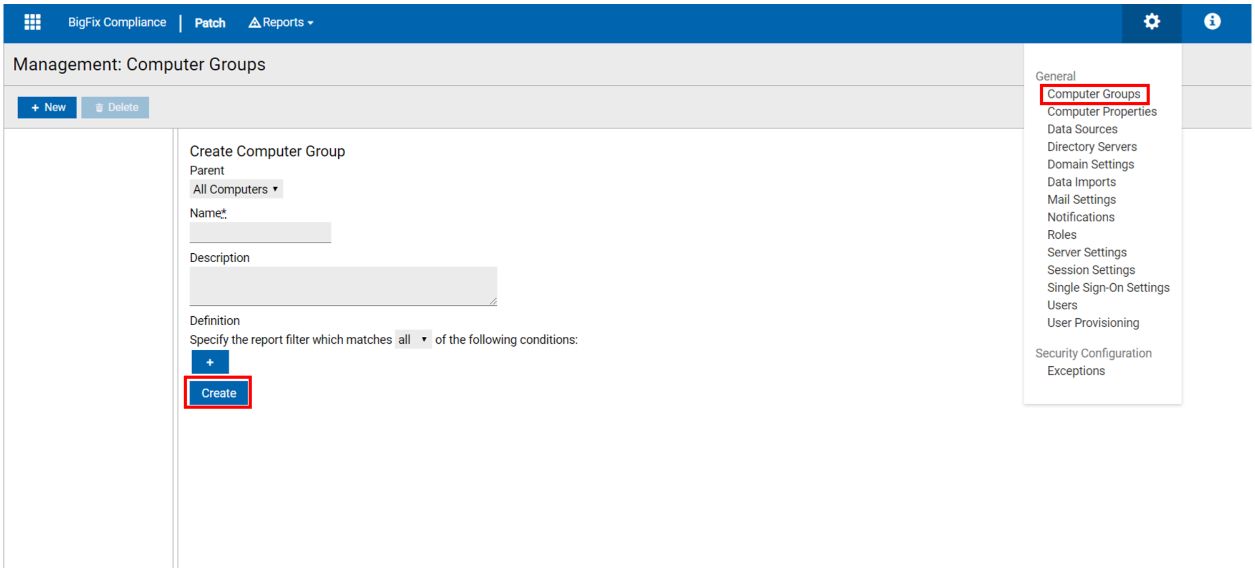
Computer Groups

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 Gear Icon**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. Enter the **Name** and **Description** of the computer group. Use the **Definition** field to assign parameters to your group.

When finished, click *Create*.



Create Computer Group

Parent

All Computers

Name*

Description

Definition

Specify the report filter which matches all of the following conditions:

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

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.

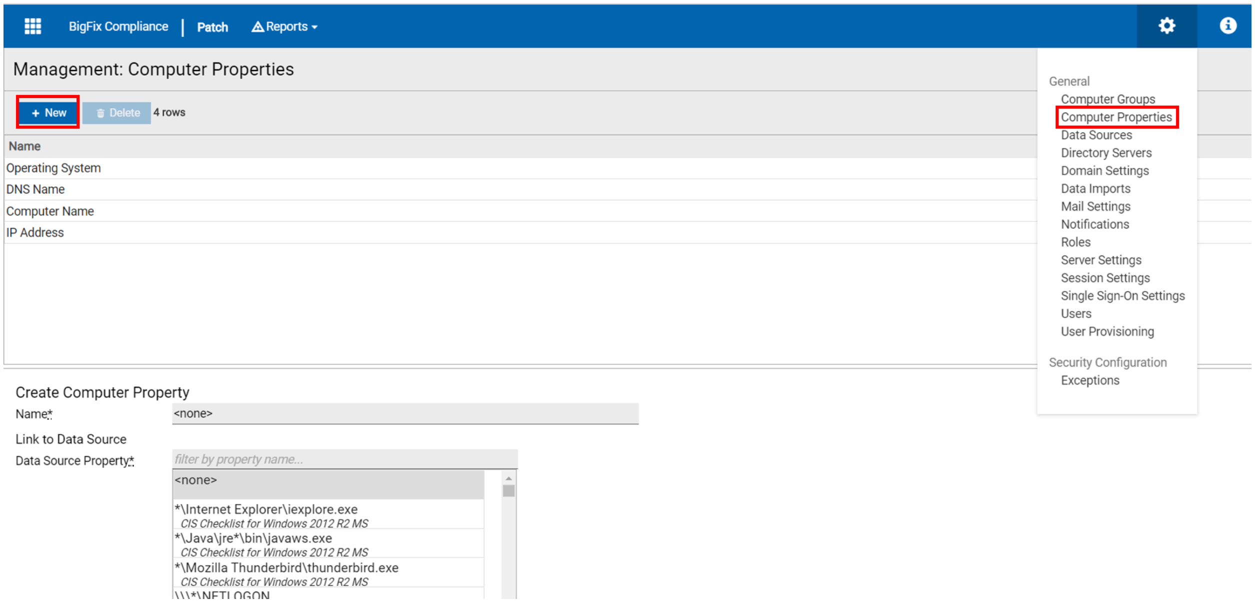
This feature enables non-Administrator users to view ranges for computer group compliance data by granting the user access to multiple computer group during user creation or user account updates.

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 Gear Icon**. 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.

Computer Properties

You can create computer properties using the BigFix data sources available for reporting and filtering within the BigFix Compliance Analytics interface. You can use the default properties in your console, or click **New** to create new properties. These computer properties are later displayed in the report columns.



Management: Computer Properties

Name
Operating System
DNS Name
Computer Name
IP Address

Create Computer Property

Name* <none>

Link to Data Source

Data Source Property* filter by property name...

<none>

*\Internet Explorer\iexplore.exe
CIS Checklist for Windows 2012 R2 MS

\Java\jre\bin\javaws.exe
CIS Checklist for Windows 2012 R2 MS

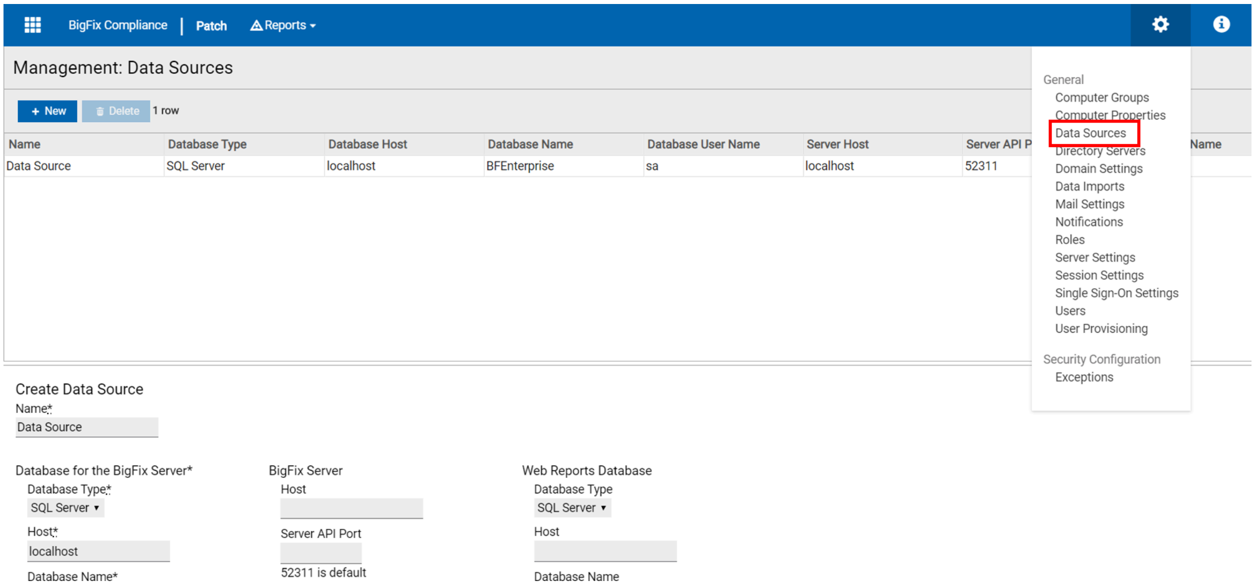
*\Mozilla Thunderbird\thunderbird.exe
CIS Checklist for Windows 2012 R2 MS

\*\NETLOGON

Note: You must perform an import *(on page 22)* after saving your changes.

Data Sources

Using data sources, you can view information about the BigFix Compliance database on which your BigFix Compliance Analytics 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.



Management: Data Sources

Name	Database Type	Database Host	Database Name	Database User Name	Server Host	Server API P	Name
Data Source	SQL Server	localhost	BFEnterprise	sa	localhost	52311	

Create Data Source

Name*: Data Source

Database for the BigFix Server*
Database Type*: SQL Server
Host*: localhost
Database Name*

BigFix Server
Host:
Server API Port:
52311 is default

Web Reports Database
Database Type: SQL Server
Host:
Database Name

Domain Settings

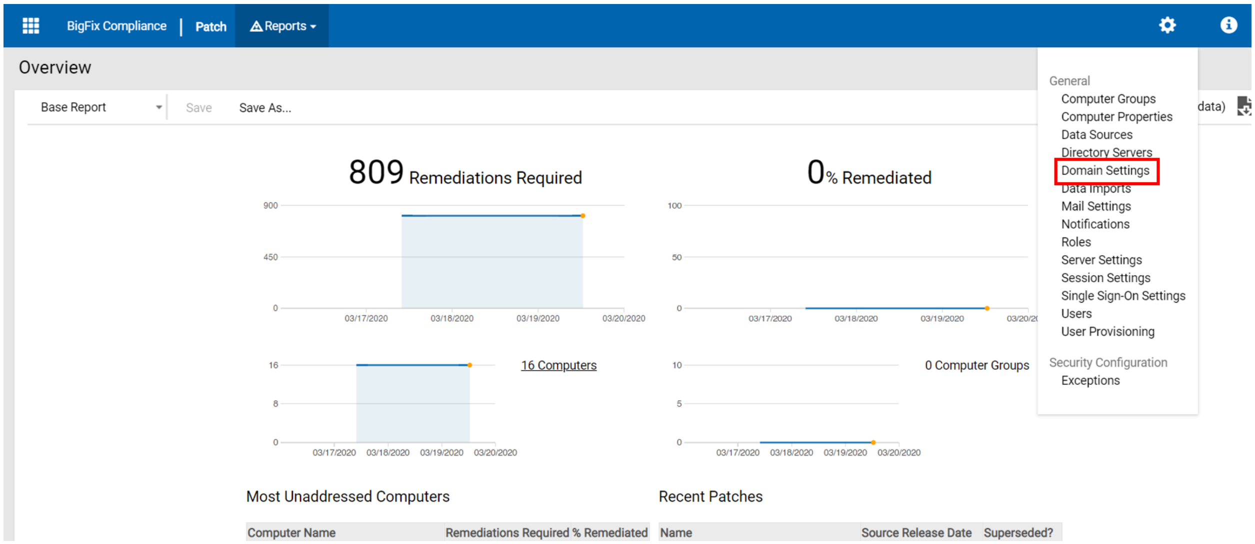
You can enable the patch and vulnerability report, and security configuration report using the **Domain Settings**.

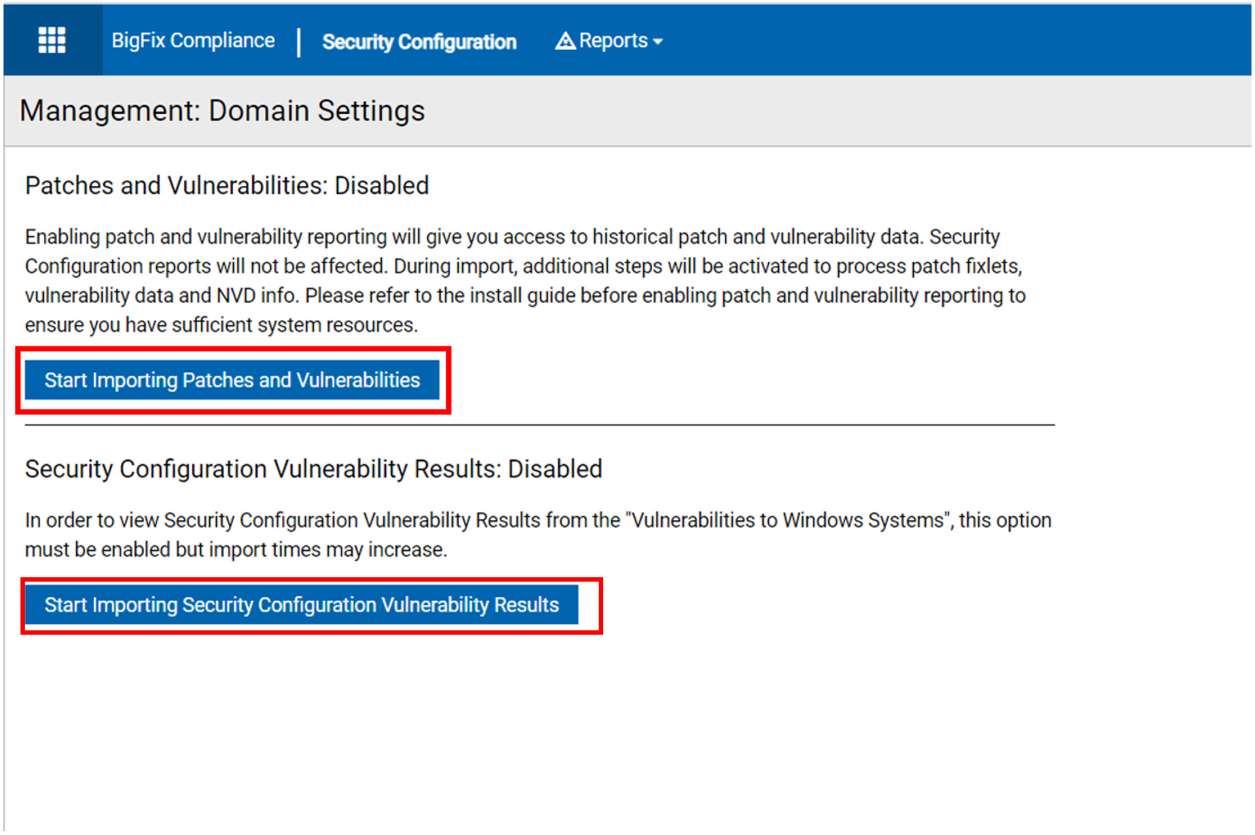
Enabling patch and vulnerability reporting will give you access to historical patch and vulnerability data. Security Configuration reports will not be affected. During import, additional steps will be activated to process patch fixlets, vulnerability data and NVD info.

If must enable Security Configuration Vulnerability Results to view the vulnerabilities to Windows systems.

To enable the Patch and Vulnerability Report, and Security Configuration Vulnerability Results:

1. On the header bar, click **Management Gear Icon**.
2. Select **Domain Settings** from the menu.
3. Under Patches and Vulnerabilities, click **Start Importing Patches and Vulnerabilities**.
4. In the window that opens, click **Yes, include** to enable the patch and vulnerability reporting.
5. Under Security Configuration Vulnerability Results, click **Start Importing Security Configuration Vulnerability Results**.
6. In the window that opens, click **Yes, include** to enable Security Configuration Vulnerability Results.





Management: Domain Settings

Patches and Vulnerabilities: Disabled

Enabling patch and vulnerability reporting will give you access to historical patch and vulnerability data. Security Configuration reports will not be affected. During import, additional steps will be activated to process patch fixlets, vulnerability data and NVD info. Please refer to the install guide before enabling patch and vulnerability reporting to ensure you have sufficient system resources.

Security Configuration Vulnerability Results: Disabled

In order to view Security Configuration Vulnerability Results from the "Vulnerabilities to Windows Systems", this option must be enabled but import times may increase.

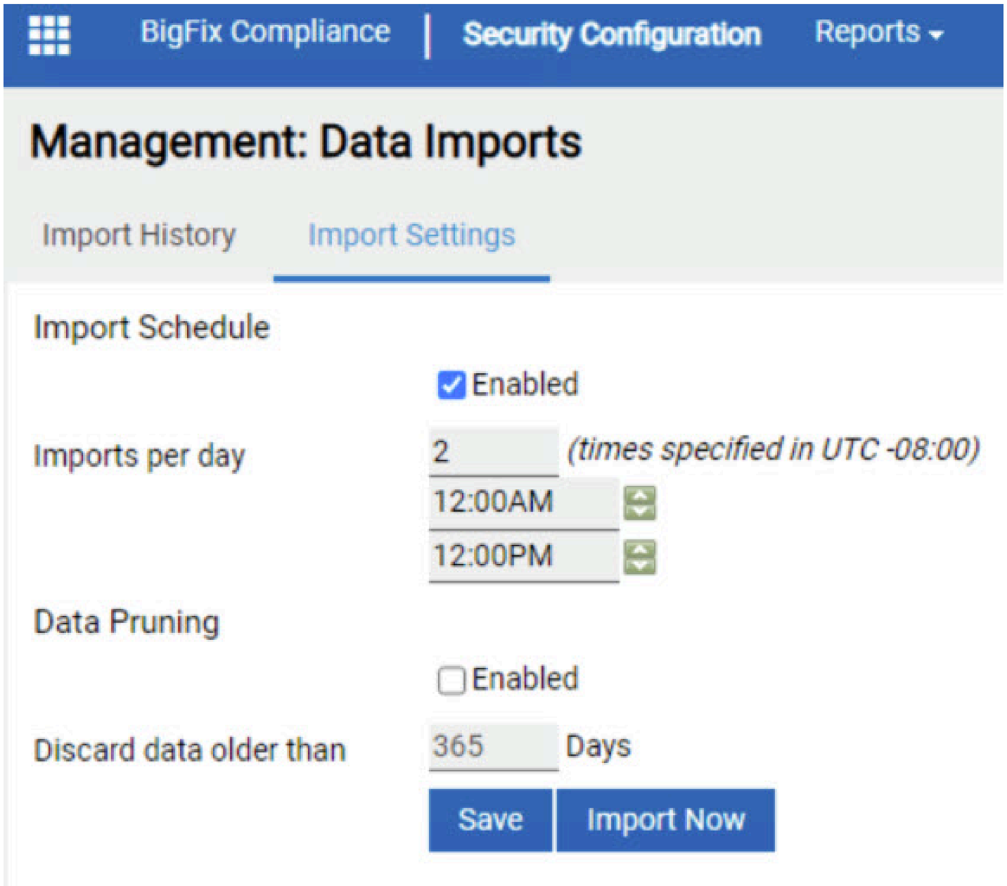
Start Importing Security Configuration Vulnerability Results

Note: Enabling the patch and vulnerability reporting increases the duration of import processes and requires additional resources from the BigFix Compliance database. For information about importing data to the patch and vulnerability reporting application, see Data Imports *(on page 22)*.

Note: Pleaes refer to Primary Menus to switch between the **Security Configuration**, **Patch** and **Vulnerability** domains.

Data Imports

Use the **Import Settings** tab to schedule a recurring import, disable recurring imports, start a manual import, and view current import status.



Management: Data Imports

Import Schedule

☑ Enabled

Imports per day: 2 *(times specified in UTC -08:00)*

12:00AM

12:00PM

Data Pruning

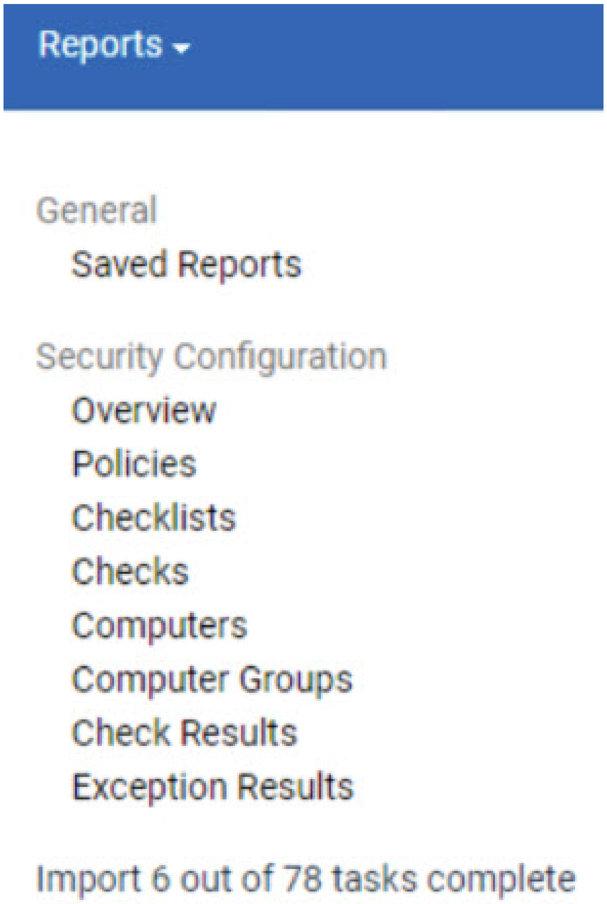
☐ Enabled

Discard data older than: 365 Days

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

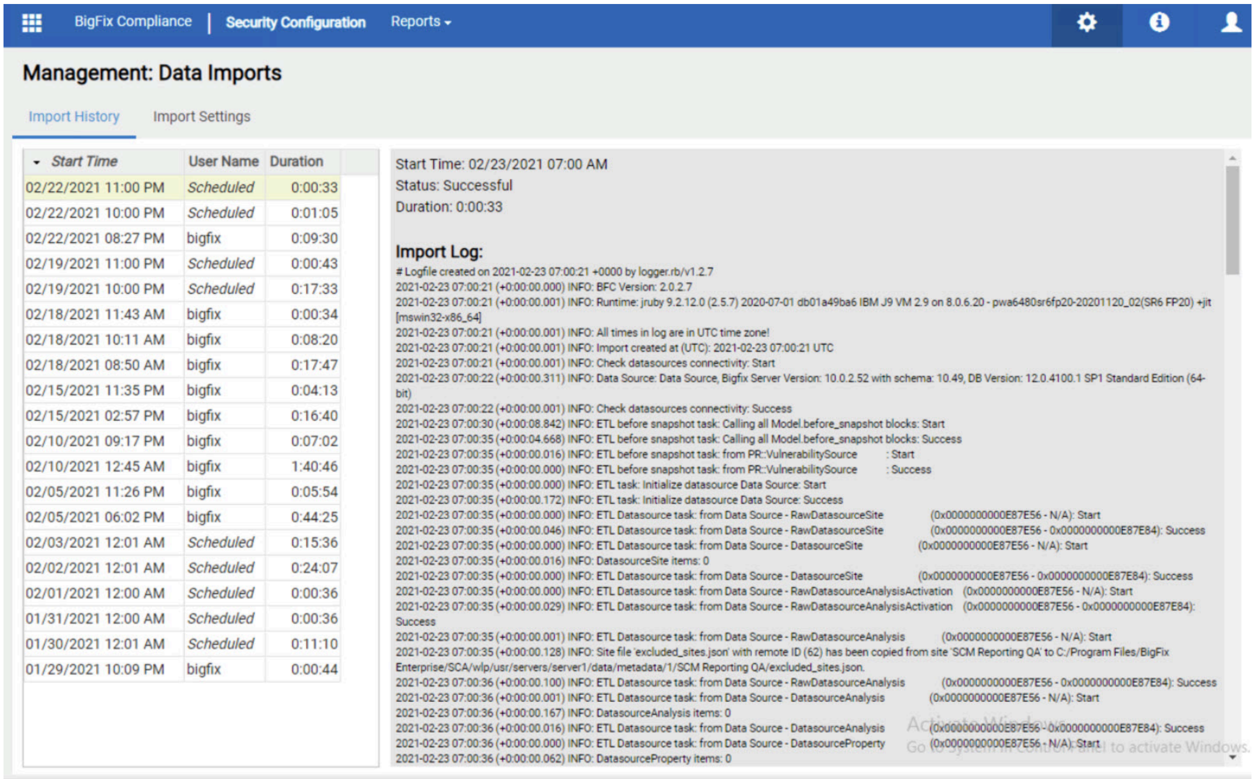
From the Data Imports interface, you can also enable Data Pruning and discard older data. Click **Save** to confirm the change.

Import progress is measured by the number of tasks completed.



Import 6 out of 78 tasks complete

Use the **Import History** tab to view the logs of previous imports.



Management: Data Imports

Import History | Import Settings

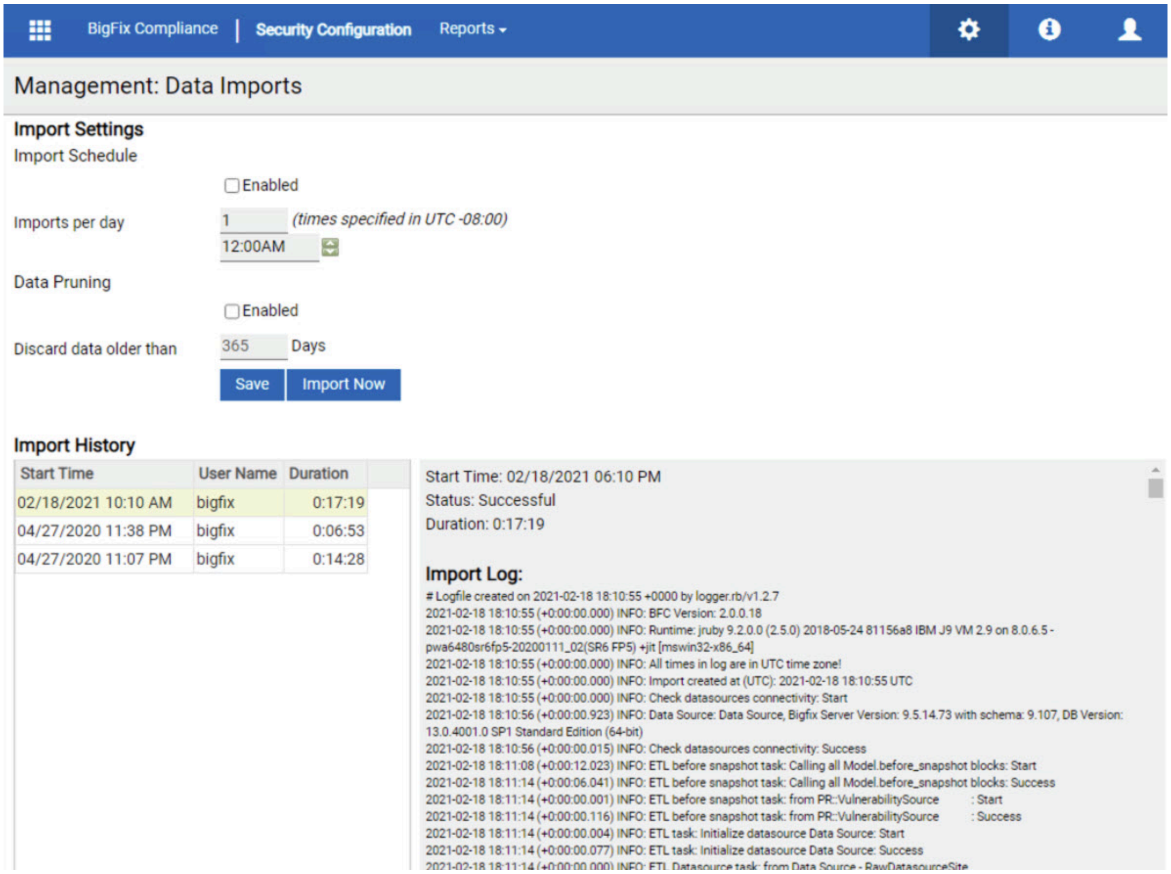
Start Time	User Name	Duration
02/22/2021 11:00 PM	*Scheduled*	0:00:33
02/22/2021 10:00 PM	*Scheduled*	0:01:05
02/22/2021 08:27 PM	bigfix	0:09:30
02/19/2021 11:00 PM	*Scheduled*	0:00:43
02/19/2021 10:00 PM	*Scheduled*	0:17:33
02/18/2021 11:43 AM	bigfix	0:00:34
02/18/2021 10:11 AM	bigfix	0:08:20
02/18/2021 08:50 AM	bigfix	0:17:47
02/15/2021 11:35 PM	bigfix	0:04:13
02/15/2021 02:57 PM	bigfix	0:16:40
02/10/2021 09:17 PM	bigfix	0:07:02
02/10/2021 12:45 AM	bigfix	1:40:46
02/05/2021 11:26 PM	bigfix	0:05:54
02/05/2021 06:02 PM	bigfix	0:44:25
02/03/2021 12:01 AM	*Scheduled*	0:15:36
02/02/2021 12:01 AM	*Scheduled*	0:24:07
02/01/2021 12:00 AM	*Scheduled*	0:00:36
01/31/2021 12:00 AM	*Scheduled*	0:00:36
01/30/2021 12:01 AM	*Scheduled*	0:11:10
01/29/2021 10:09 PM	bigfix	0:00:44

Start Time: 02/23/2021 07:00 AM
Status: Successful
Duration: 0:00:33

Import Log:

```
# Logfile created on 2021-02-23 07:00:21 +0000 by logger.rb/v1.2.7
2021-02-23 07:00:21 (+0:00:00.000) INFO: BFC Version: 2.0.2.7
2021-02-23 07:00:21 (+0:00:00.001) INFO: Runtime: jruby 9.2.12.0 (2.5.7) 2020-07-01 db01a49ba6 IBM J9 VM 2.9 on 8.0.6.20 - pwa6480sr6fp20-20201120_02(SR6 FP20) +jit
[mswin32-x86_64]
2021-02-23 07:00:21 (+0:00:00.001) INFO: All times in log are in UTC time zone!
2021-02-23 07:00:21 (+0:00:00.001) INFO: Import created at (UTC): 2021-02-23 07:00:21 UTC
2021-02-23 07:00:21 (+0:00:00.001) INFO: Check datasources connectivity: Start
2021-02-23 07:00:22 (+0:00:00.311) INFO: Data Source: Data Source, Bigfix Server Version: 10.0.2.52 with schema: 10.49, DB Version: 12.0.4100.1 SP1 Standard Edition (64-
bit)
2021-02-23 07:00:22 (+0:00:00.001) INFO: Check datasources connectivity: Success
2021-02-23 07:00:30 (+0:00:08.842) INFO: ETL before snapshot task: Calling all Model.before_snapshot blocks: Start
2021-02-23 07:00:35 (+0:00:04.668) INFO: ETL before snapshot task: Calling all Model.before_snapshot blocks: Success
2021-02-23 07:00:35 (+0:00:00.016) INFO: ETL before snapshot task: from PR::VulnerabilitySource        : Start
2021-02-23 07:00:35 (+0:00:00.000) INFO: ETL before snapshot task: from PR::VulnerabilitySource        : Success
2021-02-23 07:00:35 (+0:00:00.000) INFO: ETL task: Initialize datasource Data Source: Start
2021-02-23 07:00:35 (+0:00:00.172) INFO: ETL task: Initialize datasource Data Source: Success
2021-02-23 07:00:35 (+0:00:00.000) INFO: ETL Datasource task: from Data Source - RawDatasourceSite           (0x0000000000E87E56 - N/A): Start
2021-02-23 07:00:35 (+0:00:00.046) INFO: ETL Datasource task: from Data Source - RawDatasourceSite           (0x0000000000E87E56 - 0x0000000000E87E84): Success
2021-02-23 07:00:35 (+0:00:00.000) INFO: ETL Datasource task: from Data Source - DatasourceSite           (0x0000000000E87E56 - N/A): Start
2021-02-23 07:00:35 (+0:00:00.016) INFO: DatasourceSite items: 0
2021-02-23 07:00:35 (+0:00:00.000) INFO: ETL Datasource task: from Data Source - DatasourceSite           (0x0000000000E87E56 - 0x0000000000E87E84): Success
2021-02-23 07:00:35 (+0:00:00.000) INFO: ETL Datasource task: from Data Source - RawDatasourceAnalysisActivation   (0x0000000000E87E56 - N/A): Start
2021-02-23 07:00:35 (+0:00:00.029) INFO: ETL Datasource task: from Data Source - RawDatasourceAnalysisActivation   (0x0000000000E87E56 - 0x0000000000E87E84):
Success
2021-02-23 07:00:35 (+0:00:00.001) INFO: ETL Datasource task: from Data Source - RawDatasourceAnalysis         (0x0000000000E87E56 - N/A): Start
2021-02-23 07:00:35 (+0:00:00.128) INFO: Site file 'excluded_sites.json' with remote ID (62) has been copied from site 'SCM Reporting QA' to C:/Program Files/BigFix
Enterprise/SCA/wlp/usr/servers/server1/data/metadata/1/SCM Reporting QA/excluded_sites.json.
2021-02-23 07:00:36 (+0:00:00.100) INFO: ETL Datasource task: from Data Source - RawDatasourceAnalysis         (0x0000000000E87E56 - 0x0000000000E87E84): Success
2021-02-23 07:00:36 (+0:00:00.001) INFO: ETL Datasource task: from Data Source - DatasourceAnalysis          (0x0000000000E87E56 - N/A): Start
2021-02-23 07:00:36 (+0:00:00.167) INFO: DatasourceAnalysis items: 0
2021-02-23 07:00:36 (+0:00:00.016) INFO: ETL Datasource task: from Data Source - DatasourceAnalysis          (0x0000000000E87E56 - 0x0000000000E87E84): Success
2021-02-23 07:00:36 (+0:00:00.000) INFO: ETL Datasource task: from Data Source - DatasourceProperty          (0x0000000000E87E56 - N/A): Start
2021-02-23 07:00:36 (+0:00:00.062) INFO: DatasourceProperty items: 0
```

Note: For SCA 2.0.1.36 and prior, Import Settings and Import History are viewed within the same page.



Management: Data Imports

Import Settings

Import Schedule

☐ Enabled

Imports per day: 1 *(times specified in UTC -08:00)*

12:00AM

Data Pruning

☐ Enabled

Discard data older than: 365 Days

Import History

Start Time	User Name	Duration
02/18/2021 10:10 AM	bigfix	0:17:19
04/27/2020 11:38 PM	bigfix	0:06:53
04/27/2020 11:07 PM	bigfix	0:14:28

Start Time: 02/18/2021 06:10 PM

Status: Successful

Duration: 0:17:19

Import Log:

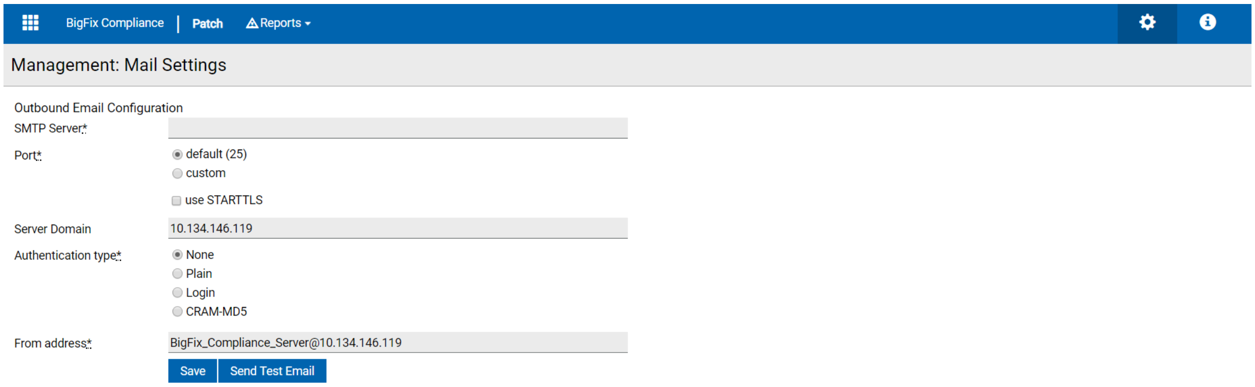
```
# Logfile created on 2021-02-18 18:10:55 +0000 by logger.rb/v1.2.7
2021-02-18 18:10:55 (+0:00:00.000) INFO: BFC Version: 2.0.0.18
2021-02-18 18:10:55 (+0:00:00.000) INFO: Runtime: jruby 9.2.0.0 (2.5.0) 2018-05-24 81156a8 IBM J9 VM 2.9 on 8.0.6.5 -
pwa6480sr6fp5-20200111_02(SR6 FP5) +jit [mswin32-x86_64]
2021-02-18 18:10:55 (+0:00:00.000) INFO: All times in log are in UTC time zone!
2021-02-18 18:10:55 (+0:00:00.000) INFO: Import created at (UTC): 2021-02-18 18:10:55 UTC
2021-02-18 18:10:55 (+0:00:00.000) INFO: Check datasources connectivity: Start
2021-02-18 18:10:56 (+0:00:00.923) INFO: Data Source: Data Source, Bigfix Server Version: 9.5.14.73 with schema: 9.107, DB Version:
13.0.4001.0 SP1 Standard Edition (64-bit)
2021-02-18 18:10:56 (+0:00:00.015) INFO: Check datasources connectivity: Success
2021-02-18 18:11:08 (+0:00:12.023) INFO: ETL before snapshot task: Calling all Model.before_snapshot blocks: Start
2021-02-18 18:11:14 (+0:00:06.041) INFO: ETL before snapshot task: Calling all Model.before_snapshot blocks: Success
2021-02-18 18:11:14 (+0:00:00.001) INFO: ETL before snapshot task: from PR::VulnerabilitySource        : Start
2021-02-18 18:11:14 (+0:00:00.116) INFO: ETL before snapshot task: from PR::VulnerabilitySource        : Success
2021-02-18 18:11:14 (+0:00:00.004) INFO: ETL task: Initialize datasource Data Source: Start
2021-02-18 18:11:14 (+0:00:00.077) INFO: ETL task: Initialize datasource Data Source: Success
2021-02-18 18:11:14 (+0:00:00.000) INFO: ETL Datasource task: from Data Source - RawDatasourceSite
```

Mail Settings

You must configure outbound email in Mail Settings to schedule an export to the desired email recipient. The reports can be sent to multiple email recipients.

Procedure

1. Click **Management**.
2. Select **Mail Settings** from the drop down.
3. Set the **Outbound Email Configuration**.
4. Enter the **SMTP Server** details.
5. Select either the **Default or Custom** port.
6. Select the **use STARTTLS** check box if you want to make the connection secure.
7. Enter the **Server Domain**.
8. Select the **Authentication type**.
9. Enter the **From address**.
10. Click **Save**.



Management: Mail Settings

Outbound Email Configuration

SMTP Server*

Port* ● default (25) ○ custom

□ use STARTTLS

Server Domain 10.134.146.119

Authentication type* ● None ○ Plain ○ Login ○ CRAM-MD5

From address* BigFix_Compliance_Server@10.134.146.119

To Schedule an export, go to Scheduling *(on page 15)*.

Notifications

You can create email notifications using this section.

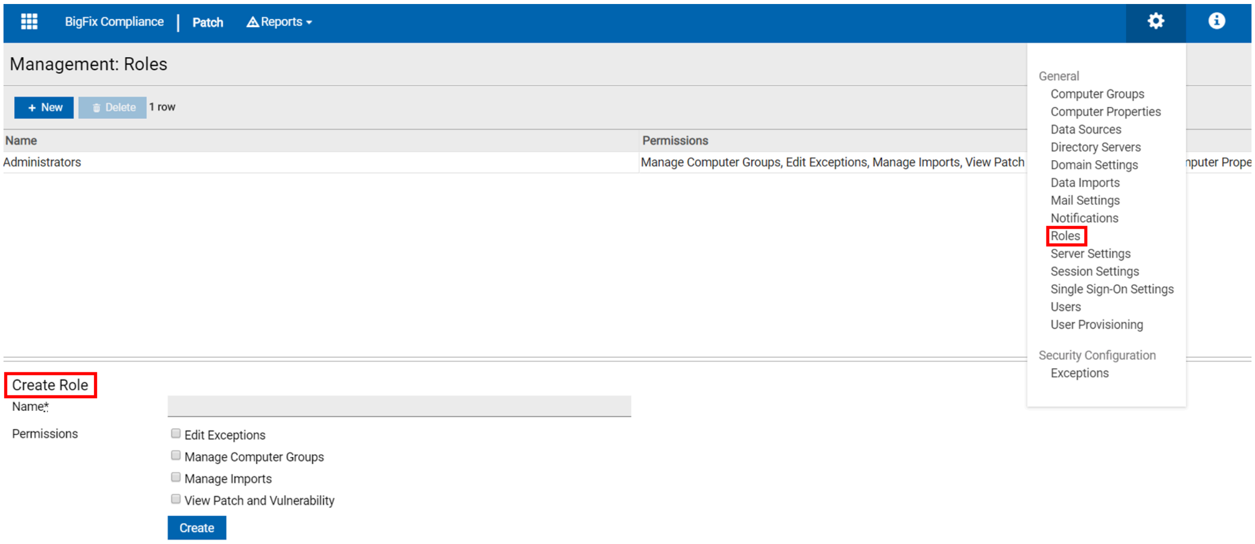
To create email notifications:

1. On the header bar, click **Management Gear Icon**.
2. Click **Notifications**.
3. Enter the **Name**.
4. Select the **Type** using the dropdown.
5. Select the **Report**.
6. Select the **Alerts**.
7. Enter the email address of the recipients.
8. Click **Create**.

   You must setup the mail settings to create email notifications to the recipients. To setup the mail settings, see Enabling mail settings.

Roles

Use the Roles to assign new roles to users or edit existing roles. You can assign permissions to the users to Edit Exceptions Manage Computer Groups, Manage Imports, and View Patch and Vulnerability etc.



Management: Roles

1 row

Name	Permissions
Administrators	Manage Computer Groups, Edit Exceptions, Manage Imports, View Patch … nputer Prope

Create Role

Name*

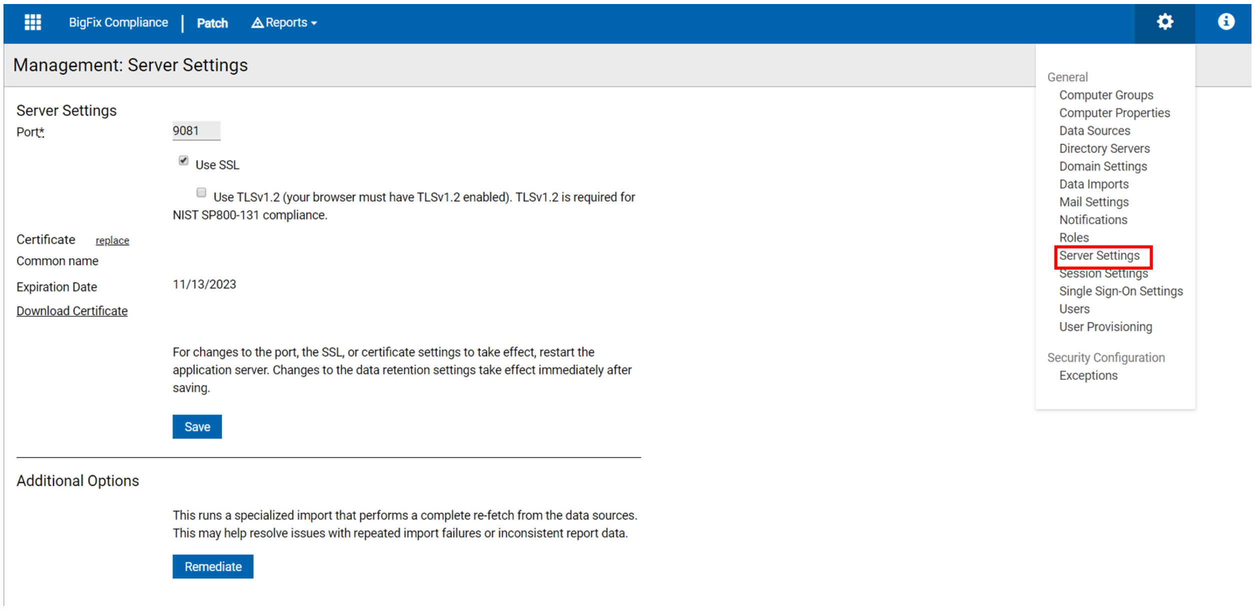
Permissions

- □ Edit Exceptions
- □ Manage Computer Groups
- □ Manage Imports
- □ View Patch and Vulnerability

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 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.



Management: Server Settings

Server Settings

Port* 9081

☑ Use SSL

□ Use TLSv1.2 (your browser must have TLSv1.2 enabled). TLSv1.2 is required for NIST SP800-131 compliance.

Certificate replace

Common name

Expiration Date 11/13/2023

Download Certificate

For changes to the port, the SSL, or certificate settings to take effect, restart the application server. Changes to the data retention settings take effect immediately after saving.

Additional Options

This runs a specialized import that performs a complete re-fetch from the data sources. This may help resolve issues with repeated import failures or inconsistent report data.

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 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.

Directory Servers

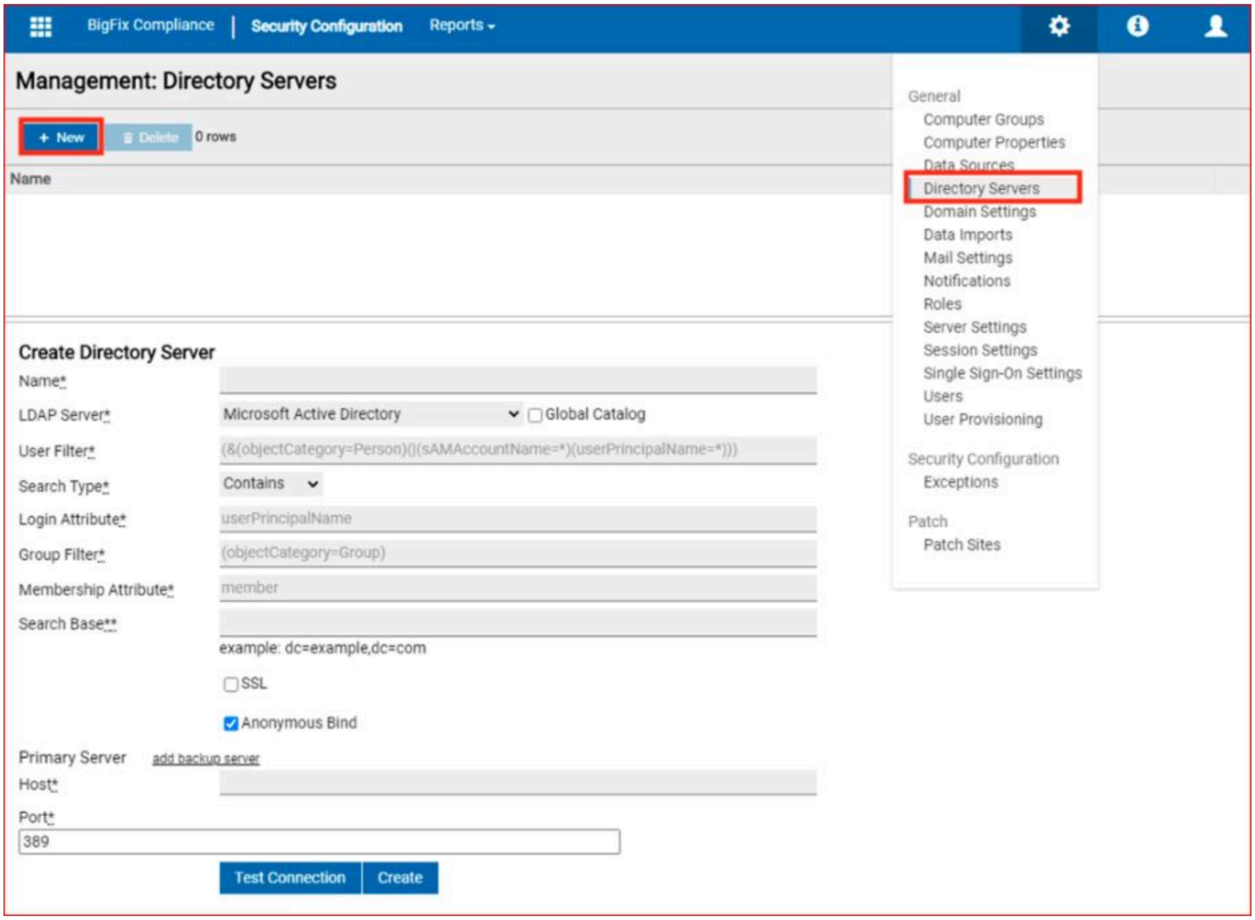
BigFix Compliance Analytics supports authentication with directory servers through Lightweight Directory Access Protocol (LDAP). You can add directory servers to BigFix Compliance Analytics so that the users can log in using credentials based on your existing authentication scheme.

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 50)* 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 *(on page 51)* section).



Create Directory Server

Name*:

LDAP Server*: Microsoft Active Directory ☐ Global Catalog

User Filter*: (&(objectCategory=Person)(|(sAMAccountName=*)(userPrincipalName=*)))

Search Type*: Contains

Login Attribute*: userPrincipalName

Group Filter*: (objectCategory=Group)

Membership Attribute*: member

Search Base**:

example: dc=example,dc=com

☐ SSL

☑ Anonymous Bind

Primary Server add backup server

Host*:

Port*: 389

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. In the top navigation bar, click **Management > Directory Servers**.
2. To create an LDAP connection, click **New**.
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. If your directory server uses Secure Socket Layer protocol, select the **SSL** check box.

7. If your server requires authentication, 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.

   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. In the **Host** text field, provide the host name or IP address of your primary LDAP server.
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. To verify whether all of the provided entries are valid, click **Test Connection**.
    A confirmation pop-up window opens.
12. 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**.

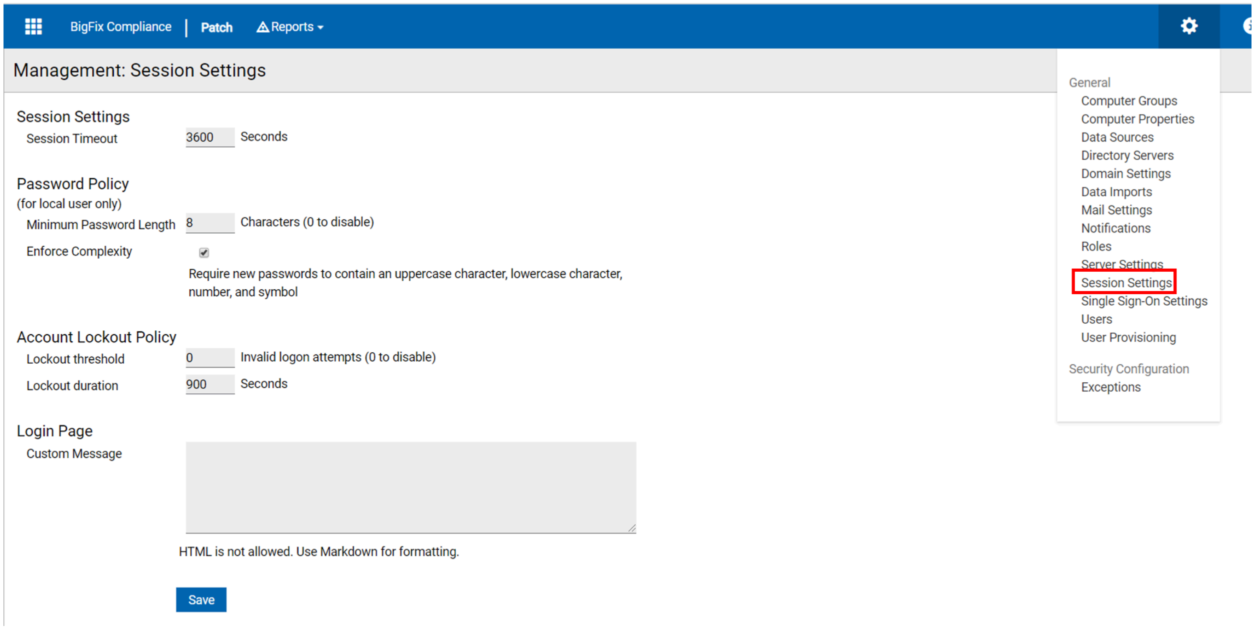
Deleting a directory server

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**.

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 Gear Icon > Session Settings**.



Management: Session Settings

Session Settings

Session Timeout 3600 Seconds

Password Policy
(for local user only)

Minimum Password Length 8 Characters (0 to disable)

Enforce Complexity ☑

Require new passwords to contain an uppercase character, lowercase character, number, and symbol

Account Lockout Policy

Lockout threshold 0 Invalid logon attempts (0 to disable)

Lockout duration 900 Seconds

Login Page

Custom Message

HTML is not allowed. Use Markdown for formatting.

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**.

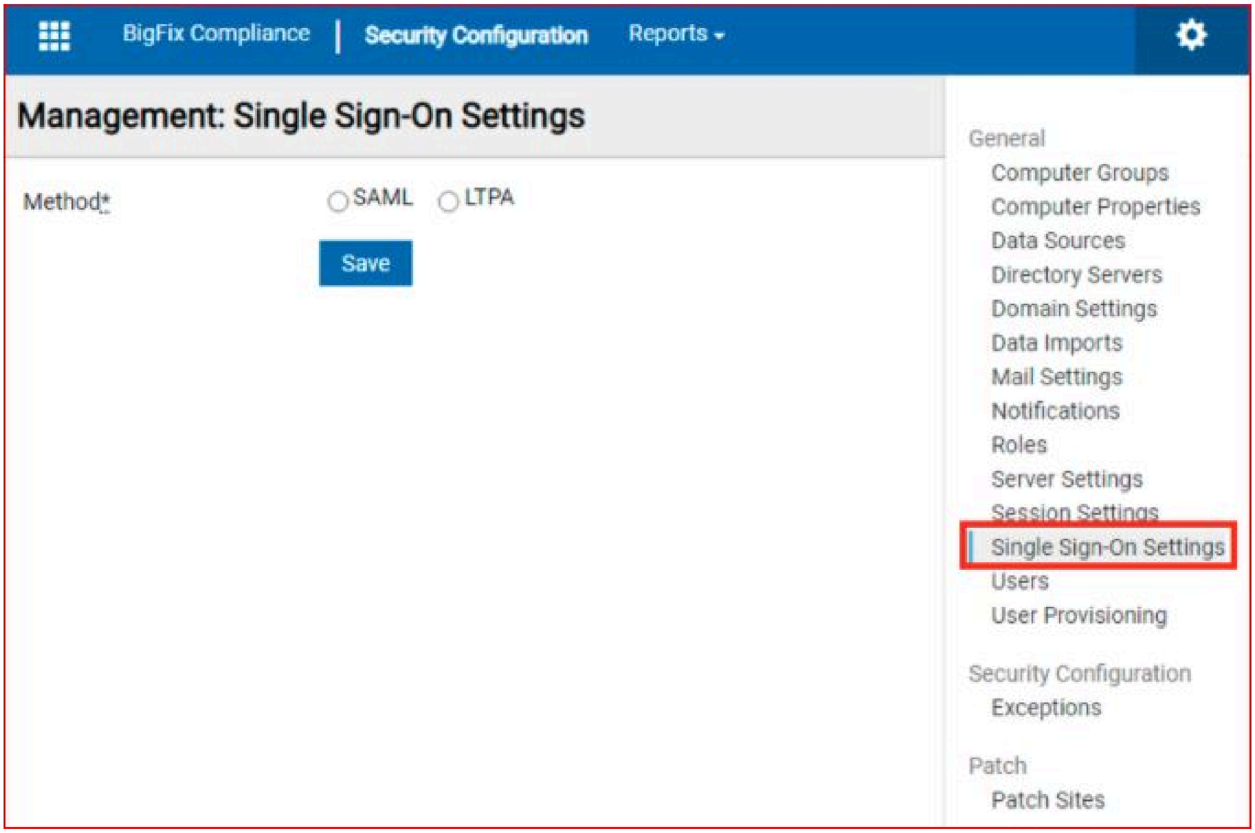
Single Sign-On Settings

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.



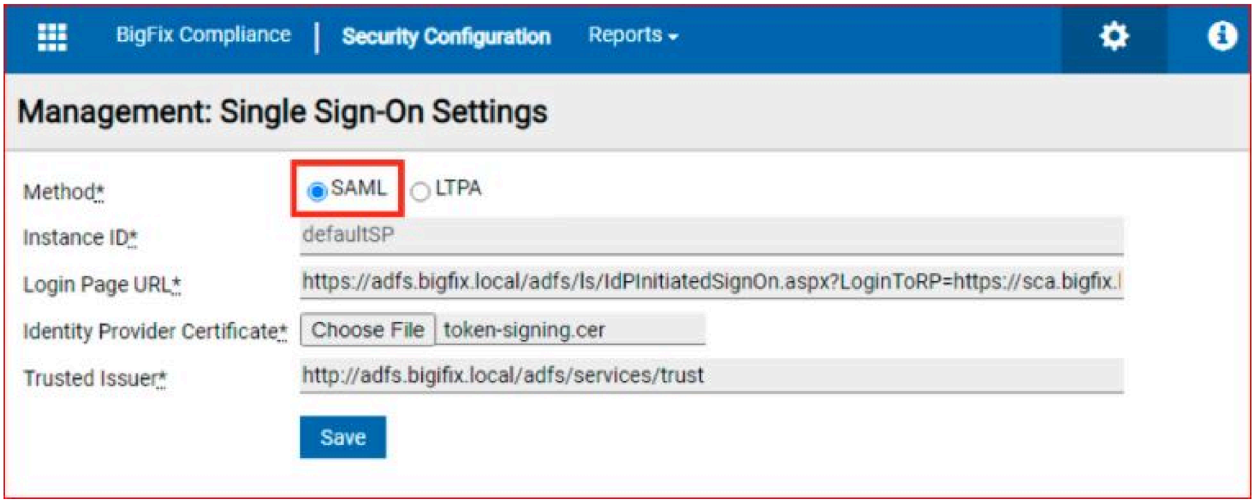
Management: Single Sign-On Settings

Method* ○ SAML ○ LTPA

Save

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).



Management: Single Sign-On Settings

Method* ● SAML ○ LTPA

Instance ID* defaultSP

Login Page URL* https://adfs.bigfix.local/adfs/ls/IdPInitiatedSignOn.aspx?LoginToRP=https://sca.bigfix.l

Identity Provider Certificate* Choose File token-signing.cer

Trusted Issuer* http://adfs.bigifix.local/adfs/services/trust

Save

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 30)* 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 *(on page 51)* 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:

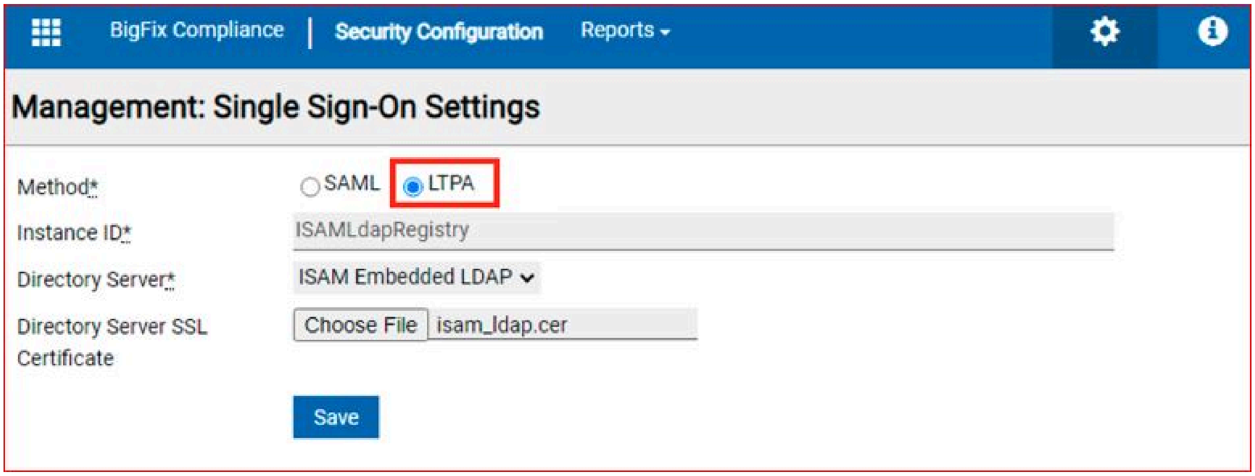
c. Click **Enable**.

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).



Management: Single Sign-On Settings

Method* ○ SAML ● LTPA
Instance ID* ISAMLdapRegistry
Directory Server* ISAM Embedded LDAP
Directory Server SSL Certificate: Choose File isam_ldap.cer

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 Directory Servers *(on page 30)* 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.

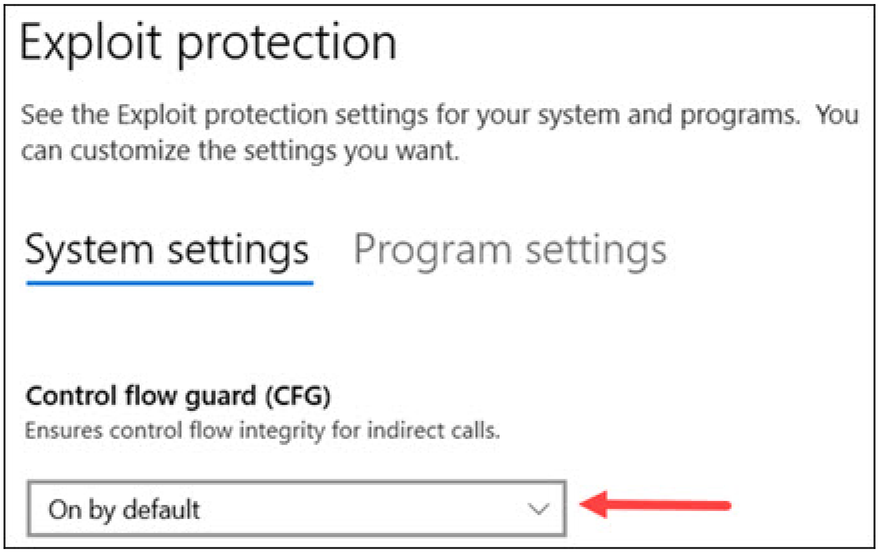
    a. Login back to Single Sign-On Settings page.
    b. Click **Download LPTA Keys** link and save `ltpa.keys`.

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`.



Exploit protection

See the Exploit protection settings for your system and programs. You can customize the settings you want.

Control flow guard (CFG)

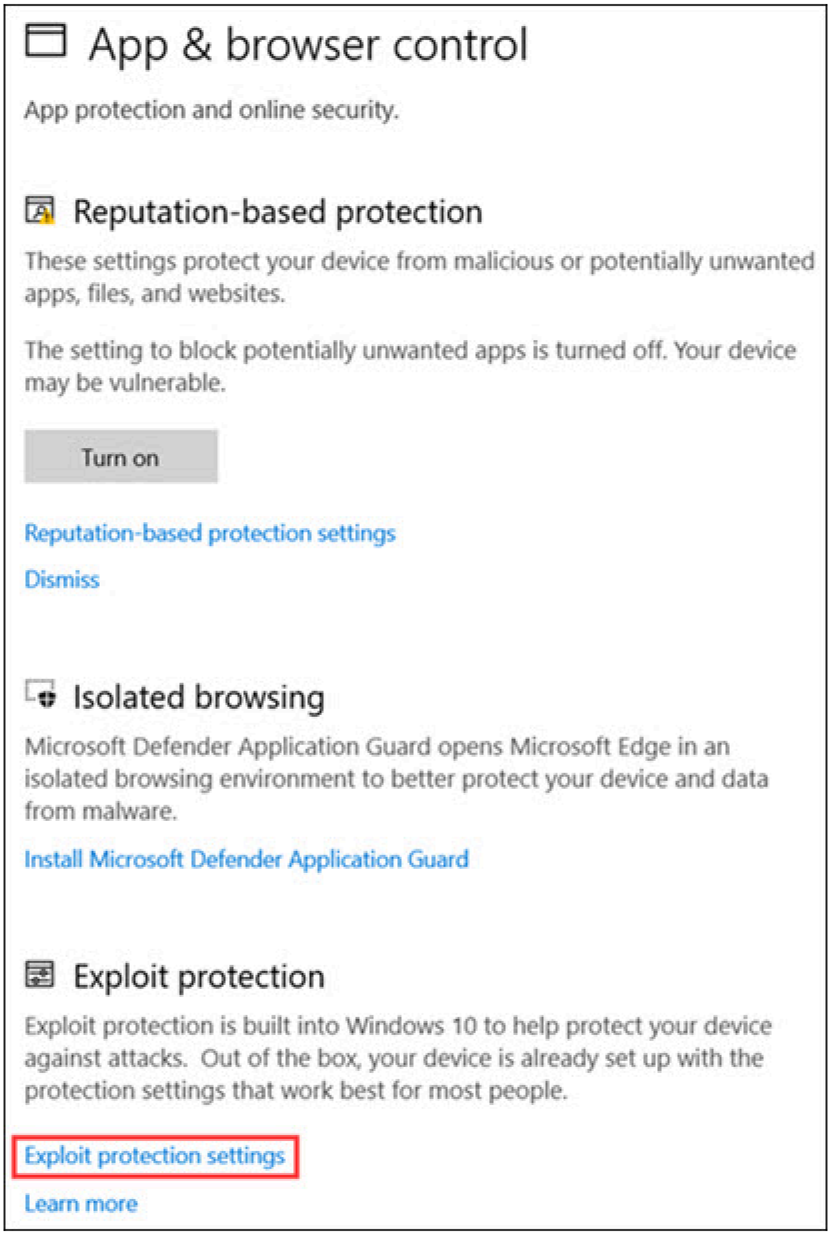
Ensures control flow integrity for indirect calls.

On by default

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**.



App & browser control

App protection and online security.

Reputation-based protection

These settings protect your device from malicious or potentially unwanted apps, files, and websites.

The setting to block potentially unwanted apps is turned off. Your device may be vulnerable.

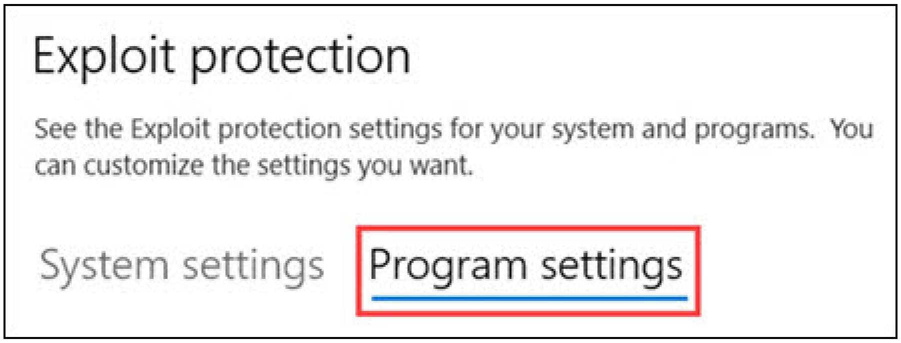
Isolated browsing

Microsoft Defender Application Guard opens Microsoft Edge in an isolated browsing environment to better protect your device and data from malware.

Exploit protection

Exploit protection is built into Windows 10 to help protect your device against attacks. Out of the box, your device is already set up with the protection settings that work best for most people.

2. Click **Program settings**.

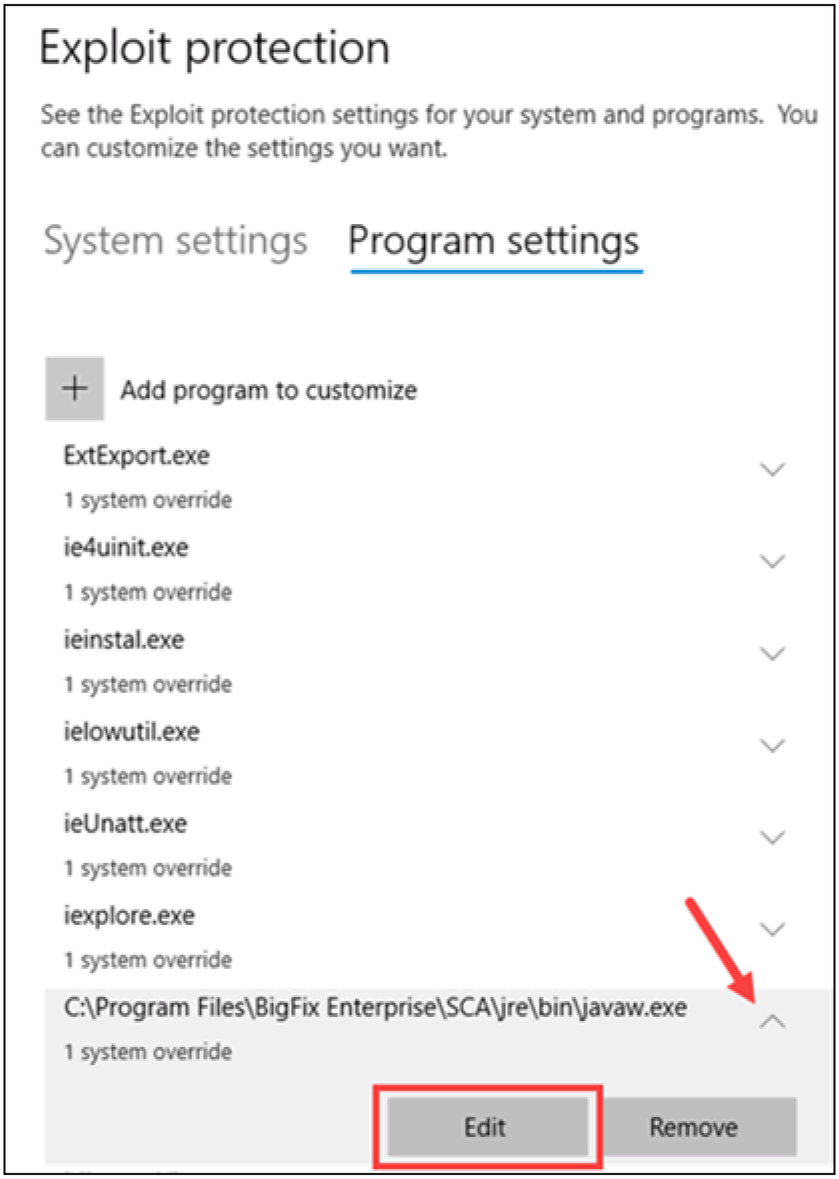


Exploit protection

See the Exploit protection settings for your system and programs. You can customize the settings you want.

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.



Exploit protection

See the Exploit protection settings for your system and programs. You can customize the settings you want.

ExtExport.exe
1 system override

ie4uinit.exe
1 system override

ieinstal.exe
1 system override

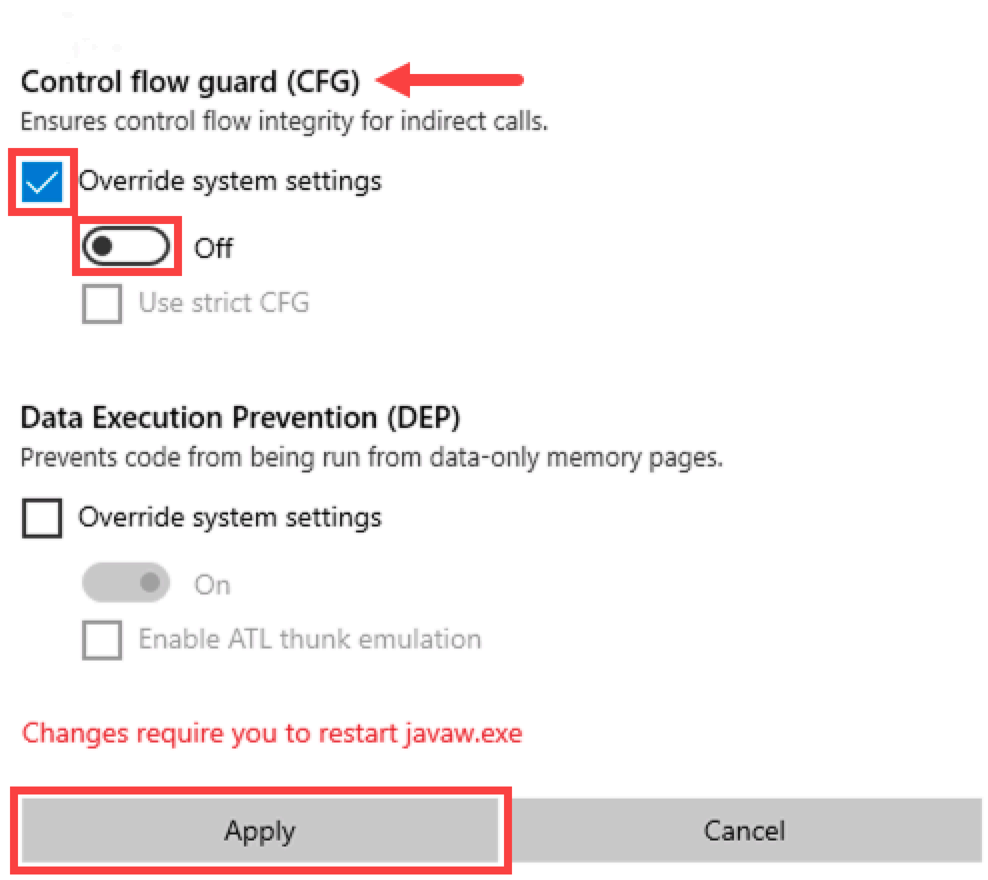
ielowutil.exe
1 system override

ieUnatt.exe
1 system override

iexplore.exe
1 system override

C:\Program Files\BigFix Enterprise\SCA\jre\bin\javaw.exe
1 system override

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



Control flow guard (CFG)

Ensures control flow integrity for indirect calls.

☑ Override system settings

Off

□ Use strict CFG

Data Execution Prevention (DEP)

Prevents code from being run from data-only memory pages.

□ Override system settings

On

□ Enable ATL thunk emulation

Changes require you to restart javaw.exe

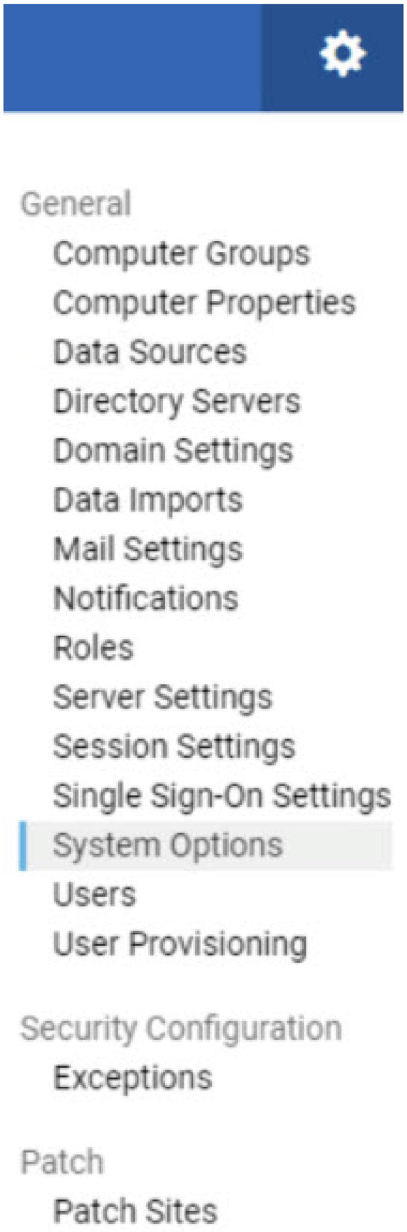
Important: Restart the BigFix Compliance service to implement the changes.

System Options

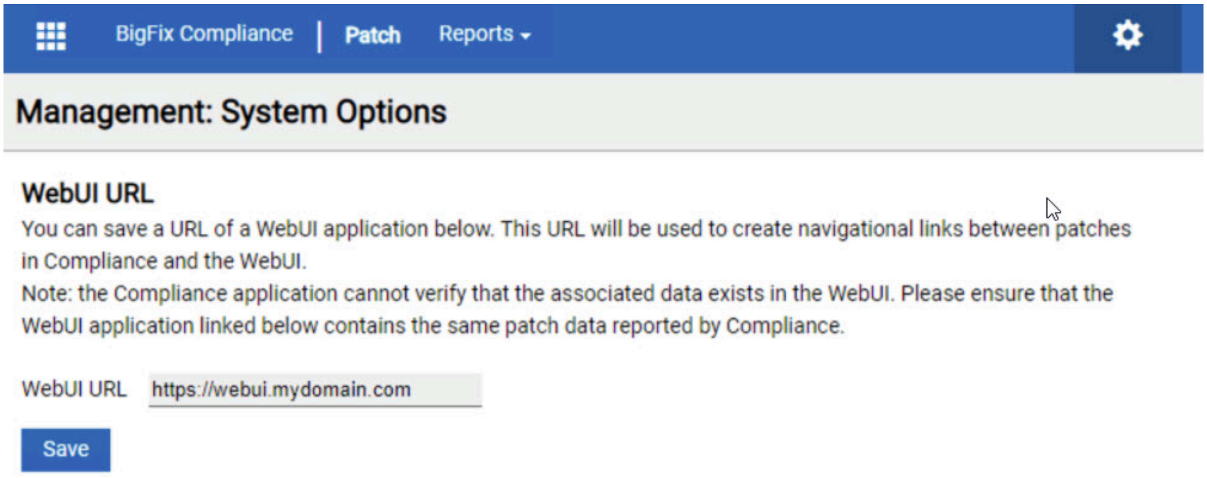
Use System Options too add WebUI URL in Compliance's report.

You can specify WebUI URL under **Management > System Options**. You can also add the WebUI URL in Compliance's report.

Note: If the WebUI URL is not specified in the System Options, then these links are not shown in the Patch details page or in 'Configure View' option.



Enter WebUI URL and click **Save**.



Management: System Options

WebUI URL

You can save a URL of a WebUI application below. This URL will be used to create navigational links between patches in Compliance and the WebUI.

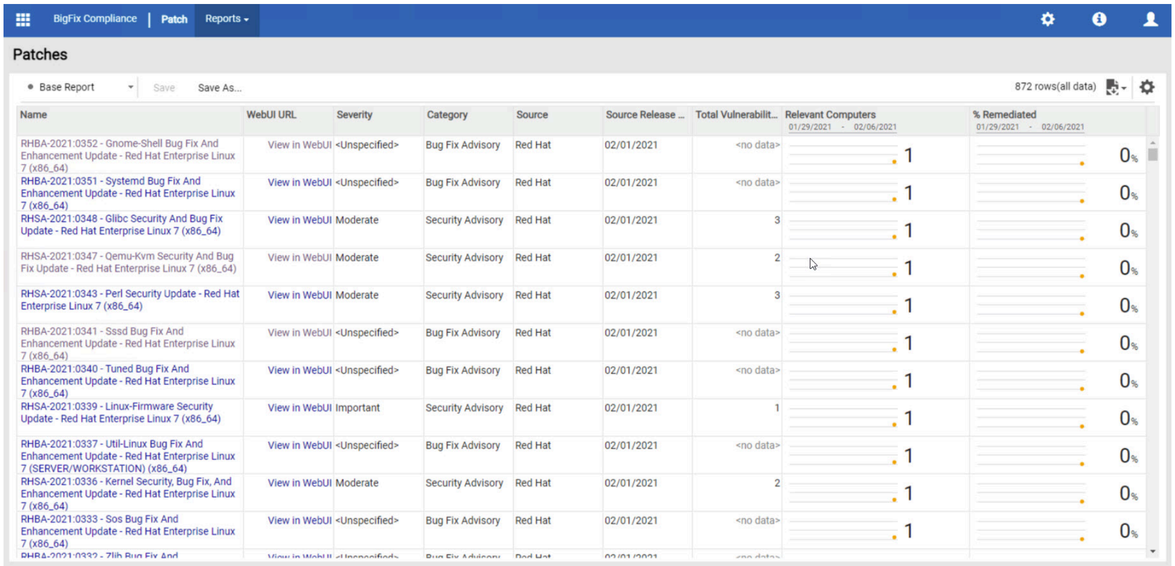
Note: the Compliance application cannot verify that the associated data exists in the WebUI. Please ensure that the WebUI application linked below contains the same patch data reported by Compliance.

WebUI URL: https://webui.mydomain.com

Note: System Options is available in Compliance 2.0p2 or above.

Adding a WebUI URL using Patch details page

1. Navigate to **Reports > Patches** or navigate to **Reports > Computers > Computer name > Subscribed Patches**
2. Click the Patch name.

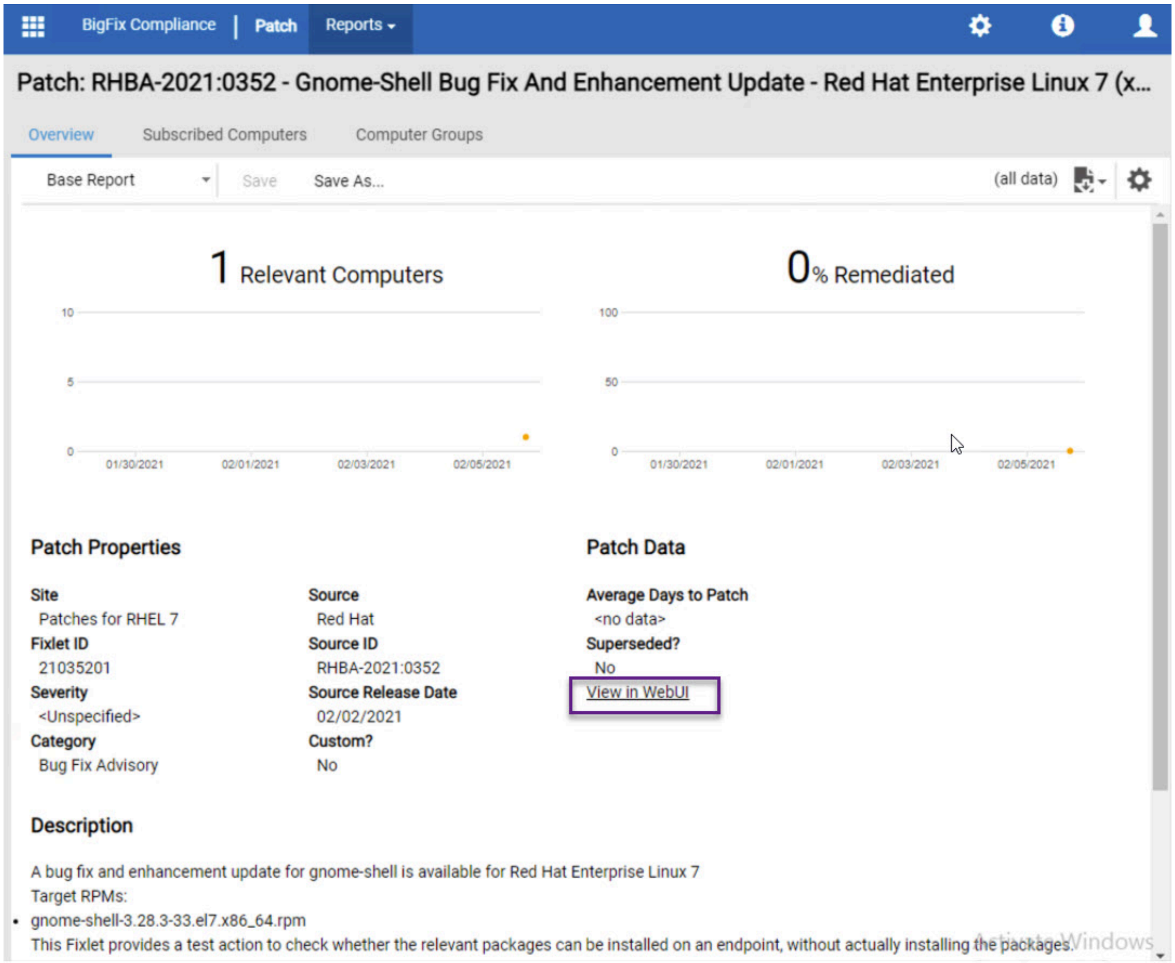


Patches

872 rows(all data)

Name	WebUI URL	Severity	Category	Source	Source Release ...	Total Vulnerabilit...	Relevant Computers 01/29/2021 - 02/06/2021	% Remediated 01/29/2021 - 02/06/2021
RHBA-2021:0352 - Gnome-Shell Bug Fix And Enhancement Update - Red Hat Enterprise Linux 7 (x86_64)	View in WebUI	<Unspecified>	Bug Fix Advisory	Red Hat	02/01/2021	<no data>	1	0%
RHBA-2021:0351 - Systemd Bug Fix And Enhancement Update - Red Hat Enterprise Linux 7 (x86_64)	View in WebUI	<Unspecified>	Bug Fix Advisory	Red Hat	02/01/2021	<no data>	1	0%
RHSA-2021:0348 - Glibc Security And Bug Fix Update - Red Hat Enterprise Linux 7 (x86_64)	View in WebUI	Moderate	Security Advisory	Red Hat	02/01/2021	3	1	0%
RHSA-2021:0347 - Qemu-Kvm Security And Bug Fix Update - Red Hat Enterprise Linux 7 (x86_64)	View in WebUI	Moderate	Security Advisory	Red Hat	02/01/2021	2	1	0%
RHSA-2021:0343 - Perl Security Update - Red Hat Enterprise Linux 7 (x86_64)	View in WebUI	Moderate	Security Advisory	Red Hat	02/01/2021	3	1	0%
RHBA-2021:0341 - Sssd Bug Fix And Enhancement Update - Red Hat Enterprise Linux 7 (x86_64)	View in WebUI	<Unspecified>	Bug Fix Advisory	Red Hat	02/01/2021	<no data>	1	0%
RHBA-2021:0340 - Tuned Bug Fix And Enhancement Update - Red Hat Enterprise Linux 7 (x86_64)	View in WebUI	<Unspecified>	Bug Fix Advisory	Red Hat	02/01/2021	<no data>	1	0%
RHSA-2021:0339 - Linux-Firmware Security Update - Red Hat Enterprise Linux 7 (x86_64)	View in WebUI	Important	Security Advisory	Red Hat	02/01/2021	1	1	0%
RHBA-2021:0337 - Util-Linux Bug Fix And Enhancement Update - Red Hat Enterprise Linux 7 (SERVER/WORKSTATION) (x86_64)	View in WebUI	<Unspecified>	Bug Fix Advisory	Red Hat	02/01/2021	<no data>	1	0%
RHSA-2021:0336 - Kernel Security, Bug Fix, And Enhancement Update - Red Hat Enterprise Linux 7 (x86_64)	View in WebUI	Moderate	Security Advisory	Red Hat	02/01/2021	2	1	0%
RHBA-2021:0333 - Sos Bug Fix And Enhancement Update - Red Hat Enterprise Linux 7 (x86_64)	View in WebUI	<Unspecified>	Bug Fix Advisory	Red Hat	02/01/2021	<no data>	1	0%
RHBA-2021:0332 - Zlib Bug Fix And	View in WebUI	<Unspecified>	Bug Fix Advisory	Red Hat	02/01/2021	<no data>		

3. Click the **View in WebUI** link in Patch details page.



Patch: RHBA-2021:0352 - Gnome-Shell Bug Fix And Enhancement Update - Red Hat Enterprise Linux 7 (x...

1 Relevant Computers

0% Remediated

Patch Properties

Site
Patches for RHEL 7
Fixlet ID
21035201
Severity
<Unspecified>
Category
Bug Fix Advisory

Source
Red Hat
Source ID
RHBA-2021:0352
Source Release Date
02/02/2021
Custom?
No

Patch Data

Average Days to Patch
<no data>
Superseded?
No

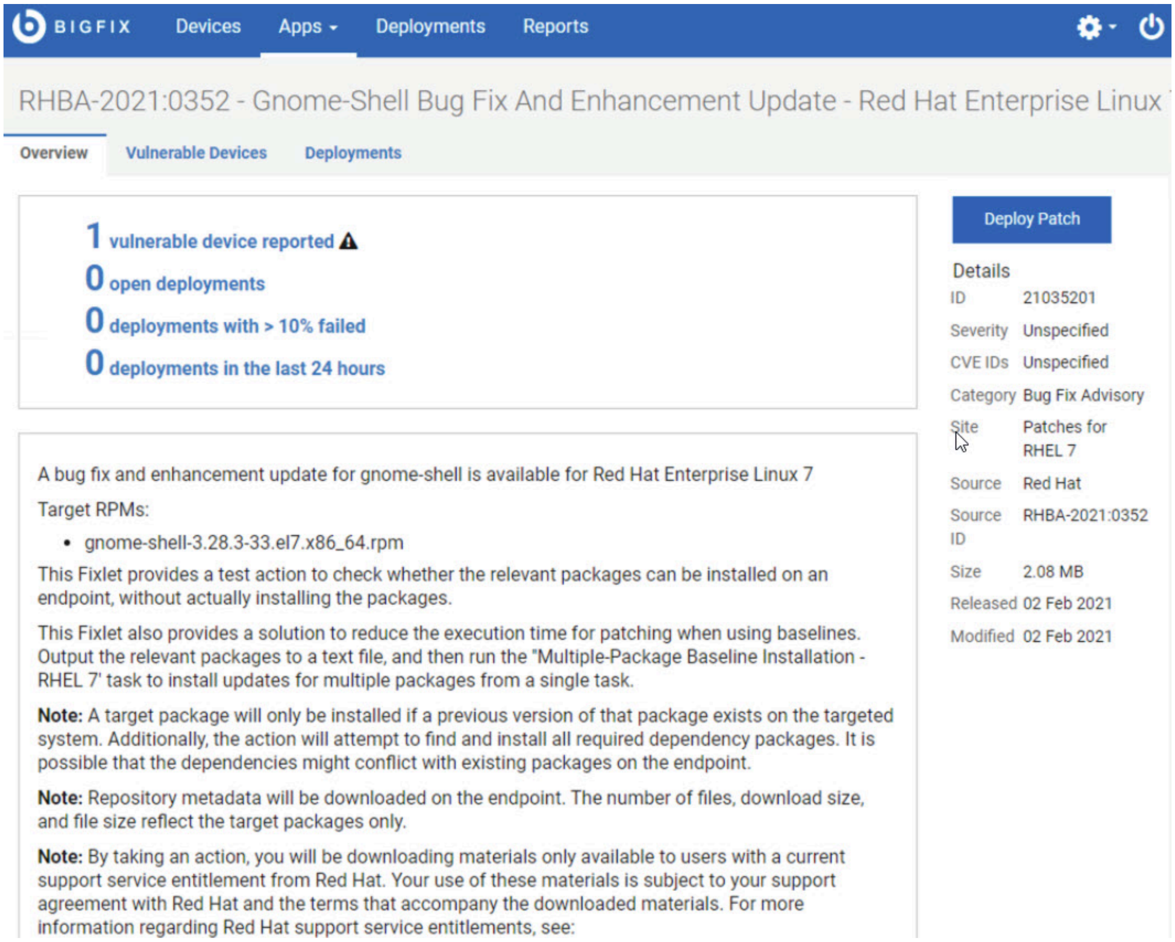
Description

A bug fix and enhancement update for gnome-shell is available for Red Hat Enterprise Linux 7
Target RPMs:

- gnome-shell-3.28.3-33.el7.x86_64.rpm

This Fixlet provides a test action to check whether the relevant packages can be installed on an endpoint, without actually installing the packages.

The following WebUI Patch page is displayed.



RHBA-2021:0352 - Gnome-Shell Bug Fix And Enhancement Update - Red Hat Enterprise Linux

1 vulnerable device reported ⚠
0 open deployments
0 deployments with > 10% failed
0 deployments in the last 24 hours

A bug fix and enhancement update for gnome-shell is available for Red Hat Enterprise Linux 7

Target RPMs:

- gnome-shell-3.28.3-33.el7.x86_64.rpm

This Fixlet provides a test action to check whether the relevant packages can be installed on an endpoint, without actually installing the packages.

This Fixlet also provides a solution to reduce the execution time for patching when using baselines. Output the relevant packages to a text file, and then run the "Multiple-Package Baseline Installation - RHEL 7' task to install updates for multiple packages from a single task.

Note: A target package will only be installed if a previous version of that package exists on the targeted system. Additionally, the action will attempt to find and install all required dependency packages. It is possible that the dependencies might conflict with existing packages on the endpoint.

Note: Repository metadata will be downloaded on the endpoint. The number of files, download size, and file size reflect the target packages only.

Note: By taking an action, you will be downloading materials only available to users with a current support service entitlement from Red Hat. Your use of these materials is subject to your support agreement with Red Hat and the terms that accompany the downloaded materials. For more information regarding Red Hat support service entitlements, see:

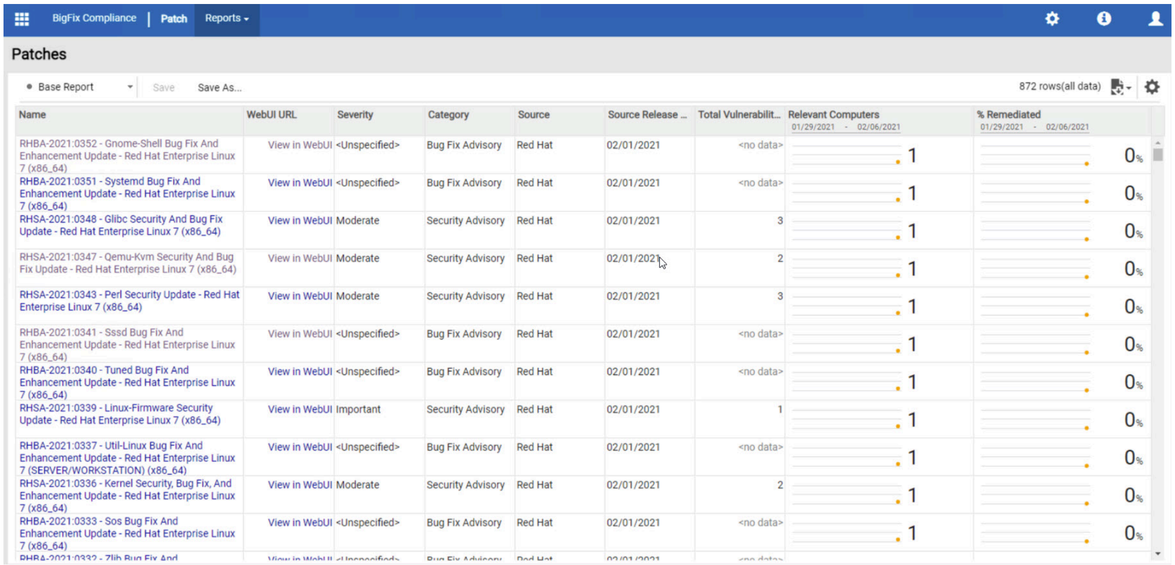
Details

ID	21035201
Severity	Unspecified
CVE IDs	Unspecified
Category	Bug Fix Advisory
Site	Patches for RHEL 7
Source	Red Hat
Source ID	RHBA-2021:0352
Size	2.08 MB
Released	02 Feb 2021
Modified	02 Feb 2021

Note: When redirected to WebUI, the WebUI login page may be displayed if the user is not authenticated in the browser. On successful authentication, destination Patch page is displayed.

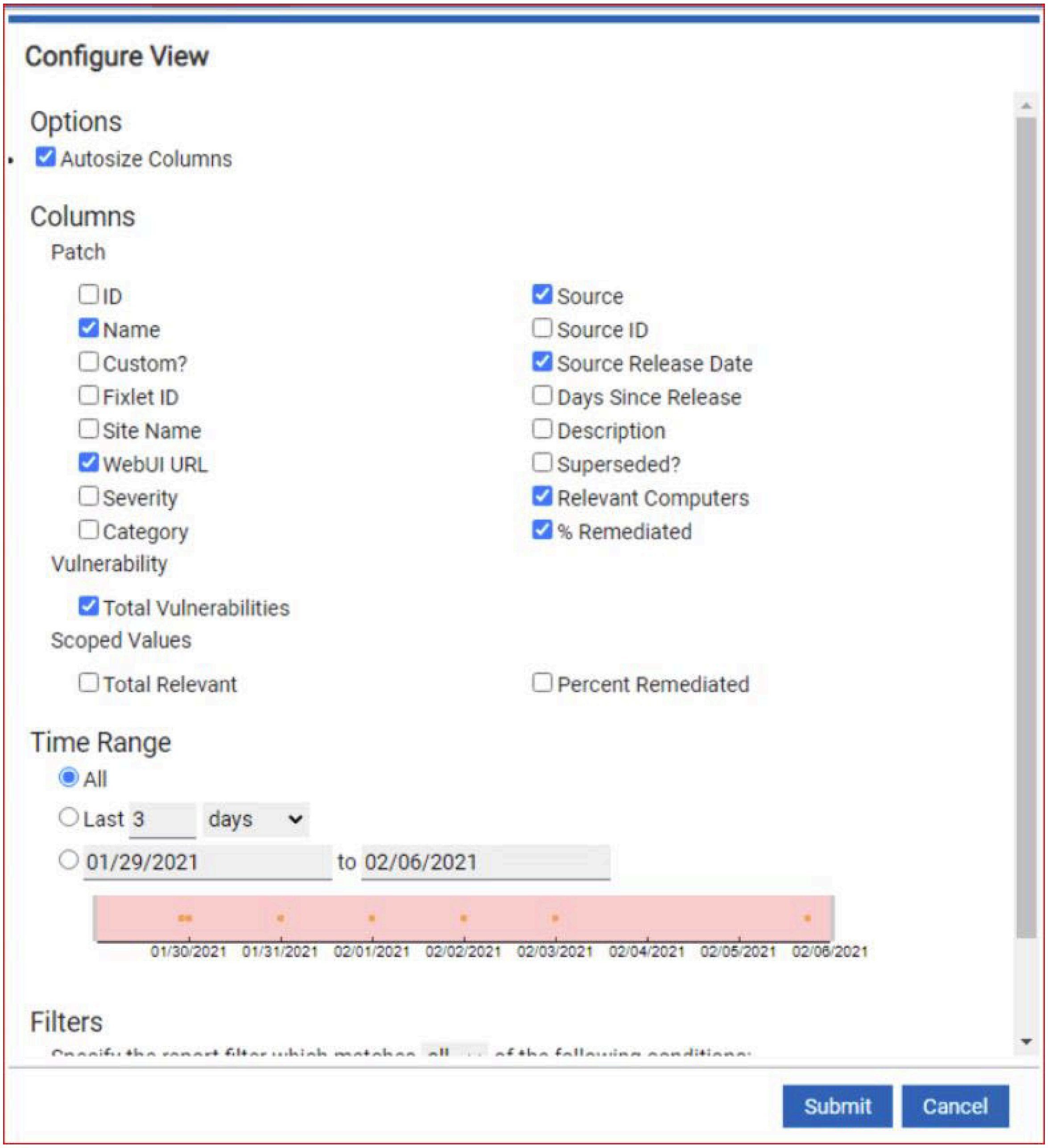
Enabling WebUI URL column in a Patch grid report

1. Navigate to **Reports > Patches** or navigate to **Reports > Computers > Computer name > Subscribed Patches**



Name	WebUI URL	Severity	Category	Source	Source Release ...	Total Vulnerabilit...	Relevant Computers 01/29/2021 - 02/06/2021	% Remediated 01/29/2021 - 02/06/2021
RHBA-2021:0352 - Gnome-Shell Bug Fix And Enhancement Update - Red Hat Enterprise Linux 7 (x86_64)	View in WebUI	<Unspecified>	Bug Fix Advisory	Red Hat	02/01/2021	<no data>	1	0%
RHBA-2021:0351 - Systemd Bug Fix And Enhancement Update - Red Hat Enterprise Linux 7 (x86_64)	View in WebUI	<Unspecified>	Bug Fix Advisory	Red Hat	02/01/2021	<no data>	1	0%
RHSA-2021:0348 - Glibc Security And Bug Fix Update - Red Hat Enterprise Linux 7 (x86_64)	View in WebUI	Moderate	Security Advisory	Red Hat	02/01/2021	3	1	0%
RHSA-2021:0347 - Qemu-Kvm Security And Bug Fix Update - Red Hat Enterprise Linux 7 (x86_64)	View in WebUI	Moderate	Security Advisory	Red Hat	02/01/2021	2	1	0%
RHSA-2021:0343 - Perl Security Update - Red Hat Enterprise Linux 7 (x86_64)	View in WebUI	Moderate	Security Advisory	Red Hat	02/01/2021	3	1	0%
RHBA-2021:0341 - Sssd Bug Fix And Enhancement Update - Red Hat Enterprise Linux 7 (x86_64)	View in WebUI	<Unspecified>	Bug Fix Advisory	Red Hat	02/01/2021	<no data>	1	0%
RHBA-2021:0340 - Tuned Bug Fix And Enhancement Update - Red Hat Enterprise Linux 7 (x86_64)	View in WebUI	<Unspecified>	Bug Fix Advisory	Red Hat	02/01/2021	<no data>	1	0%
RHSA-2021:0339 - Linux-Firmware Security Update - Red Hat Enterprise Linux 7 (x86_64)	View in WebUI	Important	Security Advisory	Red Hat	02/01/2021	1	1	0%
RHBA-2021:0337 - Util-Linux Bug Fix And Enhancement Update - Red Hat Enterprise Linux 7 (SERVER/WORKSTATION) (x86_64)	View in WebUI	<Unspecified>	Bug Fix Advisory	Red Hat	02/01/2021	<no data>	1	0%
RHSA-2021:0336 - Kernel Security, Bug Fix, And Enhancement Update - Red Hat Enterprise Linux 7 (x86_64)	View in WebUI	Moderate	Security Advisory	Red Hat	02/01/2021	2	1	0%
RHBA-2021:0333 - Sos Bug Fix And Enhancement Update - Red Hat Enterprise Linux 7 (x86_64)	View in WebUI	<Unspecified>	Bug Fix Advisory	Red Hat	02/01/2021	<no data>	1	0%
RHBA-2021:0332 - Zlib Bug Fix And	View in WebUI	<Unspecified>	Bug Fix Advisory	Red Hat	02/01/2021	<no data>		

2. Click **Configure View**.



Configure View

Options

☑ Autosize Columns

Columns

Patch

☐ ID
☑ Name
☐ Custom?
☐ Fixlet ID
☐ Site Name
☑ WebUI URL
☐ Severity
☐ Category
☑ Source
☐ Source ID
☑ Source Release Date
☐ Days Since Release
☐ Description
☐ Superseded?
☑ Relevant Computers
☑ % Remediated

Vulnerability

☑ Total Vulnerabilities

Scoped Values

☐ Total Relevant
☐ Percent Remediated

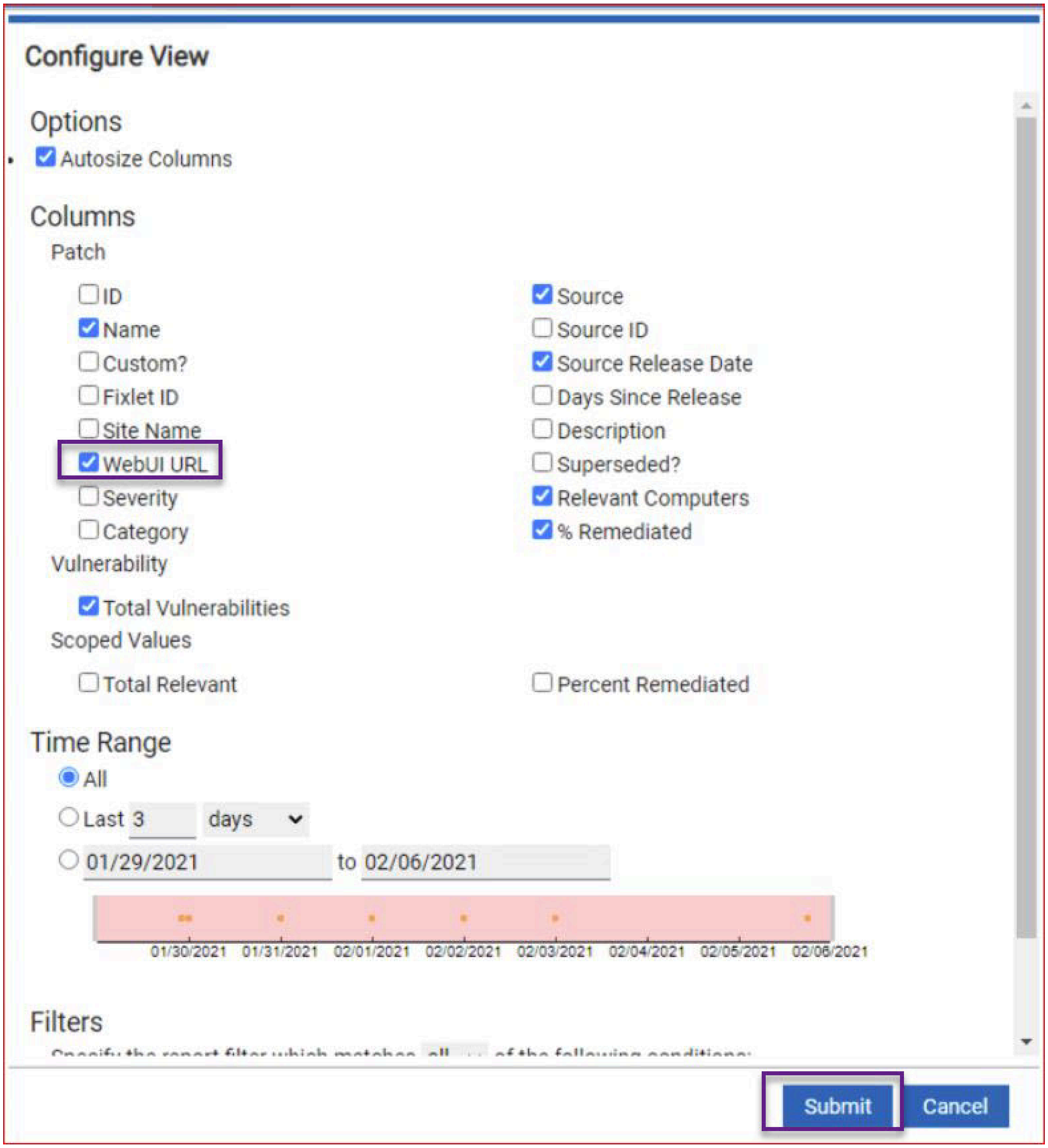
Time Range

● All
○ Last 3 days
○ 01/29/2021 to 02/06/2021

Filters

Specify the report filter which matches all of the following conditions:

3. Select the **WebUI URL** checkbox in the Columns group and click **Submit**.



Configure View

Options

☑ Autosize Columns

Columns

Patch

☐ ID
☑ Name
☐ Custom?
☐ Fixlet ID
☐ Site Name
☑ WebUI URL
☐ Severity
☐ Category

☑ Source
☐ Source ID
☑ Source Release Date
☐ Days Since Release
☐ Description
☐ Superseded?
☑ Relevant Computers
☑ % Remediated

Vulnerability

☑ Total Vulnerabilities

Scoped Values

☐ Total Relevant
☐ Percent Remediated

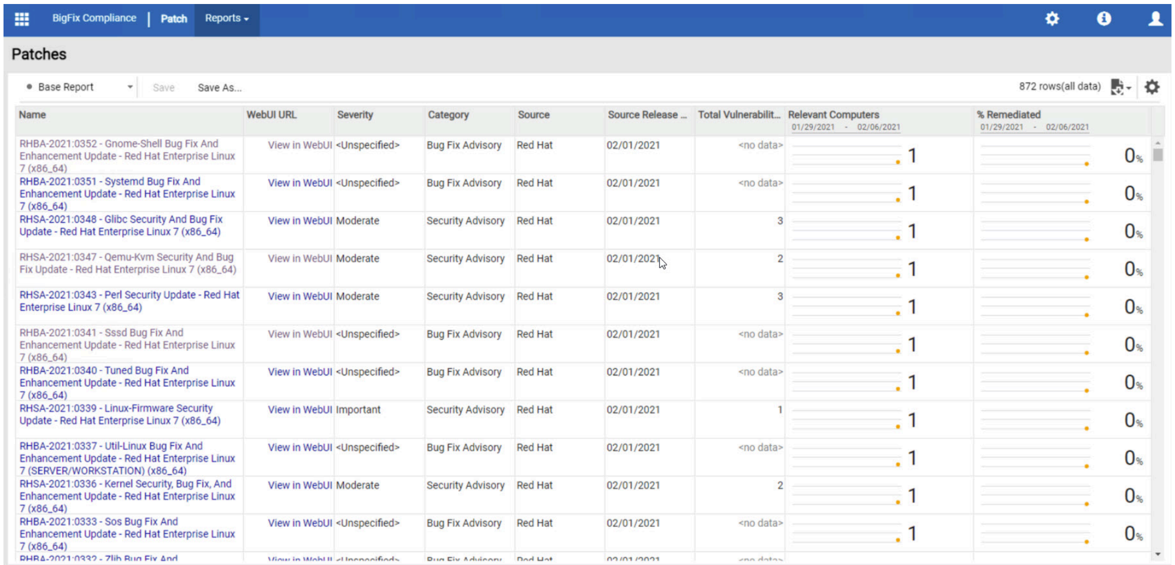
Time Range

● All
○ Last 3 days
○ 01/29/2021 to 02/06/2021

Filters

Specify the report filter which matches all of the following conditions:

4. Click **View in WebUI** in the grid report.



Patches

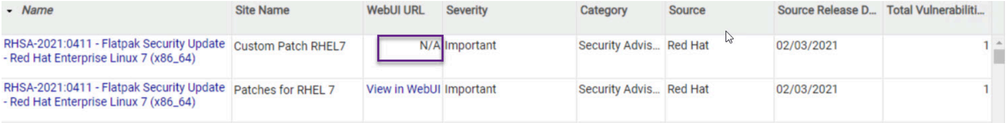
Base Report · Save · Save As...

872 rows(all data)

Name	WebUI URL	Severity	Category	Source	Source Release ...	Total Vulnerabilit...	Relevant Computers 01/29/2021 - 02/06/2021	% Remediated 01/29/2021 - 02/06/2021
RHBA-2021:0352 - Gnome-Shell Bug Fix And Enhancement Update - Red Hat Enterprise Linux 7 (x86_64)	View in WebUI	<Unspecified>	Bug Fix Advisory	Red Hat	02/01/2021	<no data>	1	0%
RHBA-2021:0351 - Systemd Bug Fix And Enhancement Update - Red Hat Enterprise Linux 7 (x86_64)	View in WebUI	<Unspecified>	Bug Fix Advisory	Red Hat	02/01/2021	<no data>	1	0%
RHSA-2021:0348 - Glibc Security And Bug Fix Update - Red Hat Enterprise Linux 7 (x86_64)	View in WebUI	Moderate	Security Advisory	Red Hat	02/01/2021	3	1	0%
RHSA-2021:0347 - Qemu-Kvm Security And Bug Fix Update - Red Hat Enterprise Linux 7 (x86_64)	View in WebUI	Moderate	Security Advisory	Red Hat	02/01/2021	2	1	0%
RHSA-2021:0343 - Perl Security Update - Red Hat Enterprise Linux 7 (x86_64)	View in WebUI	Moderate	Security Advisory	Red Hat	02/01/2021	3	1	0%
RHBA-2021:0341 - Sssd Bug Fix And Enhancement Update - Red Hat Enterprise Linux 7 (x86_64)	View in WebUI	<Unspecified>	Bug Fix Advisory	Red Hat	02/01/2021	<no data>	1	0%
RHBA-2021:0340 - Tuned Bug Fix And Enhancement Update - Red Hat Enterprise Linux 7 (x86_64)	View in WebUI	<Unspecified>	Bug Fix Advisory	Red Hat	02/01/2021	<no data>	1	0%
RHSA-2021:0339 - Linux-Firmware Security Update - Red Hat Enterprise Linux 7 (x86_64)	View in WebUI	Important	Security Advisory	Red Hat	02/01/2021	1	1	0%
RHBA-2021:0337 - Util-Linux Bug Fix And Enhancement Update - Red Hat Enterprise Linux 7 (SERVER/WORKSTATION) (x86_64)	View in WebUI	<Unspecified>	Bug Fix Advisory	Red Hat	02/01/2021	<no data>	1	0%
RHSA-2021:0336 - Kernel Security, Bug Fix, And Enhancement Update - Red Hat Enterprise Linux 7 (x86_64)	View in WebUI	Moderate	Security Advisory	Red Hat	02/01/2021	2	1	0%
RHBA-2021:0333 - Sos Bug Fix And Enhancement Update - Red Hat Enterprise Linux 7 (x86_64)	View in WebUI	<Unspecified>	Bug Fix Advisory	Red Hat	02/01/2021	<no data>	1	0%
RHBA-2021:0332 - Zlib Bug Fix And	View in WebUI	<Unspecified>	Bug Fix Advisory	Red Hat	02/01/2021	<no data>		

Note:

- When the WebUI URL link is not available, you see "N/A" for all patches under custom patch sites (specified in **Management > Patch Sites**).

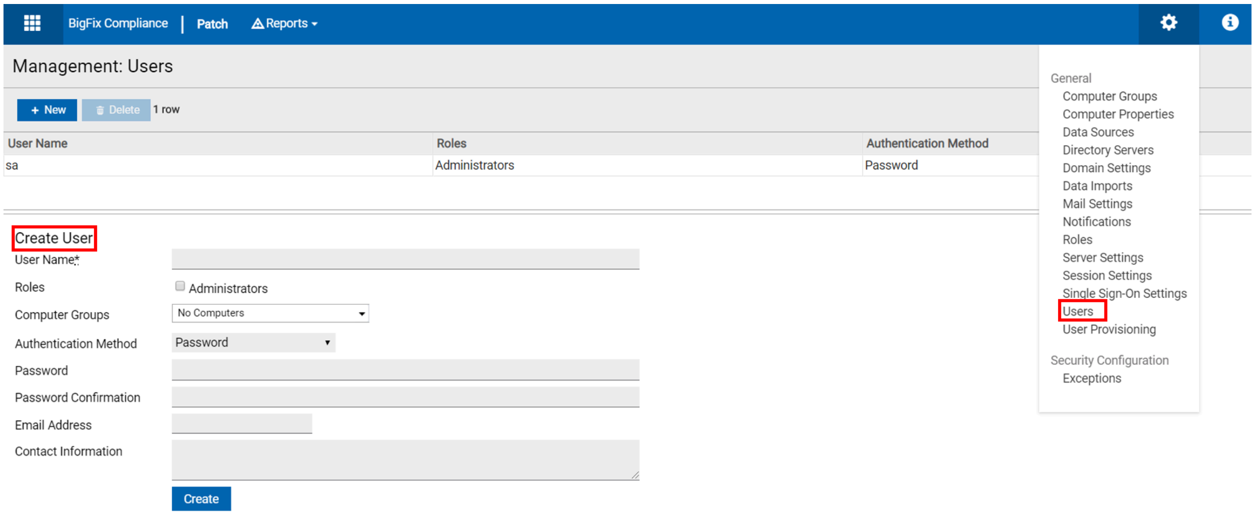


Name	Site Name	WebUI URL	Severity	Category	Source	Source Release D...	Total Vulnerabiliti...
RHSA-2021:0411 - Flatpak Security Update - Red Hat Enterprise Linux 7 (x86_64)	Custom Patch RHEL7	N/A	Important	Security Advis...	Red Hat	02/03/2021	1
RHSA-2021:0411 - Flatpak Security Update - Red Hat Enterprise Linux 7 (x86_64)	Patches for RHEL 7	View in WebUI	Important	Security Advis...	Red Hat	02/03/2021	1

- Only one WebUI URL can be specified at this time even with deployment having multiple datasources (links to the patches from rest of the datasources are invalid).

Users

Use the Users section to create and edit users, assign roles, and assign a set of computer groups to which the user has access and authentication method. Administrators can edit user passwords, email addresses, and contact information.



Management: Users

1 row

User Name	Roles	Authentication Method
sa	Administrators	Password

Create User

User Name*	
Roles	□ Administrators
Computer Groups	No Computers
Authentication Method	Password
Password	
Password Confirmation	
Email Address	
Contact Information	

Important: Administrators need to select relevant roles for the user. User will be able to view/edit the reports and management menu based on the selected role. A user without any roles can only view reports under Security Configuration and has no access to the management menu (see Roles *(on page 26)* section).

Note: Administrators must assign appropriate Computer Group(s) to a user. A user can only view reports on the computers assigned to the user. A user without a computer assigned will not be able to login.

Authentication method can be chosen from one of followings:

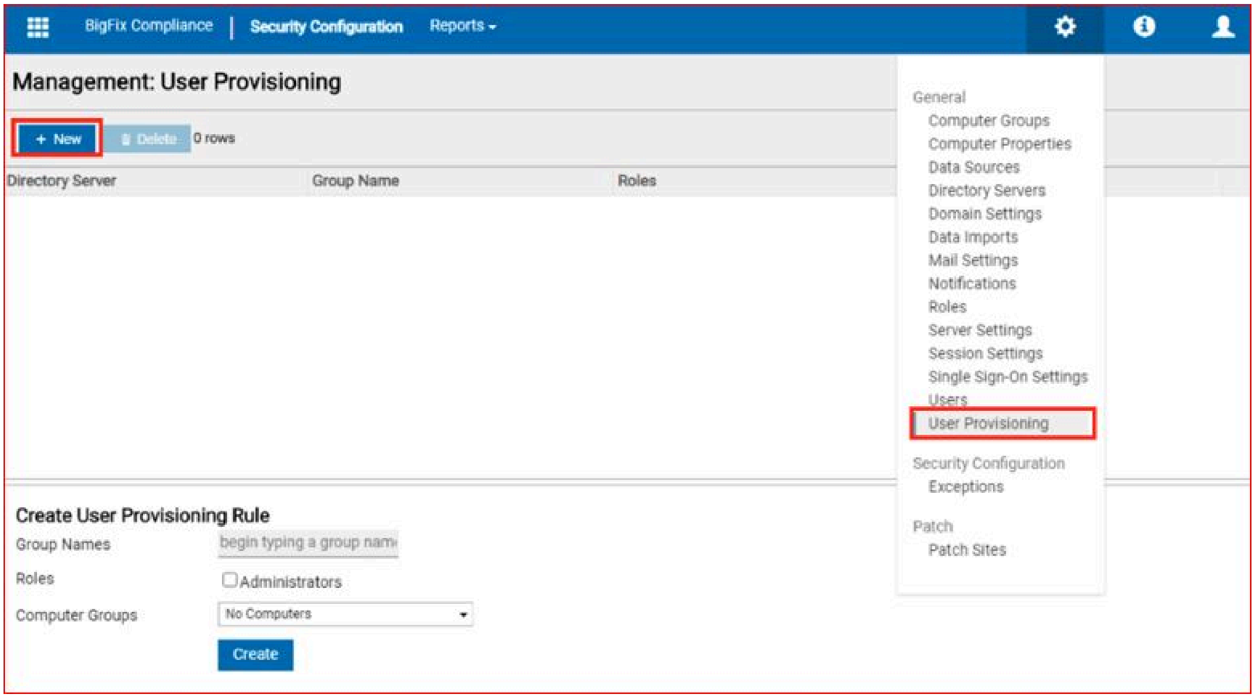
- Password
- WebReport (See Data Sources)
- Directory Server (See Directory Server)
- Single Sign-On (See Single Sign-On)

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.

You can set the Users account to configure multiple computer groups. To configure multiple groups, see Configuring multiple computer groups *(on page 18)*.

User Provisioning

Use the User Provisioning feature to automatically create a user with Directory Server authentication upon first-time login based on a rule that specifies which user group from Directory Server (LDAP group) the rule applies to, Roles, and Computer Group(s) to avoid creating users individually. However, this feature works only for the members of thea specified LDAP group and not applied to the members of the subgroups or the nested groups.



Management: User Provisioning

0 rows

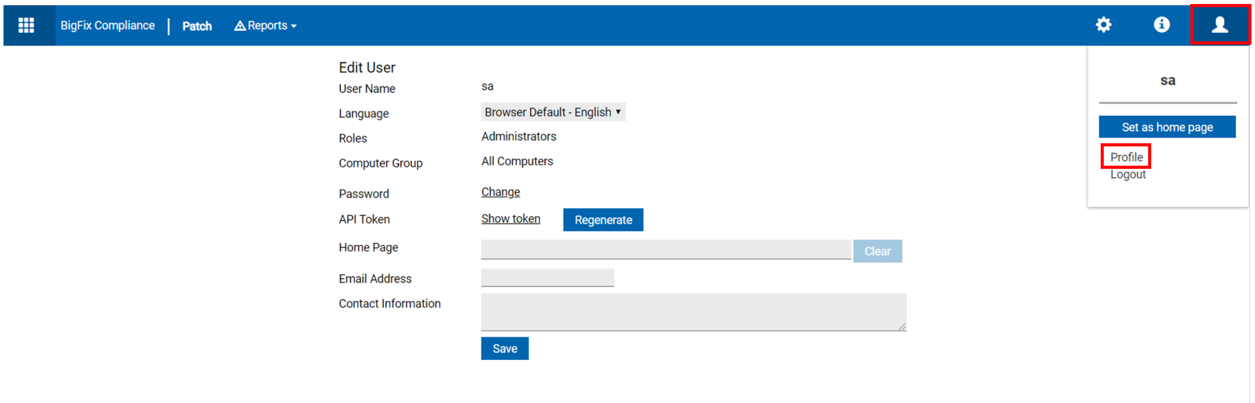
Directory Server	Group Name	Roles

Create User Provisioning Rule

Group Names	begin typing a group nam
Roles	□ Administrators
Computer Groups	No Computers

Account Preferences

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



Edit User

User Name	sa
Language	Browser Default - English
Roles	Administrators
Computer Group	All Computers
Password	Change
API Token	Show token
Home Page	
Email Address	
Contact Information	

Chapter 4. Security Configuration Reporting

For all the security and configuration checklists deployed across the entire environment using BigFix Compliance, BigFix Compliance Analytics provides various reports to show both current status and historic the trend for an individual endpoint, individual checklist, or even individual check. An aggregated compliance posture for the entire deployment is also provided to report the overall status and progress toward the desired security and configuration policies.

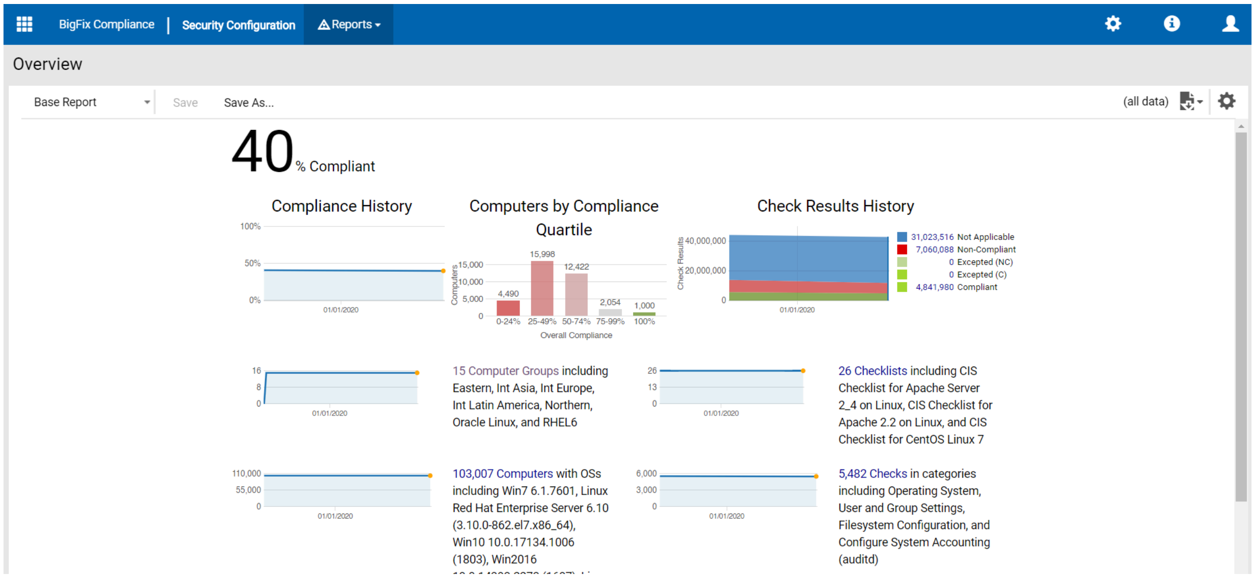
BigFix Compliance Analytics display graphical and tabular views of Security Configuration domain and different aspects of your deployment compliance status.

The following reports are available in Security Configuration domain:

- Policies
- Checklists
- Checks
- Computers
- Computer Groups
- Check Results
- Exception Results

Overview Report

The following graphical reports are available from the primary Overview window of the Security Configuration domain dashboard:



15 Computer Groups including Eastern, Int Asia, Int Europe, Int Latin America, Northern, Oracle Linux, and RHEL6

26 Checklists including CIS Checklist for Apache Server 2_4 on Linux, CIS Checklist for Apache 2.2 on Linux, and CIS Checklist for CentOS Linux 7

103,007 Computers with OSs including Win7 6.1.7601, Linux Red Hat Enterprise Server 6.10 (3.10.0-862.el7.x86_64), Win10 10.0.17134.1006 (1803), Win2016

5,482 Checks in categories including Operating System, User and Group Settings, Filesystem Configuration, and Configure System Accounting (auditd)

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

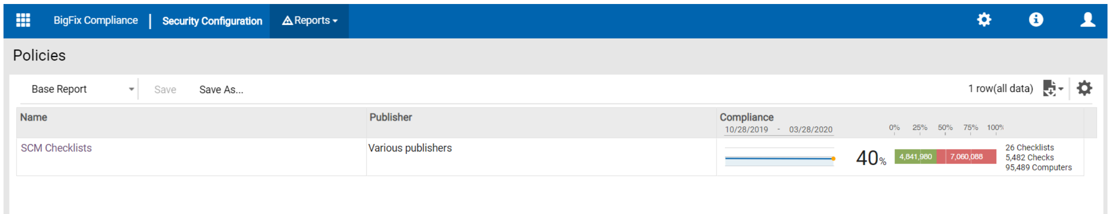
Shows information about a single check (such as check source and check description) and overall, historical aggregate compliance of the check as evaluated by all computers visible to logged in users.

Policies Report

Select Security Configuration domain using **Domains** and click **Reports** to find the following report:

Policies

Shows the list view of deployed policies, publisher details, description of the policies, and the overall, historical aggregate of the compliance results.

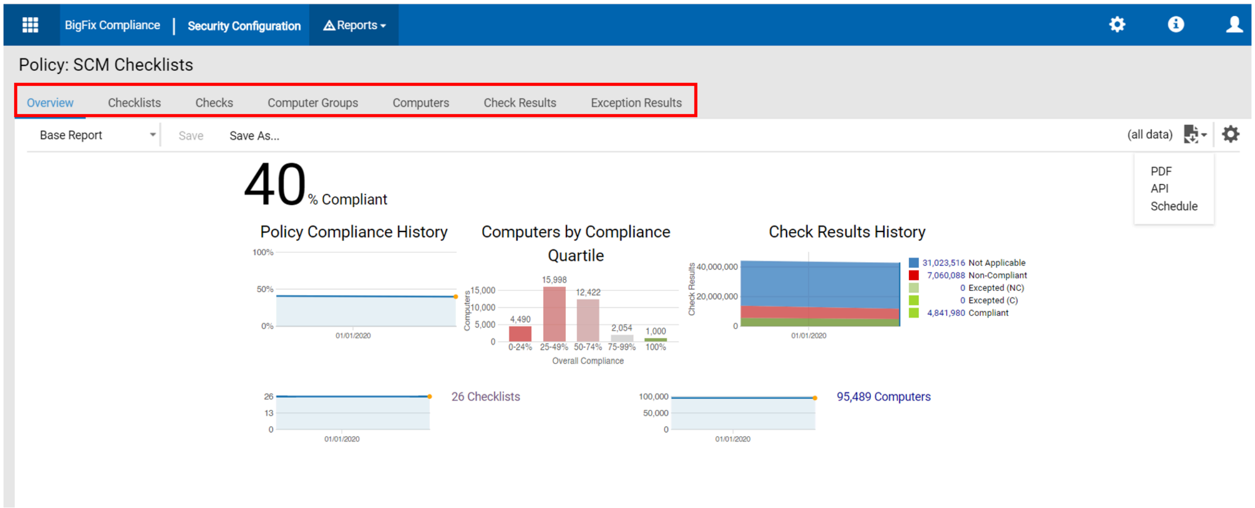


Policies

Name	Publisher	Compliance 10/28/2019 - 03/28/2020
SCM Checklists	Various publishers	40% 4,841,980 7,060,088 26 Checklists 5,482 Checks 95,489 Computers

Policy Overview Report

To access the Policy Overview report, click any policy that appears in the list view.



Policy Overview report

The Policy Overview report presents a graphical representation of the compliance history, computers by compliance quartile, and check results history with an overall compliance percentage shown in the top left corner of the console.

Policy Sub-Reports

To access the Policy sub-reports, click the Reports dropdown menu at the top of the console and select Policies. Click any policy that appears on the list view to open the sub-reports.

The sub-reports of the Policy report are Checklists, Checks, Computer Groups, Computers, Check Results and Exception Results.

Checklists

The Checklists sub-report contains a list of checklists and historical aggregate of the compliance results.

Checks

The Checks sub-report contains list of checks, desired values and historical aggregate of the compliance results.

Computer Groups

The Computer Groups sub-report contains list of computer groups and historical aggregate of the compliance results.

Computers

The Computers sub-report contains list of computers, last seen details and historical aggregate of the compliance results.

Check Results

The Check Results sub-report contains list of checklist, checks, computers, last seen details, and historical aggregate of the compliance results.

Exception Results

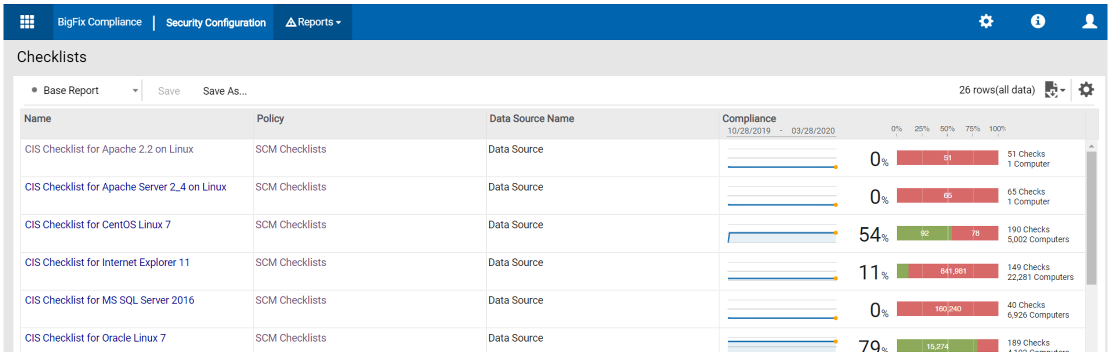
The Exception Results sub-report contains list of checklist, check name, computer name, last seen details, expiration date, reason and state.

Checklists Report

Select Security Configuration domain using **Domains** and click **Reports** to find the following report:

Checklists

Shows the list view of checklists, policy, data source name and the overall, historical aggregate of the compliance results.



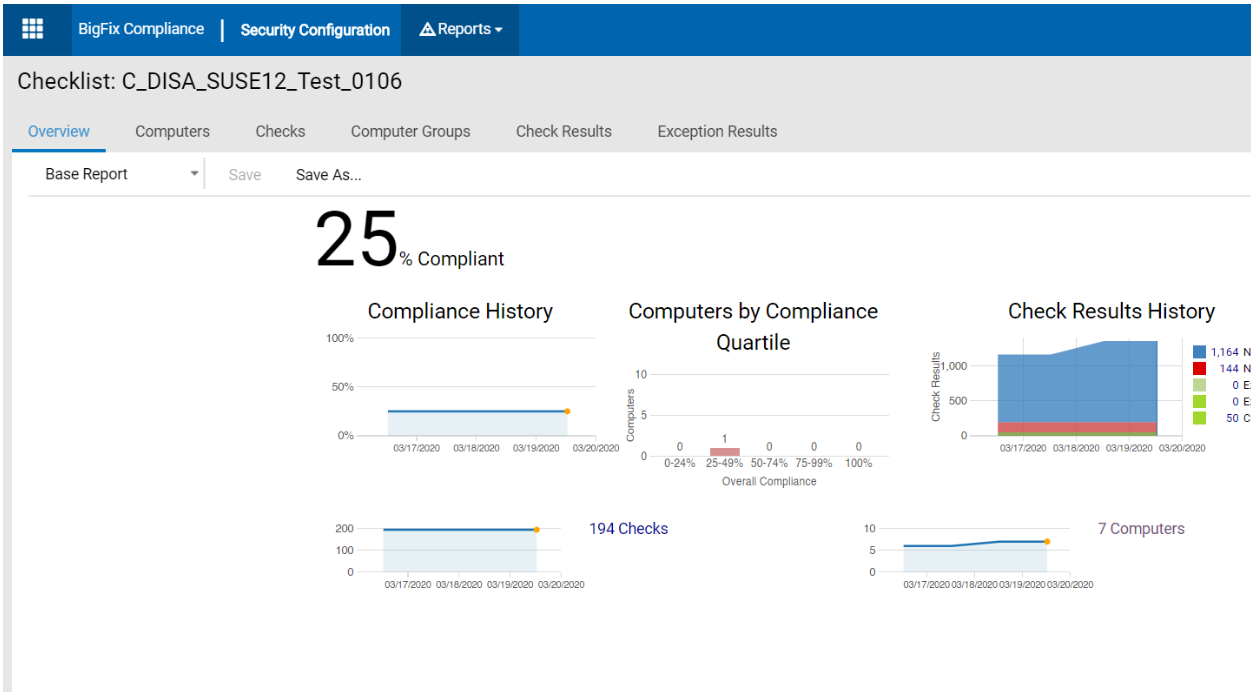
Checklists

26 rows(all data)

Name	Policy	Data Source Name	Compliance 10/28/2019 - 03/28/2020
CIS Checklist for Apache 2.2 on Linux	SCM Checklists	Data Source	0% 51 51 Checks 1 Computer
CIS Checklist for Apache Server 2_4 on Linux	SCM Checklists	Data Source	0% 65 65 Checks 1 Computer
CIS Checklist for CentOS Linux 7	SCM Checklists	Data Source	54% 92 78 190 Checks 5,002 Computers
CIS Checklist for Internet Explorer 11	SCM Checklists	Data Source	11% 841,981 149 Checks 22,281 Computers
CIS Checklist for MS SQL Server 2016	SCM Checklists	Data Source	0% 160,240 40 Checks 6,926 Computers
CIS Checklist for Oracle Linux 7	SCM Checklists	Data Source	79% 15,274 189 Checks

Checklist Overview Report

To access the Checklists Overview report, click any checklist that appears in the list view.



Checklist Overview report

The Checklist Overview report represents 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.

Checklist Sub-Reports

To access the Checklists sub-reports, click the Reports dropdown menu at the top of the console and select Checklists. Click any checklist that appears on the list to open the sub-reports.

The sub-reports of the Checklist report are Computers, Checks, Computer Groups, Check Results and Exception Results.

Computers

The Computers sub-report contains list of computers, last seen details and historical aggregate of the compliance results.

Checks

The Checks sub-report contains list of checks, desired values and historical aggregate of the compliance results.

Computer Groups

The Computer Groups sub-report contains list of computer groups and historical aggregate of the compliance results.

Check Results

The Check Results sub-report contains list of checks, computers, last seen details, and historical aggregate of the compliance results.

Checks Report

Select Security Configuration domain using **Domains** and click **Reports** to find the following report:

Checks

Shows the detailed view of various checks, their descriptions, desired values, and the overall, historical aggregate of the compliance results.

Columns

Name:

This section lists all the checks by their names. Each check represents a specific criterion or setting that must undergo validation to ensure compliance with security standards.

Description:

This part provides a detailed explanation of what each check entails. It includes the specific details of what the check monitors or evaluates within the system.

Desired Values:

1. Each check has a 'desired value' which represents the expected or compliant state for that check.
2. The desired value can be of different types such as integer, string, or none.
3. It is important to note that not all checks have a designated desired value. If a check does not have a desired value, it implies that it is not modifiable, and its value will be shown as <none> or none.
4. Checks with desired values can be configured to meet different requirements.

This part provides a detailed explanation of what each check entails. It includes the specific details of what the check monitors or evaluates within the system.

Compliance Results:

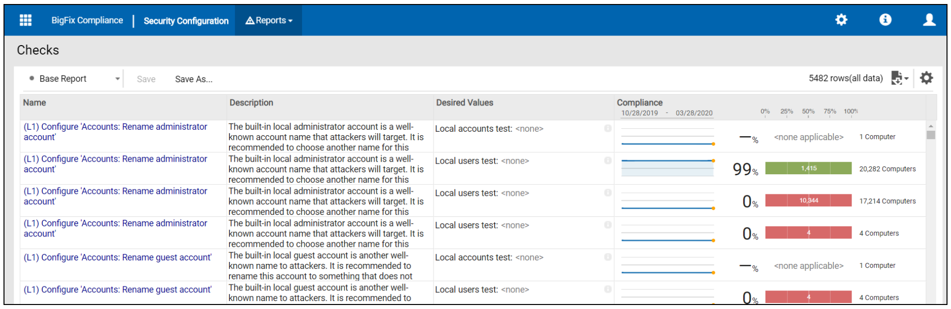
This shows the historical cumulative data depicting how the systems have adhered to each check over a period of time.

Note: The values from both the BigFix Console and CIS Benchmarks, including their desired states, can be retrieved and, if configurable, modified through the BigFix console.

Note: CIS benchmark documents are accessible in the console via fixlet descriptions of each check.

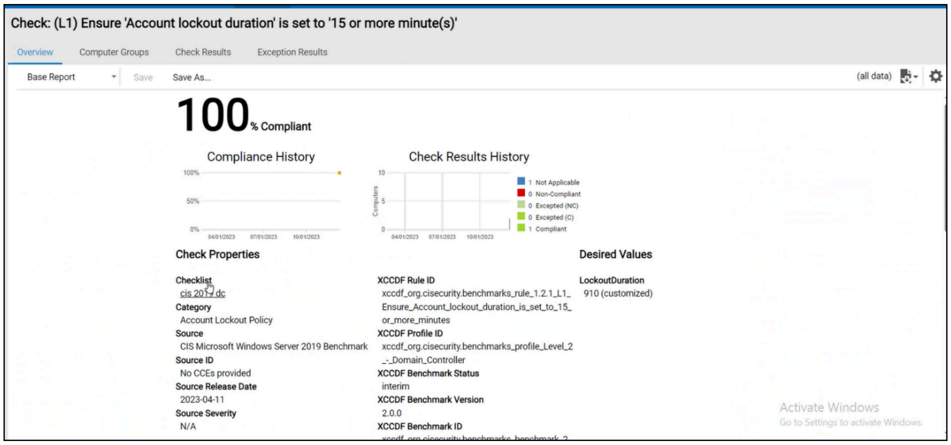
Note: The desired value is customer-defined, while the default value aligns with CIS recommendations.

Figure 1. Sample of Check Report from Security Configuration Domain



Name	Description	Desired Values	Compliance 10/28/2019 - 03/28/2020			
(L1) Configure 'Accounts: Rename administrator account'	The built-in local administrator account is a well-known account name that attackers will target. It is recommended to choose another name for this	Local accounts test: <none>		—%	<none applicable>	1 Computer
(L1) Configure 'Accounts: Rename administrator account'	The built-in local administrator account is a well-known account name that attackers will target. It is recommended to choose another name for this	Local users test: <none>		99%	1,415	20,282 Computers
(L1) Configure 'Accounts: Rename administrator account'	The built-in local administrator account is a well-known account name that attackers will target. It is recommended to choose another name for this	Local users test: <none>		0%	10,344	17,214 Computers
(L1) Configure 'Accounts: Rename administrator account'	The built-in local administrator account is a well-known account name that attackers will target. It is recommended to choose another name for this	Local users test: <none>		0%	4	4 Computers
(L1) Configure 'Accounts: Rename guest account'	The built-in local guest account is another well-known name to attackers. It is recommended to rename this account to something that does not	Local accounts test: <none>		—%	<none applicable>	1 Computer
(L1) Configure 'Accounts: Rename guest account'	The built-in local guest account is another well-known name to attackers. It is recommended to	Local users test: <none>		0%	4	4 Computers

Figure 2. Check with customized Desired Value



Check: (L1) Ensure 'Account lockout duration' is set to '15 or more minute(s)'

100% Compliant

- 🟦 1 Not Applicable
- 🟥 0 Non-Compliant
- 🟩 0 Excepted (NC)
- 🟩 0 Excepted (C)
- 🟩 1 Compliant

Check Properties

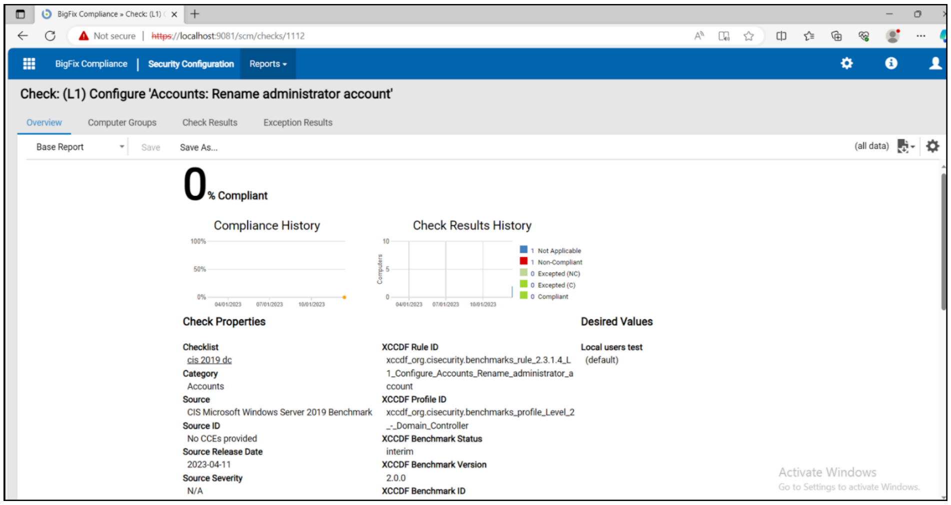
Checklist
cis 2019 dc
Category
Account Lockout Policy
Source
CIS Microsoft Windows Server 2019 Benchmark
Source ID
No CCEs provided
Source Release Date
2023-04-11
Source Severity
N/A

XCCDF Rule ID
xccdf_org.cisecurity.benchmarks_rule_1.2.1_L1_Ensure_Account_lockout_duration_is_set_to_15_or_more_minutes
XCCDF Profile ID
xccdf_org.cisecurity.benchmarks_profile_Level_2_-_Domain_Controller
XCCDF Benchmark Status
interim
XCCDF Benchmark Version
2.0.0
XCCDF Benchmark ID
xccdf_org.cisecurity.benchmarks_benchmark_2

Desired Values

LockoutDuration
910 (customized)

Figure 3. Check with no default Desired Value



Check: (L1) Configure 'Accounts: Rename administrator account'

0% Compliant

Check Properties

Checklist
cis 2019 dc
Category
Accounts
Source
CIS Microsoft Windows Server 2019 Benchmark
Source ID
No CCEs provided
Source Release Date
2023-04-11
Source Severity
N/A

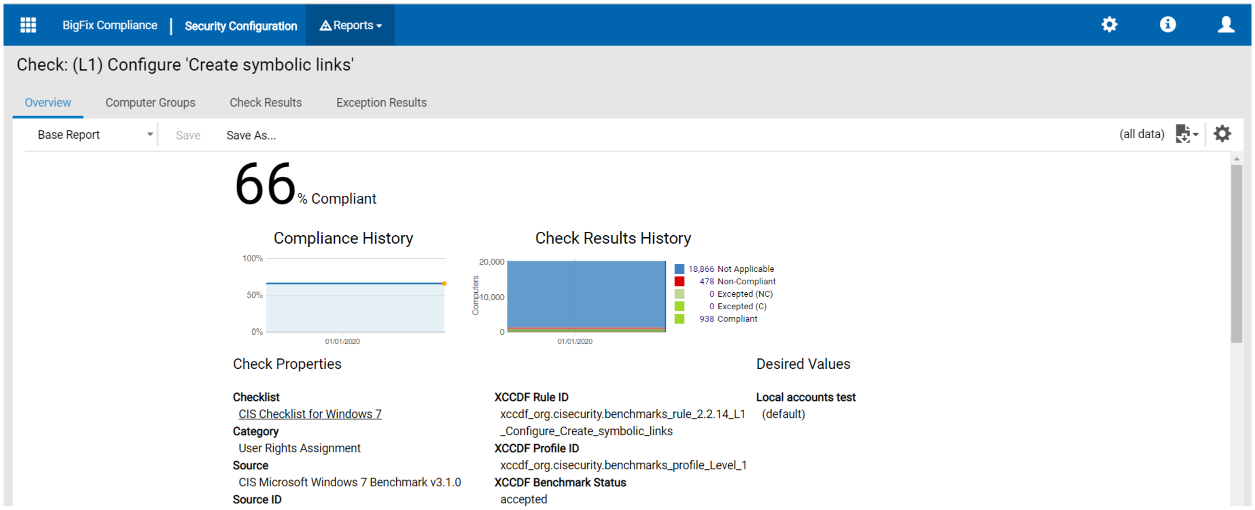
XCCDF Rule ID
xccdf_org.cisecurity.benchmarks_rule_2.3.1.4_L1_Configure_Accounts_Rename_administrator_account
XCCDF Profile ID
xccdf_org.cisecurity.benchmarks_profile_Level_2_-_Domain_Controller
XCCDF Benchmark Status
interim
XCCDF Benchmark Version
2.0.0
XCCDF Benchmark ID

Desired Values

Local users test
(default)

Check Overview Report

To access the Check Overview report, click any check that appears in the list view.



Check: (L1) Configure 'Create symbolic links'

66% Compliant

Check Properties

Checklist
CIS Checklist for Windows 7
Category
User Rights Assignment
Source
CIS Microsoft Windows 7 Benchmark v3.1.0
Source ID

XCCDF Rule ID
xccdf_org.cisecurity.benchmarks_rule_2.2.14_L1_Configure_Create_symbolic_links
XCCDF Profile ID
xccdf_org.cisecurity.benchmarks_profile_Level_1
XCCDF Benchmark Status
accepted

Desired Values

Local accounts test
(default)

Check Overview report

The Check Overview report represents a graphic representation of compliance history, check properties, and check results history with an overall compliance percentage shown in the top left corner of the console.

Check Sub-Reports

To access the Checks sub-reports, click the Reports dropdown menu at the top of the console and select Checks. Click any check that appears on the list to open the sub-reports.

The sub-reports of the Check report are Computer Groups, Check Results and Exception Results.

Computer Groups

The Computer Groups sub-report contains list of computer groups and historical aggregate of the compliance results.

Check Results

The Check Results sub-report contains list of checks, computers, last seen details, and historical aggregate of the compliance results.

Exception Results

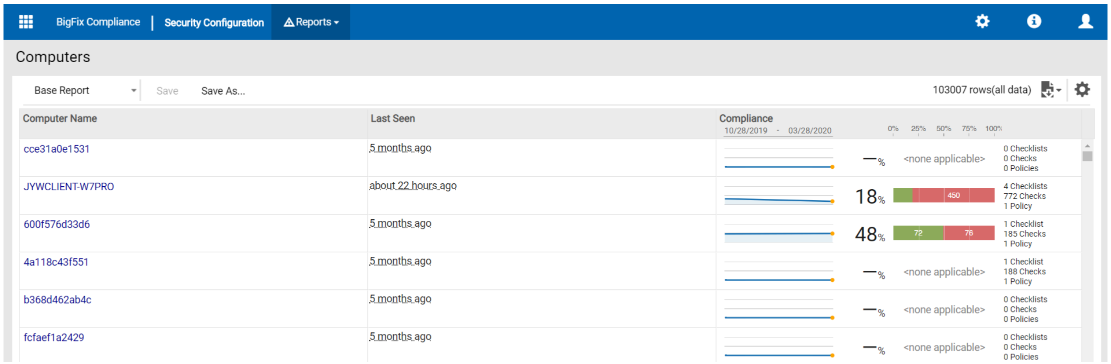
The Exception Results sub-report contains list of computers, last seen details, expiration date, reason and state.

Computers Report

Select Security Configuration domain using **Domains** and click **Reports** to find the following report:

Computers

Shows the list view of computers, last seen and the overall, historical aggregate of the compliance results.



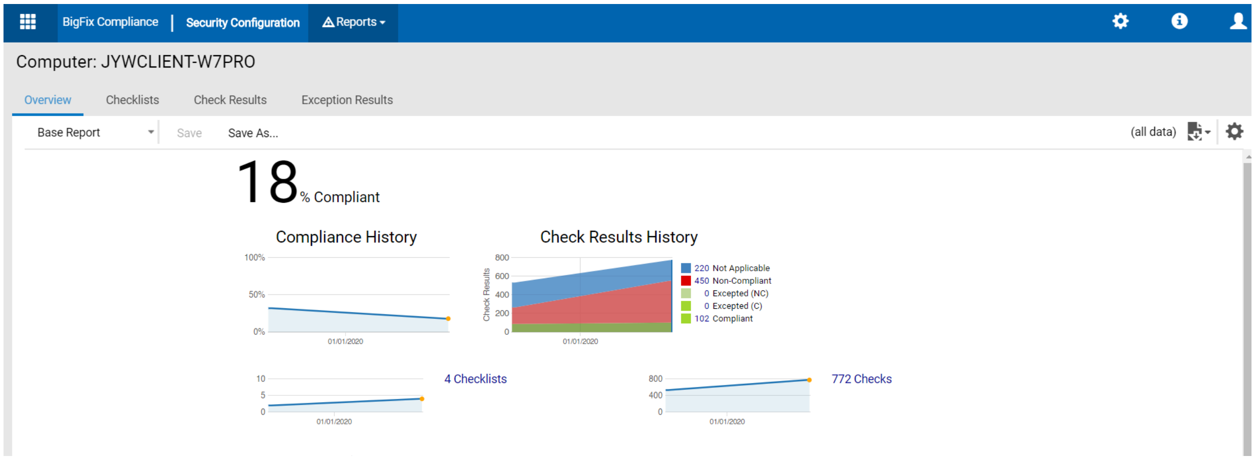
Computers

103007 rows(all data)

Computer Name	Last Seen	Compliance 10/28/2019 - 03/28/2020	0% 25% 50% 75% 100%	
cce31a0e1531	5 months ago	—%	<none applicable>	0 Checklists 0 Checks 0 Policies
JYWCLIENT-W7PRO	about 22 hours ago	18%	450	4 Checklists 772 Checks 1 Policy
600f576d33d6	5 months ago	48%	72 76	1 Checklist 185 Checks 1 Policy
4a118c43f551	5 months ago	—%	<none applicable>	1 Checklist 188 Checks 1 Policy
b368d462ab4c	5 months ago	—%	<none applicable>	0 Checklists 0 Checks 0 Policies
fcfaef1a2429	5 months ago	—%	<none applicable>	0 Checklists 0 Checks 0 Policies

Computer Overview Report

To access the Computer Overview report, click any computer that appears in the list view.



Computer Overview report

The Computer Overview report represents a graphic representation of compliance history, computer properties, and check results history with an overall compliance percentage shown in the top left corner of the console.

Computer Sub-Reports

To access the Computer sub-reports, click the Reports dropdown menu at the top of the console and select Computers. Click any computer that appears on the list to open the sub-reports.

The sub-reports of the Computer report are Checklists, Check Results and Exception Results.

Checklists

The Checklists sub-report contains a list of checklists and historical aggregate of the compliance results.

Check Results

The Check Results sub-report contains list of checklist, checks, and historical aggregate of the compliance results.

Exception Results

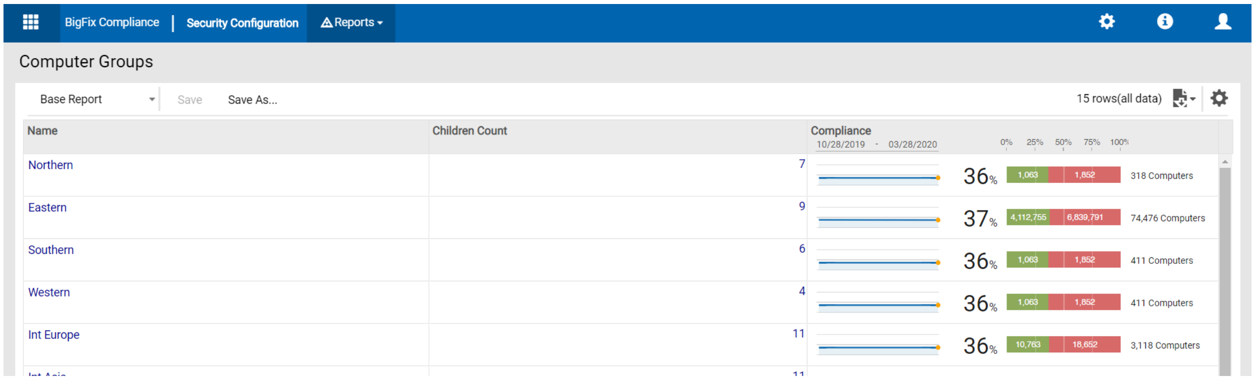
The Exception Results sub-report contains list of checklist, checks, expiration date, reason and state.

Computer Groups Report

Select Security Configuration domain using **Domains** and click **Reports** to find the following report:

Computer Groups

Shows the list view of computer groups, sub-groups (children) and the overall, historical aggregate of the compliance results.

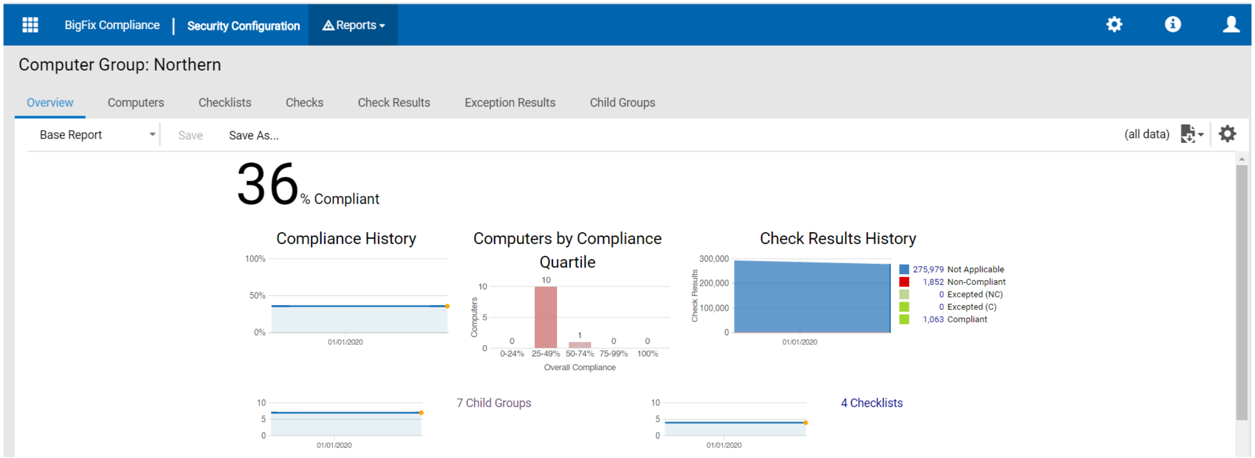


Computer Groups

Name	Children Count	Compliance 10/28/2019 - 03/28/2020			
Northern	7	36%	1,063	1,852	318 Computers
Eastern	9	37%	4,112,755	6,839,791	74,476 Computers
Southern	6	36%	1,063	1,852	411 Computers
Western	4	36%	1,063	1,852	411 Computers
Int Europe	11	36%	10,763	18,652	3,118 Computers
Int Asia	11				

Computer Group Overview Report

To access the Computer Groups Overview report, click any computer group that appears in the list view.



Computer Group: Northern

36% Compliant

🟦 275,979	Not Applicable
🟥 1,852	Non-Compliant
🟩 0	Excepted (NC)
🟩 0	Excepted (C)
🟩 1,063	Compliant

7 Child Groups

4 Checklists

Computer Group Overview report

The Computer Group Overview report represents a graphic representation of compliance history, computers by compliance quartile, child groups, checklists and check results history with an overall compliance percentage shown in the top left corner of the console.

Computer Group Sub-Reports

To access the Computer Groups sub-reports, click the Reports dropdown menu at the top of the console and select Computer Groups. Click any computer group that appears on the list to open the sub-reports.

The sub-reports of the Computer Group report are Computers, Checklists, Checks, Check Results, Exception Results and Child Groups.

Computers

The Computers sub-report contains list of computers, last seen details and historical aggregate of the compliance results.

Checklists

The Checklists sub-report contains a list of checklists and historical aggregate of the compliance results.

Checks

The Checks sub-report contains list of checks, desired values and historical aggregate of the compliance results.

Check Results

The Check Results sub-report contains list of checklist, checks, computers, last seen details, and historical aggregate of the compliance results.

Exception Results

The Exception Results sub-report contains list of checklist, check name, computer name, last seen details, expiration date, reason and state.

Child Groups

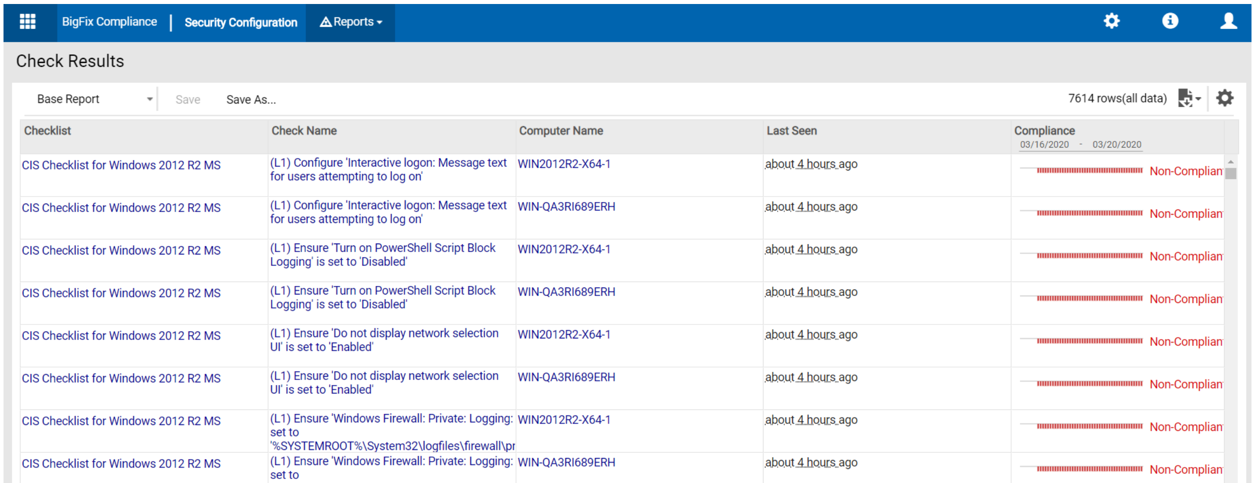
The Child Groups sub-report contains list of computer group, children count, and and historical aggregate of the compliance results.

Check Results Report

Select Security Configuration domain using **Domains** and click **Reports** to find the following report:

Check Results

Shows the list view of checklist, check name, computer name, last seen, and the overall, historical aggregate of the compliance results.



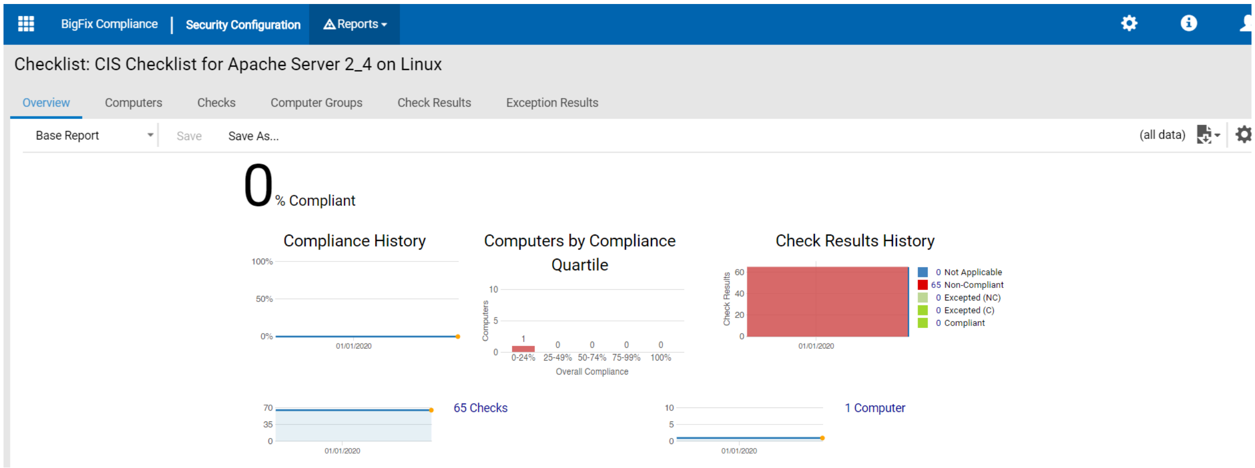
Check Results

7614 rows(all data)

Checklist	Check Name	Computer Name	Last Seen	Compliance 03/16/2020 - 03/20/2020
CIS Checklist for Windows 2012 R2 MS	(L1) Configure 'Interactive logon: Message text for users attempting to log on'	WIN2012R2-X64-1	about 4 hours ago	Non-Complian
CIS Checklist for Windows 2012 R2 MS	(L1) Configure 'Interactive logon: Message text for users attempting to log on'	WIN-QA3RI689ERH	about 4 hours ago	Non-Complian
CIS Checklist for Windows 2012 R2 MS	(L1) Ensure 'Turn on PowerShell Script Block Logging' is set to 'Disabled'	WIN2012R2-X64-1	about 4 hours ago	Non-Complian
CIS Checklist for Windows 2012 R2 MS	(L1) Ensure 'Turn on PowerShell Script Block Logging' is set to 'Disabled'	WIN-QA3RI689ERH	about 4 hours ago	Non-Complian
CIS Checklist for Windows 2012 R2 MS	(L1) Ensure 'Do not display network selection UI' is set to 'Enabled'	WIN2012R2-X64-1	about 4 hours ago	Non-Complian
CIS Checklist for Windows 2012 R2 MS	(L1) Ensure 'Do not display network selection UI' is set to 'Enabled'	WIN-QA3RI689ERH	about 4 hours ago	Non-Complian
CIS Checklist for Windows 2012 R2 MS	(L1) Ensure 'Windows Firewall: Private: Logging: set to '%SYSTEMROOT%\System32\logfiles\firewall\pr	WIN2012R2-X64-1	about 4 hours ago	Non-Complian
CIS Checklist for Windows 2012 R2 MS	(L1) Ensure 'Windows Firewall: Private: Logging: set to	WIN-QA3RI689ERH	about 4 hours ago	Non-Complian

Check Results Overview Report

To access the Check Results Overview report, click any checklist that appears in the list view..



Checklist: CIS Checklist for Apache Server 2_4 on Linux

0 % Compliant

Checklist Overview report

The Checklist Overview report represents a graphic representation of compliance history, computers by compliance quartile, checklists, computer and check results history with an overall compliance percentage shown in the top left corner of the console.

Check Results Sub-Report

To access the Check Results sub-reports, click the Reports dropdown menu at the top of the console and select Check Results. Click any checklist that appears on the list to open the sub-reports..

The sub-reports of the Check Results report are Computers, Checks, Computer Groups, Check Results and Exception Results.

Computers

The Computers sub-report contains list of computers, last seen details and historical aggregate of the compliance results.

Checks

The Checks sub-report contains list of checks, desired values and historical aggregate of the compliance results.

Computer Groups

The Computer Groups sub-report contains list of computer groups and historical aggregate of the compliance results.

Check Results

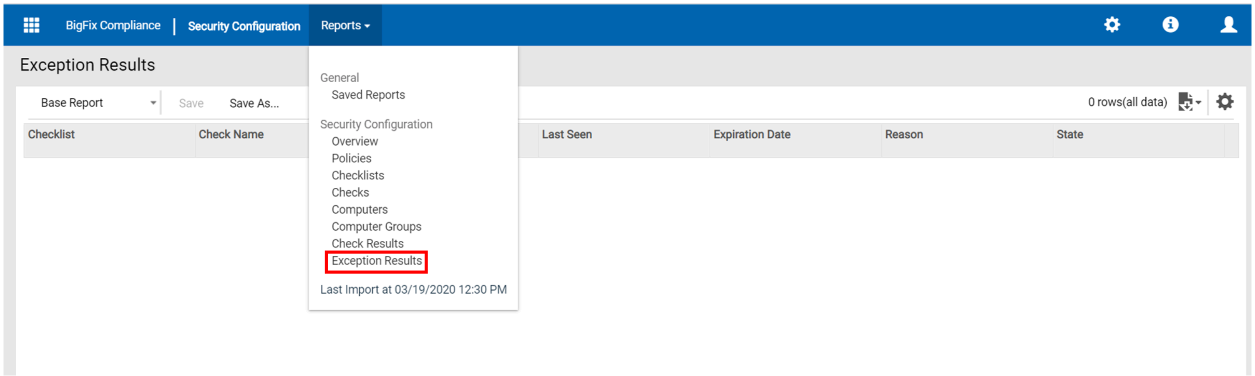
The Check Results sub-report contains list of checklist, checks, computers, last seen details, and historical aggregate of the compliance results.

Exception Results

The Exception Results sub-report contains list of checklist, check name, computer name, last seen details, expiration date, reason and state.

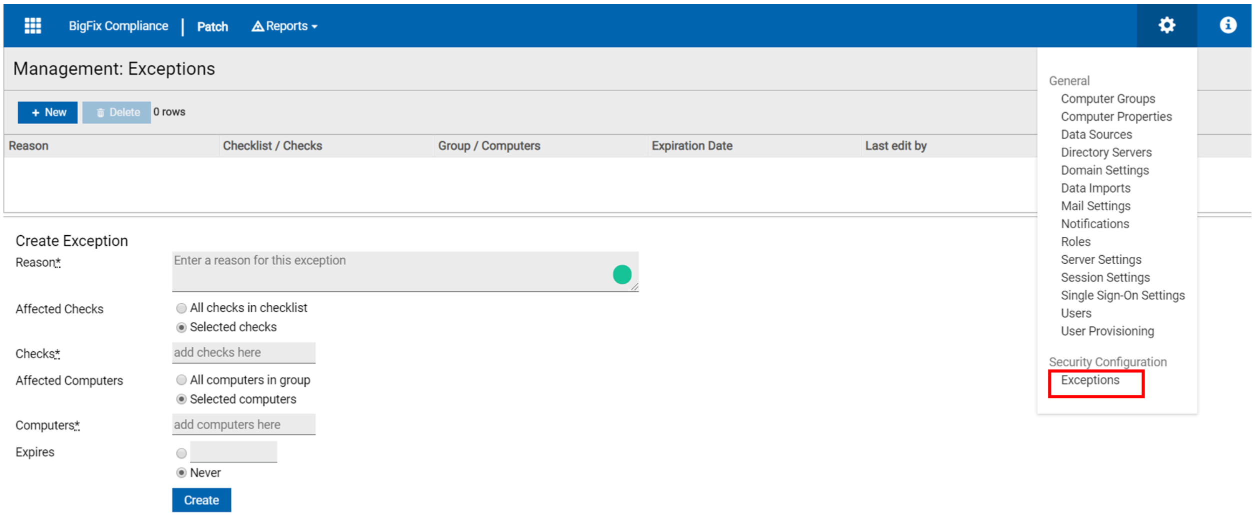
Exception Results report

The Exception Reults report shows the list view of checklist, check name, last seen, expiration date reason, and state.



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.



Chapter 5. Patch Domain

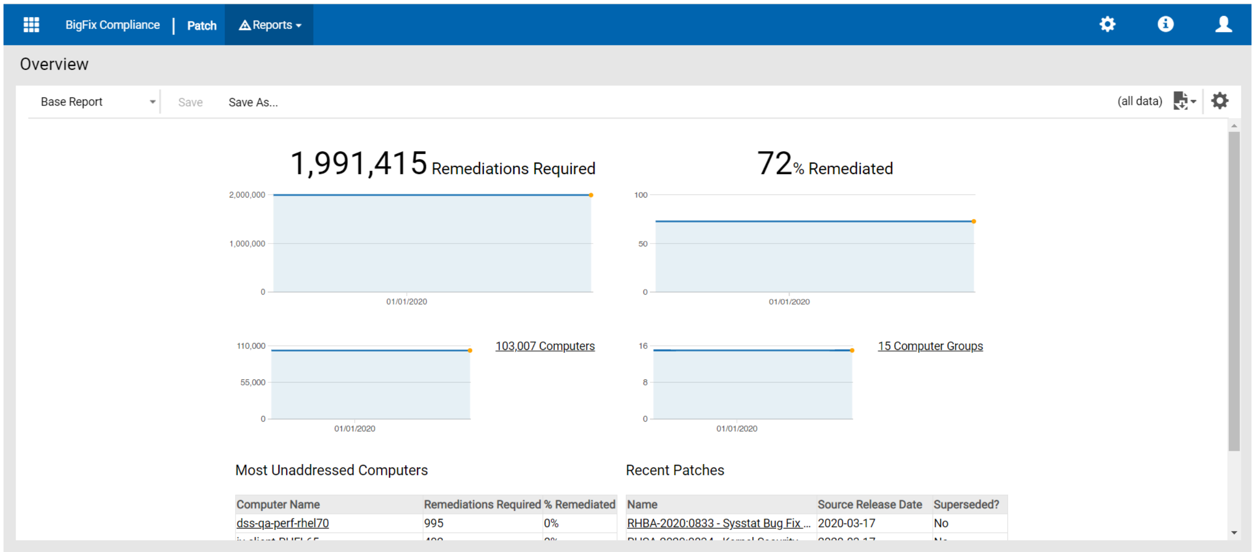
Patch report extends the analytics and reporting capabilities of BigFix Compliance from security configuration to security patching. This feature allows you to gain a comprehensive and historical view of patching activities across the entire deployment to assess the overall patching posture. It enables more efficient prioritization of vulnerability remediation by identifying the critical and high severity patches that have to be applied. It also tracks when a new patch is released by the vendors and applies to each endpoint to help you demonstrate compliance with regulations or policies and pass the audits

BigFix Patch domain report is a component of BigFix Compliance Analytics. The patch domain report has a different category of reports like Overview, Patches, Computers, Computer Groups, and Unsupported Computers. The generated reports can be filtered, sorted, grouped, customized, or exported by using various tools.

Prerequisites: You have to enable patch reporting to import the patch data. To enable the patch reports, see Domain Settings *(on page 20)*.

Overview Report

The following graphical reports are available from the primary Overview window of the Patch domain dashboard:



Most Unaddressed Computers

Computer Name	Remediations Required	% Remediated
dss-qa-perf-rhel70	995	0%

Recent Patches

Name	Source Release Date	Superseded?
RHBA-2020:0833 - Sysstat Bug Fix ...	2020-03-17	No

Deployment Overview

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

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 Unaddressed Computers Overview

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

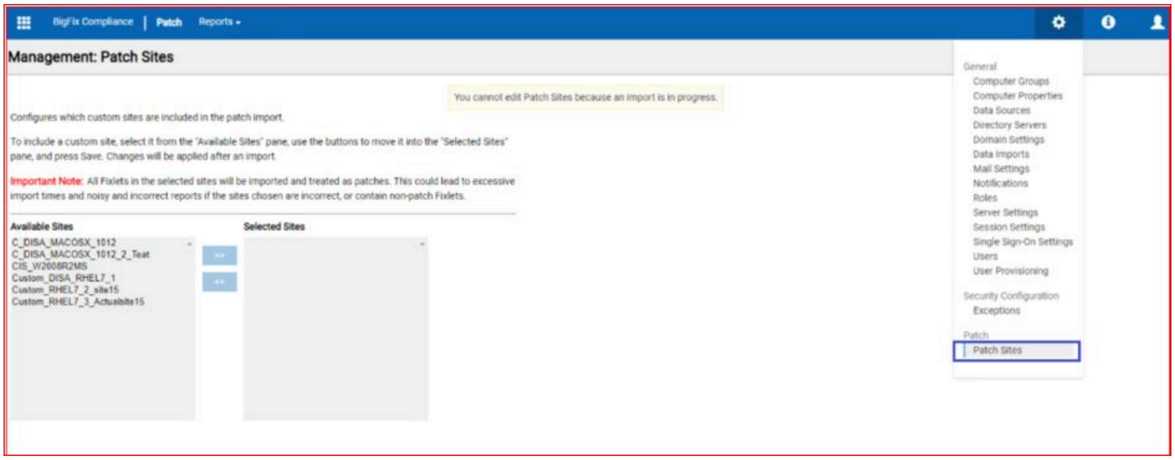
Recent Patch Overview

Displays the list of the most recently available patches

Custom Patch Sites

Out of the box, Patch and Vulnerability Reporting uses data from the supported external patch sites. Starting with version 2.0.1, user with the "Edit Patch Sites" permission can configure Compliance to include specified custom sites.

1. Click the gear icon in the management page and click **Patch Sites**.



Management: Patch Sites

You cannot edit Patch Sites because an import is in progress.

Configures which custom sites are included in the patch import.

To include a custom site, select it from the "Available Sites" pane, use the buttons to move it into the "Selected Sites" pane, and press Save. Changes will be applied after an import.

Important Note: All Fixlets in the selected sites will be imported and treated as patches. This could lead to excessive import times and noisy and incorrect reports if the sites chosen are incorrect, or contain non-patch Fixlets.

Available Sites

C_DISA_MACOSX_1012
C_DISA_MACOSX_1012_2_Test
CIS_W2008R2MS
Custom_DISA_RHEL7_1
Custom_RHEL7_2_site15
Custom_RHEL7_3_Actualsite15

Selected Sites

2. Select and move sites from the **Available Sites** list into the **Selected Sites** list.
3. After confirming the changes, click **Save**. Subsequent imports include the selected sites in reports.

   Custom site patches are reported as normal with the external site patches. However, the important distinction is that the custom site patches cannot be superseded. Any patch that originates from a custom site is treated as non-superseded. This means that the vulnerabilities associated with the patch through its superseded patches cannot be included in the related vulnerabilities. If you want to associate a patch with additional vulnerabilities, the patch must be amended to include the additional CVEs in the CVENames or MIME_x-fixlet-cve fields.

   Ensure that the patch has working relevance. If the patch was copied from a Windows site, any relevance that disables evaluation including *false* relevance and relevance that checks for the **EnableSuperseedEval** client setting must be removed.

EnableSupersededEval

In normal conditions, superseded patch fixlets have their relevance always evaluated to `not relevant`. This freezes the ETL logic for `PR::PatchResult` to the previous patch results or to return unknown status when a patch fixlet becomes superseded. In a client setting when `BESClient_WindowsOS_EnableSupersededEval` is set to 1, the superseded patch fixlet do not auto evaluate to `not relevant`.

If patch_a that addresses vuln_x and is superseded by patch_b which also addresses vuln_y.

Unpatched computer with setting enabled.

Scenario A: When the computer applies patch_a

patch_a result in console: not relevant

patch_a result in sca: not applied

patch_b result in console: relevant

patch_b result in sca: not applied

vuln_x result in sca: vulnerable

vuln_y result in sca: vulnerable

By applying the superseded fixlet, from both patch results view and vulnerability results view, Compliance becomes incorrect.

Scenario B: When the computer applies patch_b

patch_a result in console: not relevant

patch_a result in sca: not applied

patch_b result in console: not relevant

patch_b result in sca: applied

vuln_x result in sca: not vulnerable

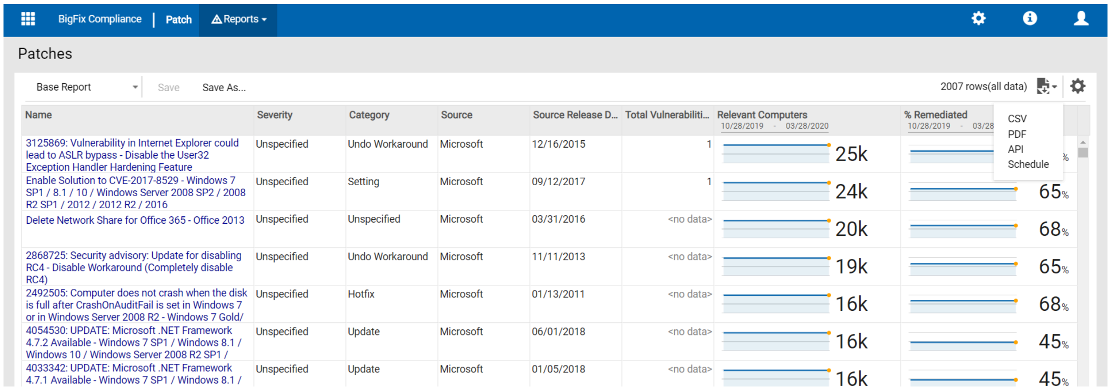
vuln_y result in sca: not vulnerable

Patches Report

Select Patches domain using **Domains** and click **Reports** to find the following report:

Patches

Shows the list view of patches, severity, category, source, source release date, total vulnerability, relevant computers, and % remediated.



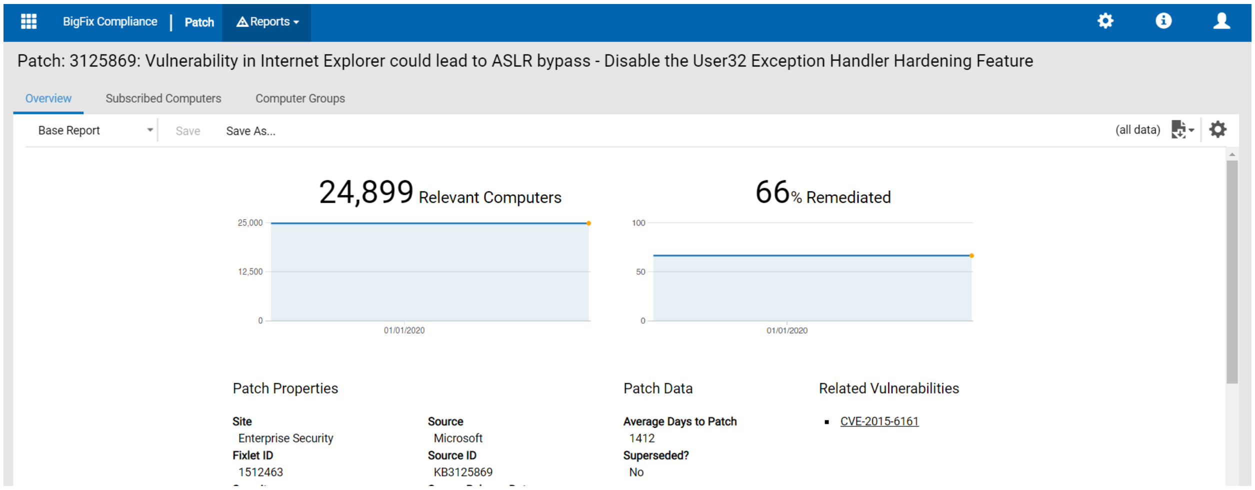
Patches

2007 rows(all data)

Name	Severity	Category	Source	Source Release D...	Total Vulnerabiliti...	Relevant Computers 10/28/2019 - 03/28/2020	% Remediated 10/28/2019 - 03/28
3125869: Vulnerability in Internet Explorer could lead to ASLR bypass - Disable the User32 Exception Handler Hardening Feature	Unspecified	Undo Workaround	Microsoft	12/16/2015	1	25k	%
Enable Solution to CVE-2017-8529 - Windows 7 SP1 / 8.1 / 10 / Windows Server 2008 SP2 / 2008 R2 SP1 / 2012 / 2012 R2 / 2016	Unspecified	Setting	Microsoft	09/12/2017	1	24k	65%
Delete Network Share for Office 365 - Office 2013	Unspecified	Unspecified	Microsoft	03/31/2016	<no data>	20k	68%
2868725: Security advisory: Update for disabling RC4 - Disable Workaround (Completely disable RC4)	Unspecified	Undo Workaround	Microsoft	11/11/2013	<no data>	19k	65%
2492505: Computer does not crash when the disk is full after CrashOnAuditFail is set in Windows 7 or in Windows Server 2008 R2 - Windows 7 Gold/	Unspecified	Hotfix	Microsoft	01/13/2011	<no data>	16k	68%
4054530: UPDATE: Microsoft .NET Framework 4.7.2 Available - Windows 7 SP1 / Windows 8.1 / Windows 10 / Windows Server 2008 R2 SP1 /	Unspecified	Update	Microsoft	06/01/2018	<no data>	16k	45%
4033342: UPDATE: Microsoft .NET Framework 4.7.1 Available - Windows 7 SP1 / Windows 8.1 /	Unspecified	Update	Microsoft	01/05/2018	<no data>	16k	45%

Patch overview Report

To access the Patches Overview report, click any patch that appears in the list view.



Patch: 3125869: Vulnerability in Internet Explorer could lead to ASLR bypass - Disable the User32 Exception Handler Hardening Feature

(all data)

24,899 Relevant Computers

66% Remediated

Patch Properties

Site
Enterprise Security
Fixlet ID
1512463

Source
Microsoft
Source ID
KB3125869

Patch Data

Average Days to Patch
1412
Superseded?
No

Related Vulnerabilities

- CVE-2015-6161

Patch Overview report

The Patch Overview report represents a graphical representation of the relevant computers, %remediated, patch properties, patch data and related vulnerabilities.

Patch Sub-Reports

To access the Patches sub-reports, click the Reports dropdown menu at the top of the console and select Patches. Click any patches that appears on the list to open the sub-reports.

The sub-reports of the Patch report are Subscribed Computers and Computer Groups.

Subscribed Computers

The Subscribed Computers sub-report contains list of computers, last seen details and remediated status.

Computer Groups

The Computer Groups sub-report contains list of computer groups, computer count, relevant computers, and % remediated.

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. Edit the `custom_patch_sites.json` and add the missing sites ID.
6. Start the BigFix Compliance service.
7. 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 1. Supported Sites

Site name	URL	Notes
Patches for Windows English	http://sync.bigfix.com/cgi-bin/bf-gather/bessecurity	No

Table 1. Supported Sites (continued)

Site name	URL	Notes
Patches for Windows (Brazilian Portuguese)	http://sync.bigfix.com/cgi-bin/bfgather/windowspatchesbrazilianportuguese	No
Patches for Windows (Czech)	http://sync.bigfix.com/cgi-bin/bfgather/windowspatchesczech	No
Patches for Windows (NLD)	http://sync.bigfix.com/cgi-bin/bfgather/windowspatchesnld	No
Patches for Windows (Finnish)	http://sync.bigfix.com/cgi-bin/bfgather/windowspatchesfinnish	No
Patches for Windows (French)	http://sync.bigfix.com/cgi-bin/bfgather/windowspatchesfrench	No
Patches for Windows (German)	http://sync.bigfix.com/cgi-bin/bfgather/windowspatchesgerman	No
Patches for Windows (Hungarian)	http://sync.bigfix.com/cgi-bin/bfgather/windowspatcheshungarian	No
Patches for Windows (Italian)	http://sync.bigfix.com/cgi-bin/bfgather/windowspatchesitalian	No
Patches for Windows (Japanese)	http://sync.bigfix.com/cgi-bin/bfgather/windowspatchesjapanese	No
Patches for Windows (Korean)	http://sync.bigfix.com/cgi-bin/bfgather/windowspatcheskorean	No
Patches for Windows (Norwegian)	http://sync.bigfix.com/cgi-bin/bfgather/windowspatchesnorwegian	No
Patches for Windows (Polish)	http://sync.bigfix.com/cgi-bin/bfgather/windowspatchespolish	No
Patches for Windows (Simplified Chinese)	http://sync.bigfix.com/cgi-bin/bfgather/windowspatcheschineses	No
Patches for Windows (Spanish)	http://sync.bigfix.com/cgi-bin/bfgather/windowspatchesspanish	No
Patches for Windows (Swedish)	http://sync.bigfix.com/cgi-bin/bfgather/windowspatchesswedish	No

Table 1. Supported Sites (continued)

Site name	URL	Notes
Patches for Windows (Turkish)	http://sync.bigfix.com/cgi-bin/bf-gather/windowspatchesturkish	No
Patches for Windows (CHT)	http://sync.bigfix.com/cgi-bin/bf-gather/windowspatchescht	No
Patches for Windows (Russian)	http://sync.bigfix.com/cgi-bin/bf-gather/windowspatchesrussian	No
Patches for Windows (Danish)	http://sync.bigfix.com/cgi-bin/bf-gather/windowspatchesdanish	No
Patches for Windows (Hebrew)	http://sync.bigfix.com/cgi-bin/bf-gather/windowspatcheshebrew	No
Patches for Windows (Greek)	http://sync.bigfix.com/cgi-bin/bf-gather/patchesforwindowsgreek	No
Updates for Windows Applications	http://sync.bigfix.com/cgi-bin/bf-gather/updateswindowsapps	No
Windows Point of Sale	http://sync.bigfix.com/cgi-bin/bf-gather/windowspointofsale	No
Patches for RHEL 5 Extended Support	http://sync.bigfix.com/cgi-bin/bf-gather/patchesforrhel5ESU	Added to all SCA Versions
Patches for RHEL 6 Extended Support	http://sync.bigfix.com/cgi-bin/bf-gather/patchesforrhel6ESU	Added to all SCA Versions
Patches for RHEL 7 Extended Support	http://sync.bigfix.com/cgi-bin/bf-gather/patchesforrhel7ESU	Added to all SCA Versions
Patches for RHEL 8 Extended Support	http://sync.bigfix.com/cgi-bin/bf-gather/patchesforrhel8ESU	Added to all SCA Versions
Patches for RHEL 7	http://sync.bigfix.com/cgi-bin/bf-gather/patchesforrhel7	No
Patches for RHEL RHSM 7 on System z	http://sync.bigfix.com/cgi-bin/bf-gather/patchesforrhelrhsm7z	No
Patches for RHEL RHSM 6 on System z	http://sync.bigfix.com/cgi-bin/bf-gather/patchesforrhelrhsm6z	No
Patches for RHEL 7 PPC64LE	http://sync.bigfix.com/cgi-bin/bf-gather/patchesforrhelppc64le7	No

Table 1. Supported Sites (continued)

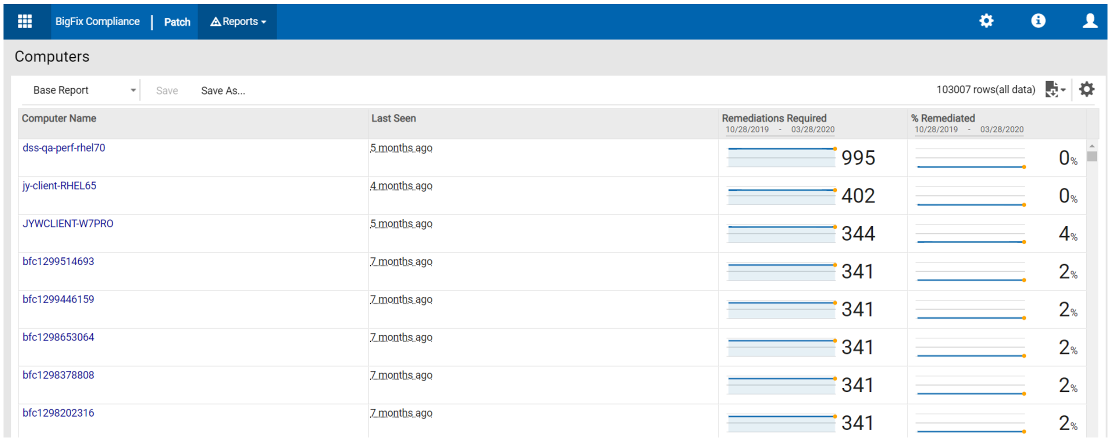
Site name	URL	Notes
Patches for RHEL PPC64BE 7	http://sync.bigfix.com/cgi-bin/bf-gather/patchesforrhelppc64be7	No
Patches for RHEL 6 Native Tools	http://sync.bigfix.com/cgi-bin/bf-gather/patchesforrhelppc64be7	No
Patches for RHEL 8 (BFC 2.0)	http://sync.bigfix.com/cgi-bin/bf-gather/patchesforrhel8	No
Patches for CentOS6 Plugin R2 (BFC 2.0.1)	http://sync.bigfix.com/cgi-bin/bf-gather/patchesforcentos6pluginr2	Added to all SCA versions
Patches for CentOS7 Plugin R2 (2.0.1)	http://sync.bigfix.com/cgi-bin/bf-gather/patchesforcentos7pluginr2	Added to all SCA versions
Patches for Mac OS X (2.0.1)	http://sync.bigfix.com/cgi-bin/bf-gather/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/bf-gather/updatesmacapps	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/bf-gather/win7esu	Added to all SCA versions.
Windows 2008 ESU (2.0.1)	http://sync.bigfix.com/cgi-bin/bf-gather/win2008ESU	Added to all SCA versions.

Computers Report

Select Patches domain using **Domains** and click **Reports** to find the following report:

Computers

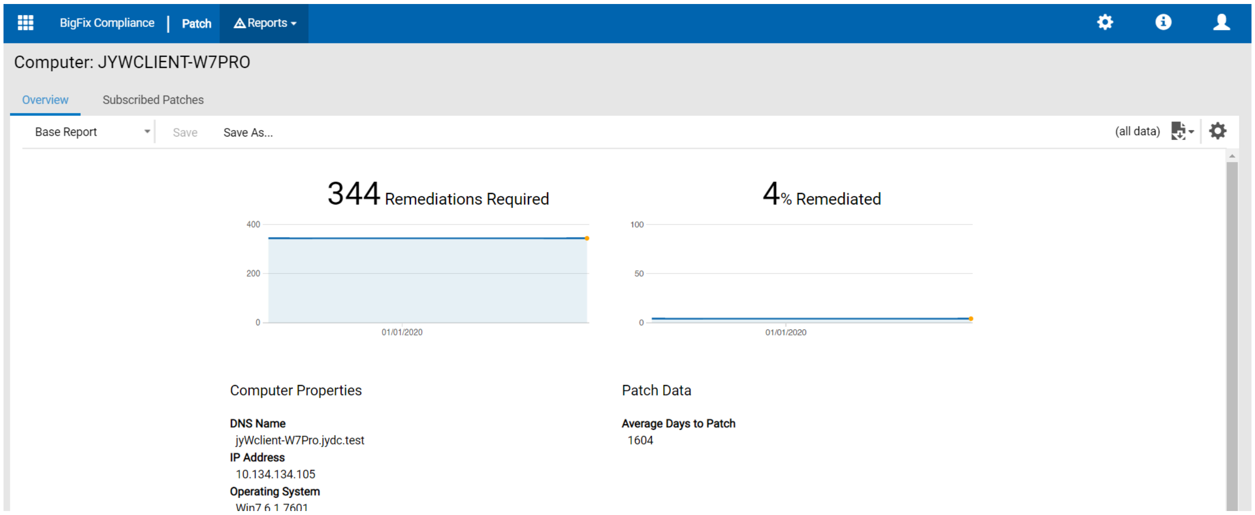
Shows the list view of computers, remediations required and % remediated.



Computer Name	Last Seen	Remediations Required 10/28/2019 - 03/28/2020	% Remediated 10/28/2019 - 03/28/2020
dss-qa-perf-rhel70	5 months ago	995	0%
jy-client-RHEL65	4 months ago	402	0%
JYWCLIENT-W7PRO	5 months ago	344	4%
bfc1299514693	7 months ago	341	2%
bfc1299446159	7 months ago	341	2%
bfc1298653064	7 months ago	341	2%
bfc1298378808	7 months ago	341	2%
bfc1298202316	7 months ago	341	2%

Computer Overview Report

To access the Computers Overview report, click any computer that appears in the list view.



Computer Properties

DNS Name
jyWclient-W7Pro.jydc.test
IP Address
10.134.134.105
Operating System
Win7 6.1.7601

Patch Data

Average Days to Patch
1604

Computer Overview report

The Computer Overview report represents a graphic representation of remediations required, % remediated, computer properties and patch data.

Computer Sub-Report

To access the Computers sub-reports, click the Reports dropdown menu at the top of the console and select Computers. Click any computers that appears on the list to open the sub-reports.

The sub-report of the Computer report is Subscribed Patches.

Subscribed Patches

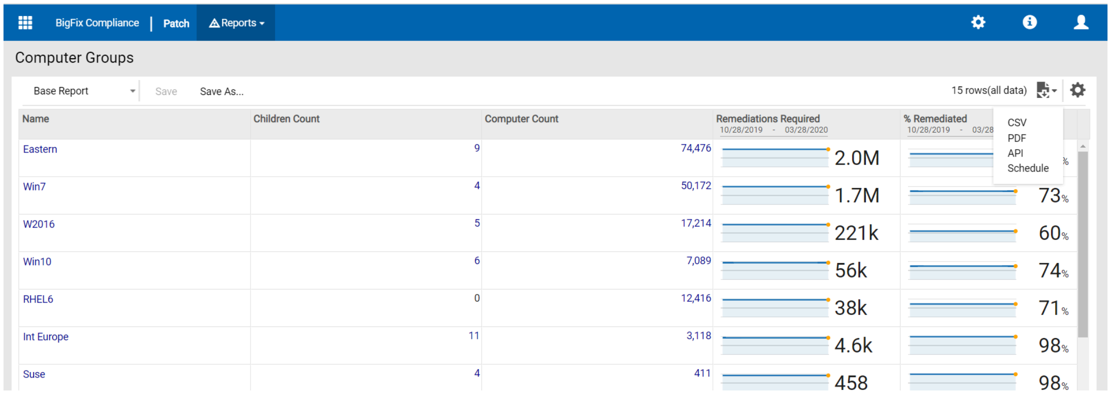
The Subscribed Patches sub-report contains a list of patches, severity, category, source, source release date, and remediated status.

Computer Groups Report

Select Patches domain using **Domains** and click **Reports** to find the following report:

Computer Groups

Shows the list view of computer groups, sub-groups (children), computer count, remediations required and % remediated.

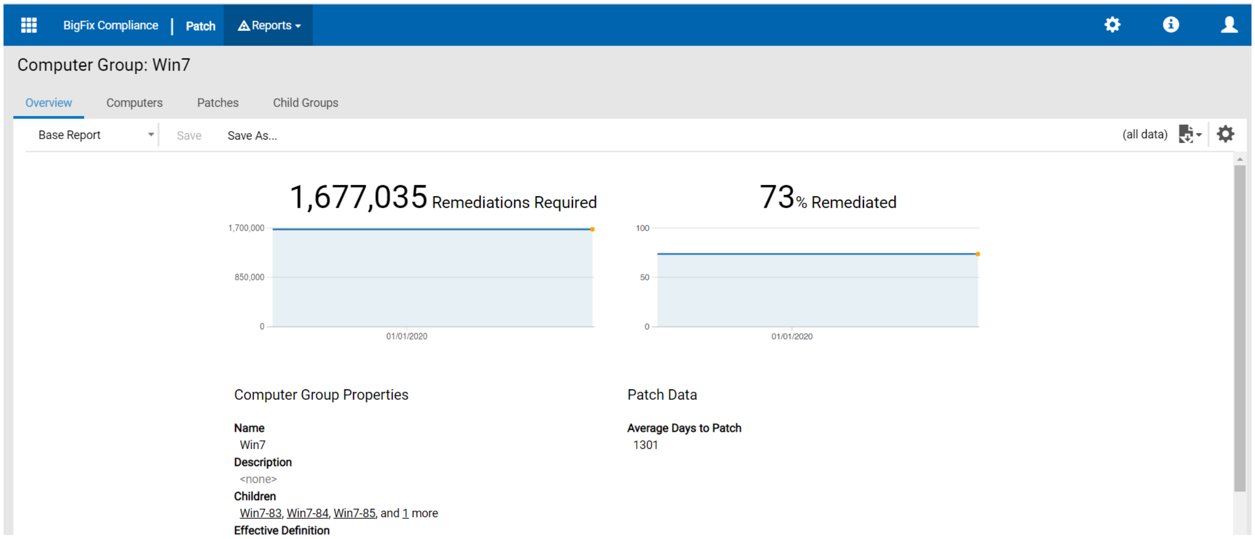


Computer Groups

Name	Children Count	Computer Count	Remediations Required 10/28/2019 - 03/28/2020	% Remediated 10/28/2019 - 03/28
Eastern	9	74,476	2.0M	%
Win7	4	50,172	1.7M	73%
W2016	5	17,214	221k	60%
Win10	6	7,089	56k	74%
RHEL6	0	12,416	38k	71%
Int Europe	11	3,118	4.6k	98%
Suse	4	411	458	98%

Computer Group Overview Report

To access the Computer Group Overview report, click any computer group that appears in the list view.



Computer Group: Win7

1,677,035 Remediations Required

73% Remediated

Computer Group Properties

Name
Win7
Description
<none>
Children
Win7-83, Win7-84, Win7-85, and 1 more
Effective Definition

Patch Data

Average Days to Patch
1301

Computer Group Overview report

The Computer Group Overview report represents a graphic representation of remediations required, % remediated, computer group properties, and patch data.

Computer Group Sub-Reports

To access the Computer Group sub-reports, click the Reports dropdown menu at the top of the console and select Computer Groups. Click any computer group that appears on the list to open the sub-reports.

The sub-reports of the Computer Group report are Computers, Patches, and Child Groups.

Computers

The Computers sub-report contains list of computers, last seen details, remediation required, and % remediated details.

Patches

The Patches sub-report contains list patches, severity, category, source, source release date, total vulnerability, relevant computers, and % remediated details.

Child Groups

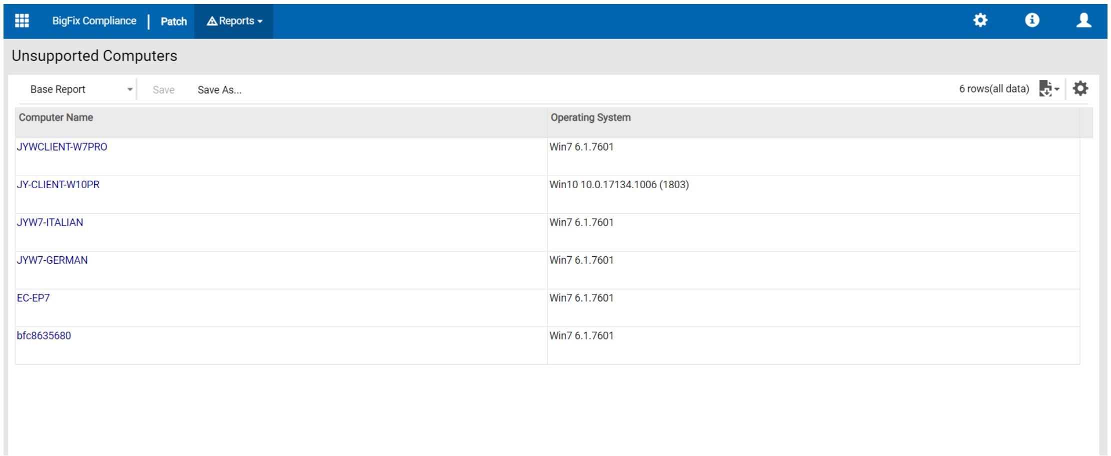
The Child Groups sub-report contains list computer groups, children count, computer count, remediations required, and % remediated details.

Unsupported Computers Report

Select Patches domain using **Domains** and click **Reports** to find the following report:

Unsupported Computers

Shows the list view of computer name and operating system.



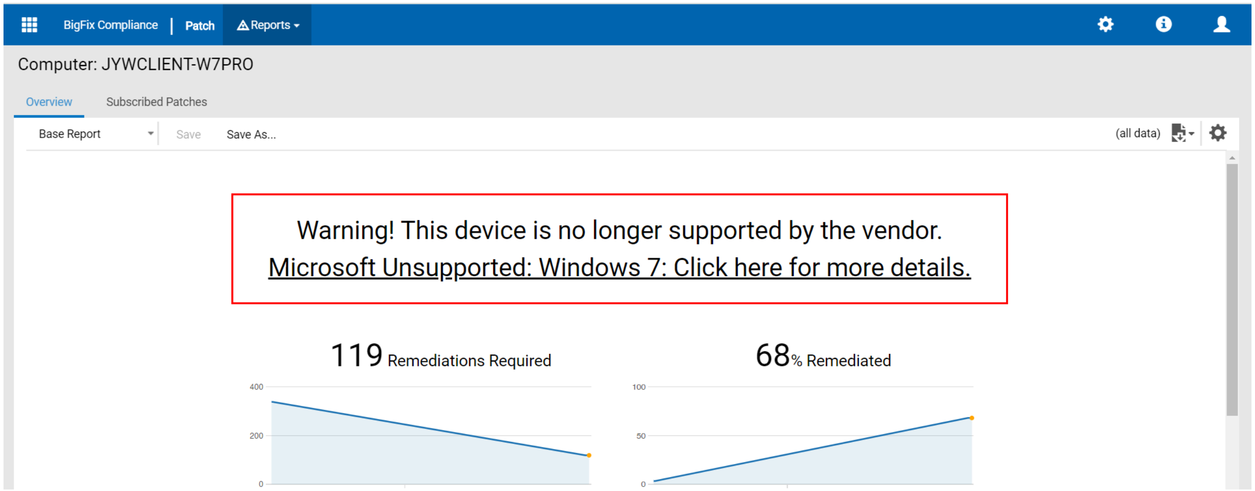
Unsupported Computers

Computer Name	Operating System
JYWCLIENT-W7PRO	Win7 6.1.7601
JY-CLIENT-W10PR	Win10 10.0.17134.1006 (1803)
JYW7-ITALIAN	Win7 6.1.7601
JYW7-GERMAN	Win7 6.1.7601
EC-EP7	Win7 6.1.7601
bfc8635680	Win7 6.1.7601

Note: If you have to remove the computer listed in this report, you must upgrade the OS of the listed computer to a supported OS.

Computer Overview Report

To access the Computers Overview report, click any computer that appears in the list view.



Warning! This device is no longer supported by the vendor.
Microsoft Unsupported: Windows 7: Click here for more details.

119 Remediations Required

68% Remediated

Computer overview report

The Computer Overview report represents a graphic representation of remediations required, % remediated and a warning note.

Computer Sub-Report

To access the Computer sub-report, click the Reports dropdown menu at the top of the console and select Unsupported Computers. Click any computer that appears on the list to open the sub-report.

The sub-report of the Computer report is Subscribed Patches.

Subscribed Patches report

The Subscribed Patches sub-report contains list of patches, severity, category, source, and source release date, and remediated status.

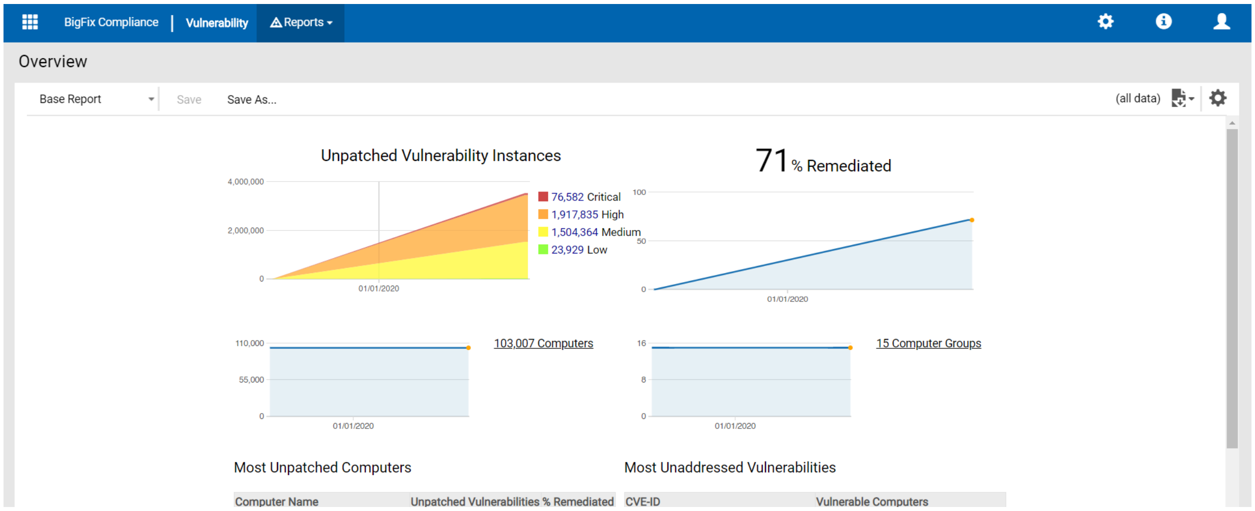
Chapter 6. Vulnerability Domain

The BigFix Compliance vulnerability reporting extends the analytics and reporting capabilities of the BigFix Compliance. The vulnerability domain report focuses on tracking and reporting the endpoint vulnerability after the patching actions. The report also enables you to identify risks, prioritize remediation, and be compliant. .

Prerequisites: You have to enable vulnerability reporting to import the data. To enable the vulnerability reports, see Domain Settings *(on page 20)*.

Overview Report

The following graphical reports are available from the primary Overview window of the Vulnerability domain dashboard:



Deployment Overview

Displays the current unpatched vulnerability instances, and the applied remediation.

The Unpatched Vulnerability Instances report displays all the instances of the vulnerability across all the endpoints. For example, if 3 vulnerabilities are unpatched and present on 10 computers, the number of Unpatched Vulnerabilities Instances calculated will be a total of 30, that will be tracked in this report graph. Similarly the remediation percentage is the remediation of these vulnerability instances.

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.

Most Unaddressed Vulnerabilities

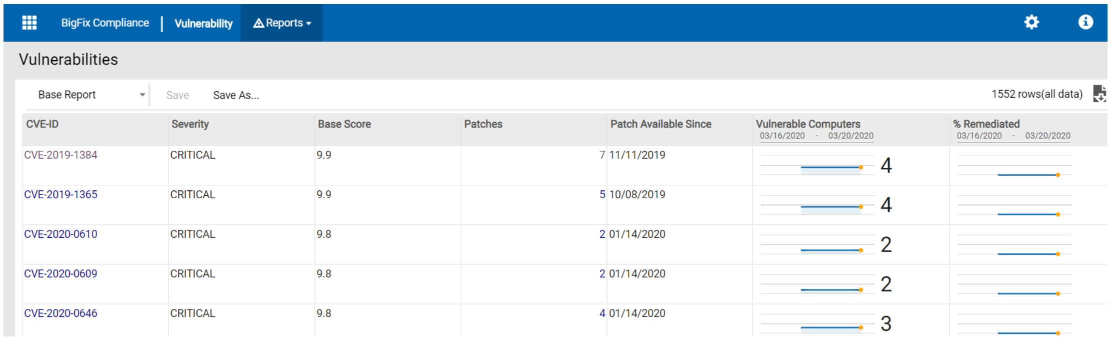
Displays the list of unaddressed vulnerabilities.

Vulnerabilities Report

Select Vulnerability domain using **Domains** and click **Reports** to find the following report:

Vulnerabilities

Shows the list view of CVE-ID, severity, base score, patches, patch available since, vulnerable computers, and % remediated.



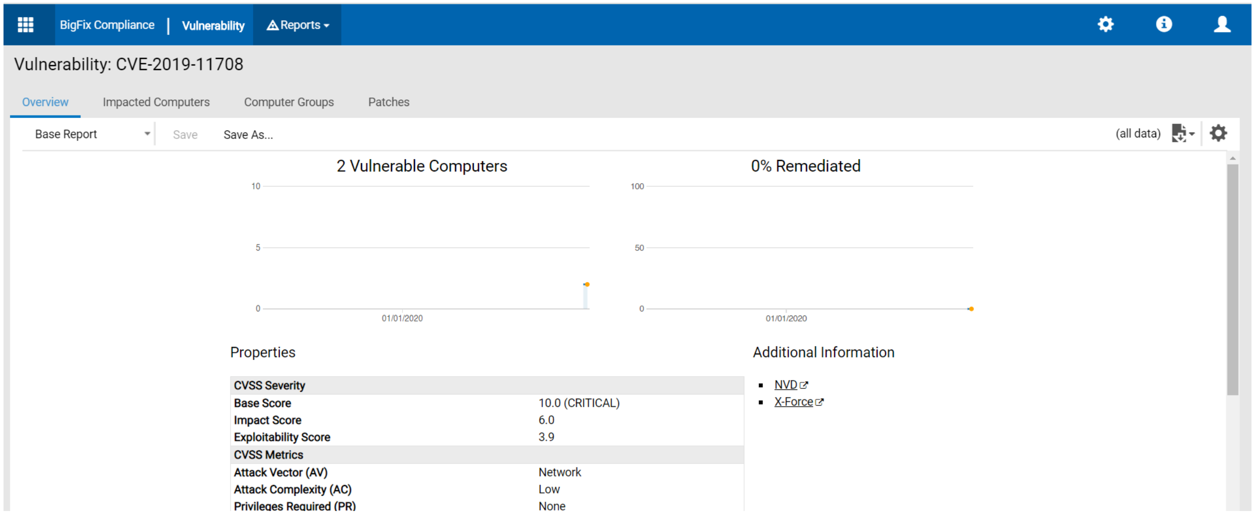
Vulnerabilities

1552 rows(all data)

CVE-ID	Severity	Base Score	Patches	Patch Available Since	Vulnerable Computers 03/16/2020 - 03/20/2020	% Remediated 03/16/2020 - 03/20/2020
CVE-2019-1384	CRITICAL	9.9	7	11/11/2019	4	
CVE-2019-1365	CRITICAL	9.9	5	10/08/2019	4	
CVE-2020-0610	CRITICAL	9.8	2	01/14/2020	2	
CVE-2020-0609	CRITICAL	9.8	2	01/14/2020	2	
CVE-2020-0646	CRITICAL	9.8	4	01/14/2020	3	

Vulnerability Overview Reports

To access the Vulnerability Overview report, click any CVE-ID that appears in the list view.



Vulnerability: CVE-2019-11708

Properties

CVSS Severity	
Base Score	10.0 (CRITICAL)
Impact Score	6.0
Exploitability Score	3.9
CVSS Metrics	
Attack Vector (AV)	Network
Attack Complexity (AC)	Low
Privileges Required (PR)	None

Additional Information

- NVD
- X-Force

Vulnerability Overview report

The Vulnerability Overview report represents a graphic representation of vulnerable computers, % remediated, and the computer properties. All the data displayed in Vulnerability Overview Report is from NVD.

Vulnerability Sub-Reports

To access the Vulnerability sub-reports, click the Reports dropdown menu at the top of the console and select Vulnerabilities. Click any CVE-ID that appears on the list to open the sub-reports.

The sub-reports of the Vulnerability report are Impacted Computers, Computer Groups and Patches.

Impacted Computers

The Impacted Computers sub-report contains list of computers, last seen details, vulnerable status, date remediated and days to remediate.

Computer Groups

The Computer Groups sub-report contains list of computer groups, computer counts, vulnerable computers, and % remediated.

Patches

The Patches sub-report contains list of patches, severity, category, source, source release date, superseded details, and relevant computers.

Vulnerability Reporting Mechanics

The vulnerability data for Compliance is extracted from the following sources:

- The vulnerability CVEs listed in the patch fixlet metadata (`CVENames`, `MIME_x-fixlet-cve`).
- The supersedence information in the patch fixlet metadata (`MIME_x-fixlet-superseded-id`).
- Vulnerability details from the external NVD feeds.
- The patch fixlet evaluation result.

Compliance do not scan devices directly for vulnerabilities. The vulnerability of a device is derived from its patch applicability status.

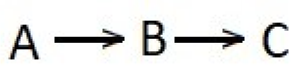
Table 2. Patch applicability status

Fixlet Status	Patch Application Status	Vulnerability Status
Not Relevant	Applied	Remediated
Relevant	Not Applied	Not Remediated

The following sections explains how the Vulnerability Reporting mechanism works and how it affects reporting.

Supersedence chain

Vendors may release patches that include fixes found in previous patches (now obsolete). This process is knows as supersedence, the old obsolete patch is now regarded and flagged as "superseded".



In the above image:

Patch A is superseded by Patch B and then Patch B is superseded by the current Patch C.

Patch C is the superseding patch that replaces the previous two patches and contains all of their security fixes. If Patch C is applied, it is no longer necessary to apply Patch A or Patch B.

However, if Compliance checks the metadata for Patch C, it cannot determine that it also resolved the vulnerabilities described in A and B. Therefore, Compliance creates a *Supersedence chain* during the import process and gathers information about an endpoint's vulnerability status. Using the *Supersedence chain*, Compliance associates implicitly resolved vulnerabilities with their respective patches. Thus, when Patch C is applied, all the vulnerabilities in A, B, and C patches are accurately marked as *Remediated*.

Patches for Windows and EnableSupersededEval

The EnableSupersededEval is a client setting used by the Patches for Windows site. By default, it is disabled, which prevents superseded patches in the site from being evaluated.

The default behavior of patch applicability evaluation (with the flag turned off) is typically desirable. When a newer patch is available, the superseded patch should no longer be applied. However when determining the vulnerability status, Compliance cannot distinguish between an applied superseded patch Fixlet and a superseded Fixlet with evaluation disabled.

Compliance handles the above described situation in the following ways:

- **If a patch is detected for the first time and is superseded**. Compliance cannot determine the patch status and may display the resolution as *Never Relevant* indicating a state of ambiguity and that it cannot determine whether or not the patch has been applied to a given endpoint.
- **If a patch that was observed previously becomes superseded**. Compliance takes forward the previous evaluation for any endpoints that had evaluated it. For example, a patch that was applied on an endpoint previously still retains a status of *remediated*.
- **If the endpoint has turned on the EnableSupersededEval flag**. Compliance continues to respect the live evaluation status for superseded patches.

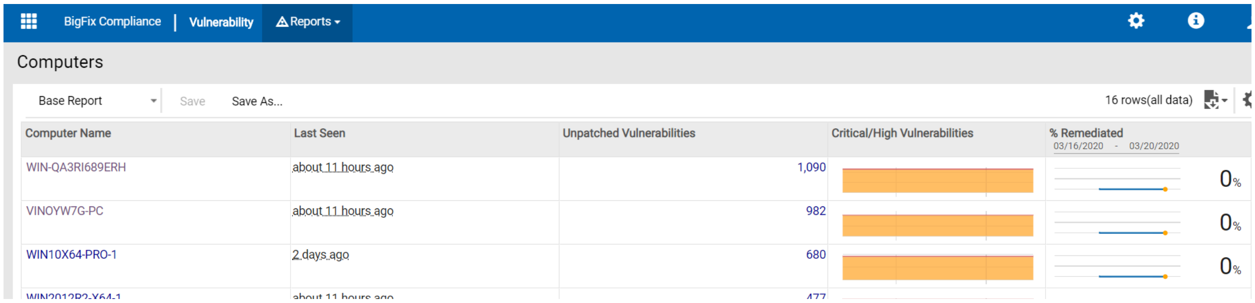
In effect, a fresh install or enablement of Patch and Vulnerability Reporting in Compliance has incomplete data about the vulnerability posture. As Compliance is installed for a longer duration, it observes details about which patches were previously applied, it becomes better and able to infer which vulnerabilities are remediated or not.

Computers Report

Select Vulnerability domain using **Domains** and click **Reports** to find the following report:

Computers

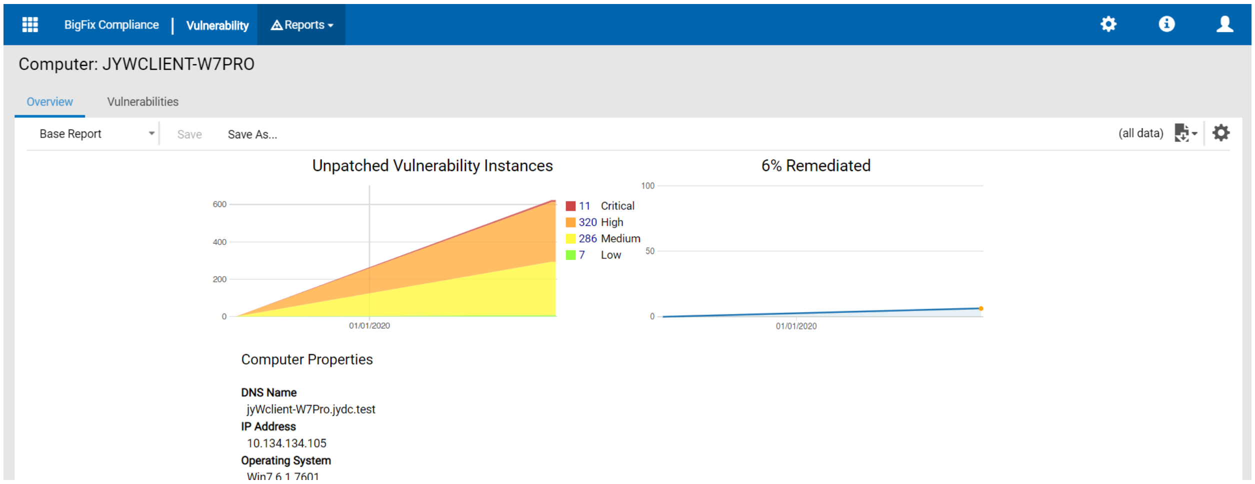
Shows the list view of computers, last seen, unpatched vulnerability, critical vulnerabilities and % remediated.



Computer Name	Last Seen	Unpatched Vulnerabilities	Critical/High Vulnerabilities	% Remediated 03/16/2020 - 03/20/2020
WIN-QA3RI689ERH	about 11 hours ago	1,090		0%
VINOYW7G-PC	about 11 hours ago	982		0%
WIN10X64-PRO-1	2 days ago	680		0%
WIN2012R2-X64-1	about 11 hours ago	477		

Computer Overview Report

To access the Computer Overview report, click any computer that appears in the list view.



Computer Properties

DNS Name
jyWclient-W7Pro.jydc.test
IP Address
10.134.134.105
Operating System
Win7 6.1.7601

Computer Overview report

The Computer Overview report represents a graphic representation of unpatched vulnerability instances, computer properties and % remediated.

Computer Sub-Report

To access the Computer sub-report, click the Reports dropdown menu at the top of the console and select Computers. Click any computer that appears on the list to open the sub-report.

The sub-report of the Computers report are Vulnerabilities.

Vulnerabilities

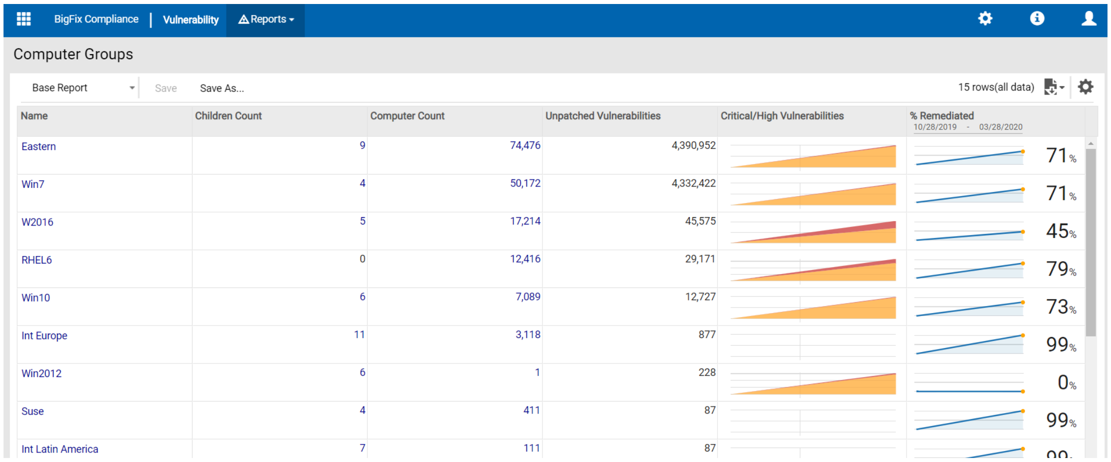
The Vulnerabilities sub-report contains list of CVE-IDs, severity, base score, vulnerable details, dates of first patch available, date remediated, and days to remediate.

Computer Groups Report

Select Vulnerability domain using **Domains** and click **Reports** to find the following report:

Computer Groups

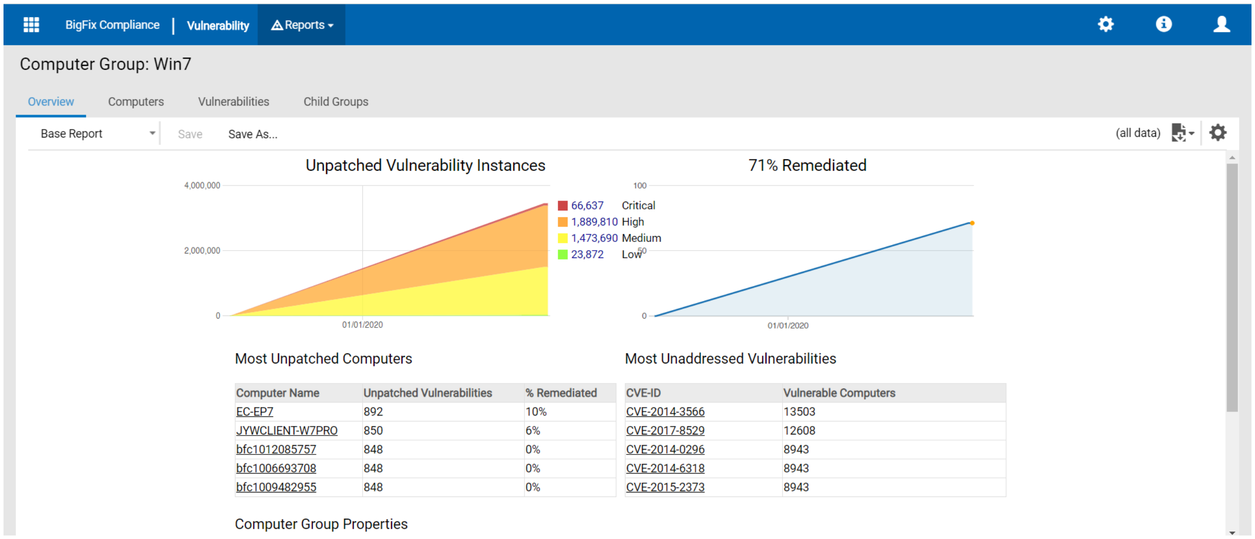
Shows the list view of computer groups, sub-groups (children), computer count, unpatched vulnerabilities, critical vulnerabilities and % remediated.



Name	Children Count	Computer Count	Unpatched Vulnerabilities	Critical/High Vulnerabilities	% Remediated 10/28/2019 - 03/28/2020
Eastern	9	74,476	4,390,952		71%
Win7	4	50,172	4,332,422		71%
W2016	5	17,214	45,575		45%
RHEL6	0	12,416	29,171		79%
Win10	6	7,089	12,727		73%
Int Europe	11	3,118	877		99%
Win2012	6	1	228		0%
Suse	4	411	87		99%
Int Latin America	7	111	87		99%

Computer Group Overview Reports

To access the Computer Group Overview report, click any computer group that appears in the list view.



Most Unpatched Computers

Computer Name	Unpatched Vulnerabilities	% Remediated
EC-EP7	892	10%
JYWCLIENT-W7PRO	850	6%
bfc1012085757	848	0%
bfc1006693708	848	0%
bfc1009482955	848	0%

Most Unaddressed Vulnerabilities

CVE-ID	Vulnerable Computers
CVE-2014-3566	13503
CVE-2017-8529	12608
CVE-2014-0296	8943
CVE-2014-6318	8943
CVE-2015-2373	8943

Computer Group Properties

Computer Group Overview report

The Computer Group Overview report represents a graphic representation of unpatched vulnerability instances, % remediated, most unpatched computers, most unaddressed vulnerabilities, and computer group properties.

Computer Group Sub-Reports

To access the Computer Group sub-reports, click the Reports dropdown menu at the top of the console and select Computer Groups. Click any computer group that appears on the list to open the sub-reports.

The sub-reports of the Computer Groups report are Computers, Vulnerabilities and Child Groups.

Computers

The Computers sub-report contains list of computers, last seen details, unpatched vulnerabilities, critical vulnerabilities, and % remediated.

Vulnerabilities

The Vulnerabilities sub-report contains list of CVE-IDs, severity, base score, patches, patch available since, vulnerable computers, and % remediated.

Child Groups

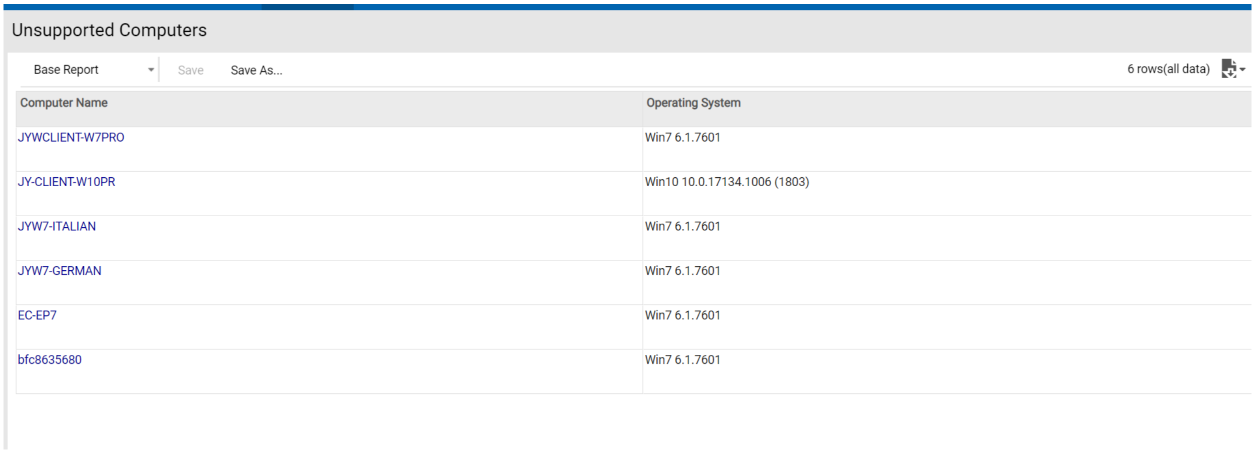
The Child Groups sub-report contains list of computer groups, children counts, computer counts, unpatched vulnerabilities, critical vulnerabilities, and % remediated.

Unsupported Computers Report

Select Vulnerability domain using **Domains** and click **Reports** to find the following report:

Unsupported Computers

Shows the list view of computer name, and operating system.



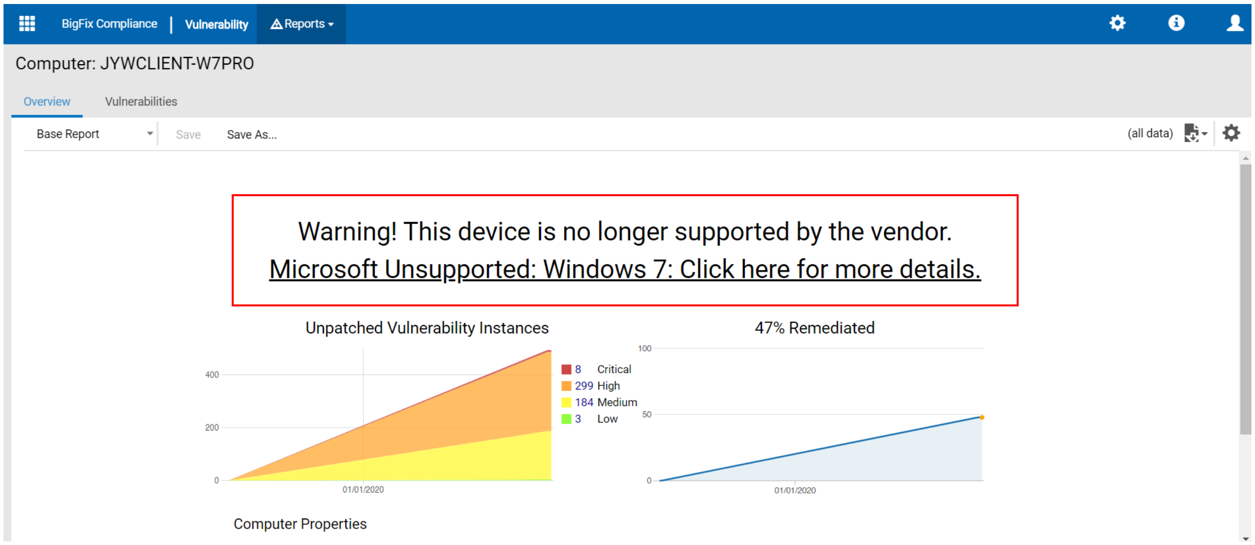
Unsupported Computers

Computer Name	Operating System
JYWCLIENT-W7PRO	Win7 6.1.7601
JY-CLIENT-W10PR	Win10 10.0.17134.1006 (1803)
JYW7-ITALIAN	Win7 6.1.7601
JYW7-GERMAN	Win7 6.1.7601
EC-EP7	Win7 6.1.7601
bfc8635680	Win7 6.1.7601

Note: If you have to remove the computer listed in this report, you must upgrade the OS of the listed computer to a supported OS.

Computer Overview Report

To access the Computer Overview report, click any computer that appears in the list view.



Computer: JYWCLIENT-W7PRO

Warning! This device is no longer supported by the vendor.
Microsoft Unsupported: Windows 7: Click here for more details.

Computer overview report

The Computer Overview report represents a graphic representation of unpatched vulnerability instances, % remediated, warning note and computer properties.

Computer Sub-Report

To access the Computer sub-reports, click the Reports dropdown menu at the top of the console and select Unsupported Computers. Click any computer that appears on the list to open the sub-report.

The sub-report of the Computer report is Vulnerabilities.

Vulnerabilities

The Vulnerabilities sub-report contains list of CVE-IDs, severity, base score, vulnerable details, dates of first patch available, date remediated, and days to remediate.

Appendix A. Support

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

- BigFix Support Portal
- BigFix Developer
- BigFix Playlist on YouTube
- BigFix Tech Advisors channel on YouTube
- 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.