BigFix
Web Reports Guide

Special notice

Before using this information and the product it supports, read the information in Notices (on page 141).

Edition notice

This edition applies to BigFix version 10 and to all subsequent releases and modifications until otherwise indicated in new editions.

Contents

Special notice.....2

Edition notice.....3

Chapter 1. Web Reports Guide.....1

Chapter 2. Configuring Web Reports.....2

Requirements.....2

Supported Browsers.....3

Updating the credentials to access the BESReporting database.....3

Setting the session inactivity timeout.....4

Restricting access to the report files.....5

Integrating LDAP with Web Reports.....6

Integration with LDAP.....7

Integration with Active Directory.....12

Setting the Number of LDAP Entries to Display.....14

SAML integration.....15

Compatibility with NT domains.....15

Chapter 3. Using the Program.....18

First Login.....18

Starting Web Reports.....18

Viewing the Data.....20

Filtering the Data.....21

Saving Reports.....23

Viewing Reports.....24

Creating Charts.....26

Setting Up Email....27
Scheduling Reports....31
Adding a Datasource....34
Editing a Datasource....36
Setting Your Preferences....37
Enabling FIPS cryptography on Web Reports....38
Setting the login lockout....39
Performing the reauthentication....40
Chapter 4. Exploring....42
Filters....43
Charts....44
Collapsing the Table....48
Columnar Report....50
Edit Columns....50
Changing Column Order....53
Computers....53
Content....55
Actions....56
Operators....56
Unmanaged Assets....57
Custom....58
Chapter 5. Reporting....59
Report List Main Page....59
Import Report....59
Only Show Starred....60

Filter by Label....60
Filter by Author....61
Add, Create, and Delete Labels....61
Delete....62
Main List....62
Overview Report....63
Total Issues....64
Total Number of Computers....65
Computer Vulnerability Status....66
Issues Remediated....67
Overall Statistics....68
Top 10 Critical/Important Issues Detected....69
Computer Properties List....70
Open Vulnerabilities List....71
Other Reports....72
Showing non-relevant results....73
Chapter 6. Administering the Program....74
Scheduled Activities....74
Creating Scheduled Activities....75
Filter Management....79
Address Book....80
User Management....82
Create Users....83
Manage Roles....84
Create Roles....85

Global User Options....86
Edit User....88
Datasource Settings....89
Add New Datasource....91
Edit Datasource....93
Errors....94
Appendix A. Tasks for advanced users....95
Understanding the Web Report File....95
Creating a Custom Report....96
Web Reports XML....98
Creating a Portable Report for Propagation....98
Exporting activity reports to CSV files....100
Exporting activity reports to PDF documents....101
On Windows Systems....101
On Linux Systems....104
Exporting the report output to a PDF file....108
Customizing HTTPS on Web Reports....108
Logging Web Reports....113
Changing the temporary files on Linux....116
Querying Using HTTP GET....116
Querying Using SOAP....117
PERL....118
Raw SOAP Request and Response Format....119
Session Inspectors....120
Displaying Web Reports from Content Sites....121

External Reports..... 122

Template Reports..... 122

Disabling local operators on Web Reports.....123

Appendix B. Glossary..... 126

Appendix C. Support..... 140

Notices.....141

Index.....

Chapter 1. Introduction

Learn how the Web Reports feature extends the power of BigFix.

Web Reports is a high-level web application that complements and extends the power of BigFix. It connects to one or more BigFix databases to aggregate and analyze your entire network. It allows you to visualize your data, with both charts and data listings, in any standard web browser. Web Reports provides you with a convenient, compact, and timely overview of your BigFix network, no matter how broadly it extends.

Web Reports is prepackaged with dozens of critical reports ready to take the pulse of all your networked computers, including real-time visualization of patch rollouts, remediations, policy compliance, and much more. In addition, you can easily customize your own reports using faceted navigation to reduce your data to its essentials for fast, targeted access.

Web Reports is organized around **domains**, which are content groupings with their own set of built-in reports to get you up and running quickly. Domains also act as primary filters that allow you to limit the scope of reports and drill down into your network with finer granularity.

Chapter 2. Configuring Web Reports

Web Reports is used whenever you want to view BigFix data that is spread over multiple databases in your deployment.

Beyond aggregation, it is also invaluable when you need real-time information quickly, but do not have direct access to a BigFix console. To use Web Reports, all you need is a browser.

You can generate listings and charts immediately with a large set of prepackaged reports. It is also easy to create custom reports to address questions or policies specific to your own network.

This guide describes all the unique features of the Web Reports Interface. Advanced topics in relevance and the low-level report language are beyond the scope of this guide.

Requirements

Web Reports can run on a stand-alone server or on the same machine that hosts the BigFix database.

Starting from V9.2 Patch 3, only the 64-bit architecture is supported for installing the BigFix Web Reports component on Windows systems.

Note: Ensure that the Web Reports component, like the BigFix console, has the same version of the BigFix servers to which it connects.

The requirements for the Web Reports server vary depending on the number of databases, computers, actions, and retrieved properties that you want to track.

The Web Reports primary resource requirements revolve around memory size for fast access and CPU speed for fast report processing. The disk stores a local cache to make load times faster, but the disk speeds have less impact on the Web Reports than memory size and CPU speeds.

Note: The Web Reports server is not supported on Server Core for Windows Server 2008 R2.

BigFix deployments with more than 30,000 agents can benefit by having a separate Web Reports server so that the main BigFix server does not need to share its resources. You can set up multiple Web Reports servers with minimal performance impact on the main server.

Web Reports server requirements:

Number of Agents	CPU	Memory
< 10,000	2ghz	1 GB
10,001-30,000	2ghz (dual core)	2 GB
30,000-100,000	2ghz (dual core)	3 GB
100,000-200,000	2ghz (quad core)	4 GB

Supported Browsers

For the supported versions, see #unique_8_Connect_42_table_pf2_k4b_xkb.

JavaScript must be enabled on your browser to use Web Reports.

Updating the credentials to access the BESReporting database

How to update the user's password to connect to the BESReporting database.

Depending on the type of authentication selected, you can change the password of the user that manages the connection between the Web Report component and the BESReporting database in one of the following ways:

If you selected the NT authentication method

Update the password of the user that the Web Reports service is running as.

If you selected the SQL authentication method:

Run the following steps:

1. Access the following key in the Windows registry:

```
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\BigFix\Enterprise Server\FillAggregateDB
```

Note: You might need to change permissions on the registry key to see it.

2. Change the value in the 'Password' key to the new password.
3. Restart Web Reports. Upon restart, the Web Reports service encrypts the new password.

Setting the session inactivity timeout

Setting a limit to the duration of a session for the user interface.

To put a limit to the length of an inactive user interface session, you must set the Web Reports property `InactivityTimeoutLength` to the amount of inactivity minutes after which the user interface session expires. The default value is 120 minutes. To insert a different value, perform the following steps:

On Windows operating systems:

1. Open a command prompt and run `Regedit`.
2. In the Registry Editor window, under the `HKEY_LOCAL_MACHINE\Software\BigFix\Enterprise Server\BESReports` key (on 32-bit Windows operating systems) or `HKEY_LOCAL_MACHINE\Software\Wow6432Node\BigFix\Enterprise Server\BESReports` (on 64-bit Windows operating systems), create a REG_SZ keyword named `InactivityTimeoutLength` and set it to the maximum number of minutes of inactivity after which the user interface session expires.
3. Close the Registry Editor window and restart the `BES Web Report Server` service to apply the new `InactivityTimeoutLength` value.

On Linux operating systems:

1. Open the `/var/opt/BESWebReportsServer/beswebreports.config` configuration file.
2. Add the `InactivityTimeoutLength` property in the `[Software\BigFix\Enterprise Server\BESReports]` section as follows:

   ```
   InactivityTimeoutLength = <max_timeout_minutes>
   ```

   where `<max_timeout_minutes>` is the maximum number of minutes of inactivity after which the user interface session expires.

   Note: The new value for `InactivityTimeoutLength` is applied the next time you launch the Web Reports application.

Note: As an alternative to the procedures described above, you can also use the **Activity Timeout Length** text box available in Web Reports under Administration -> User Management -> Global User Options.

Restricting access to the report files

In the Web Report component, you can use a new option named "ReportFilesCheck" to toggle protection on the report files.

If this option is set to "1", you can access the content under "ReportFiles" only if you are logged in and you have access to the report that "owns" the file. No login page is displayed in case of failure, since this content is accessible only if a session already exists, for example if session cookies are already set.

A fresh installation of BigFix Version 9.5 Patch 6 sets the "ReportFilesCheck" option to "1" by default.

If you upgrade from Version 9.5 Patch 5 or earlier versions, the check is not enabled.

You can enable it by performing the following steps:

On Windows systems:

1. Stop the `BES Web Report Server` service.
2. Run Regedit.
3. Add the option

   ```
   ReportFilesCheck = 1
   ```

   in the Windows registry under:

   ```
   HKLM\SOFTWARE\BigFix\Enterprise Server\BESReports
   ```
4. Restart the `BES Web Report Server` service.

On Linux systems:

1. Stop the service by running the command `service beswebreports stop`.
2. Open the `/var/opt/BESWebReportsServer/beswebreports.config` file.
3. Add the `ReportFilesCheck` option in the `[Software\BigFix\Enterprise Server \BESReports]` section as follows:

   ```
   ReportFilesCheck = 1
   ```
4. Restart the service by running the command `service beswebreports start`.

Integrating LDAP with Web Reports

There are two solutions for integrating LDAP with the Web Reports server.

The two solutions are mutually exclusive on Windows:

- The first solution supports the integration of LDAP (both Tivoli Directory Server and Active Directory) with the Web Reports server running on both Windows and Linux systems. This is the default solution for new installations starting from V9.1.
- The second solution supports the integration of Active Directory with the Web Reports server running on Windows only. It works only if the computer where the Web Reports server runs is joined to an AD Domain. This solution has been kept for compatibility with earlier versions.

When upgrading BigFix to V9.5, the Endpoint Manager 9.1 Active Directory solution is kept for compatibility with the existing environment. To switch to the LDAP solution see LDAP integration after Windows upgrade (on page 13).

Integration with LDAP

You can integrate Web Reports with LDAP in a Windows or Linux environment.

Run the following steps:

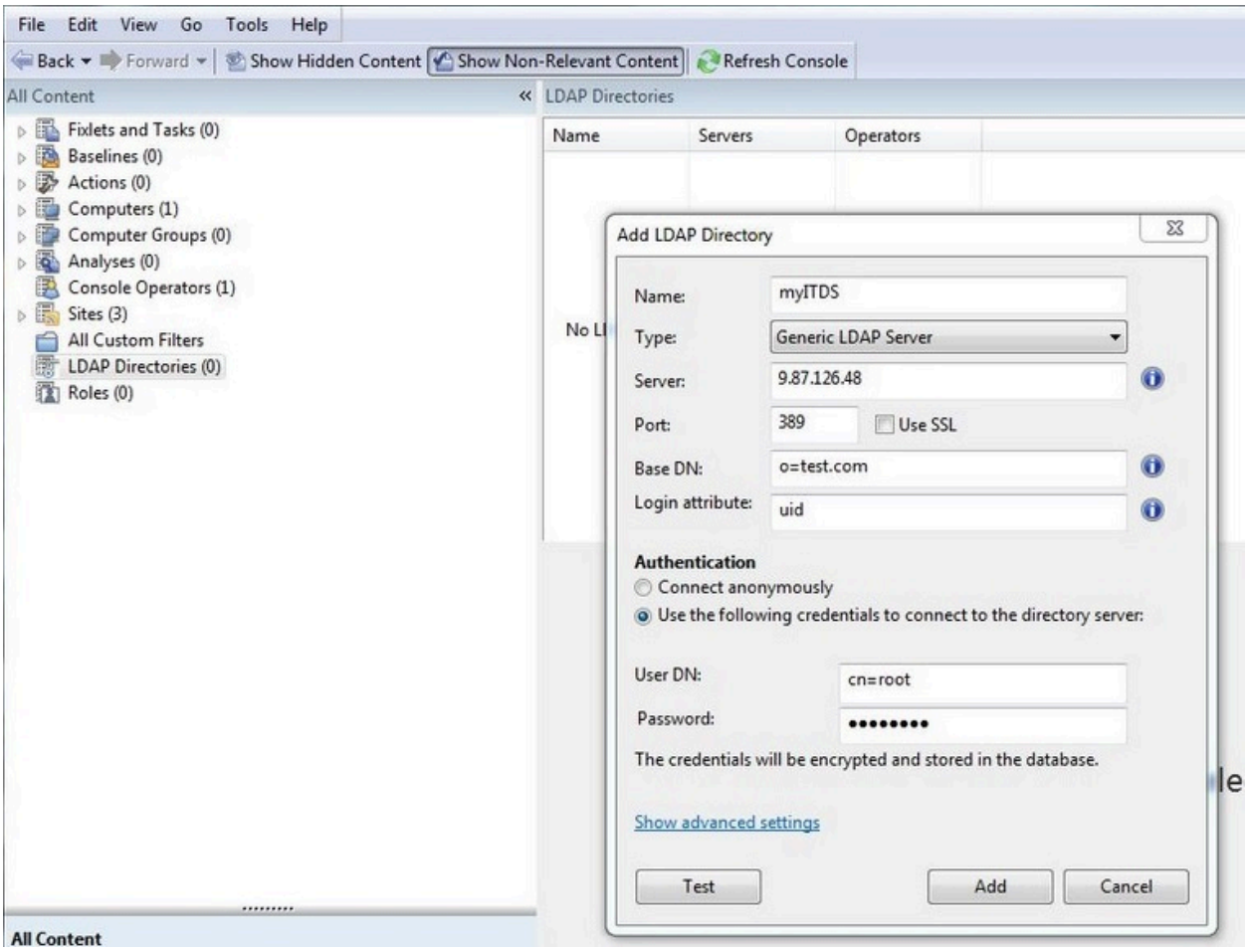
- Step 1: Add an LDAP directory to the BigFix Server *(on page 7)*
- Step 2: Assign a Web Reports role to LDAP users or groups *(on page 8)*
- Step 3: Log in with an LDAP user *(on page 11)*

Step 1: Add an LDAP directory to the BigFix Server

To use the LDAP capabilities in Web Reports, you must define LDAP Directories in the BigFix server.

In this way, Web Reports can see the same LDAP object detail level that can be seen using the BigFix console.

To add an LDAP directory to your deployment, use the BigFix console where you can choose the type of directory between Microsoft Active Directory and Generic LDAP Server:

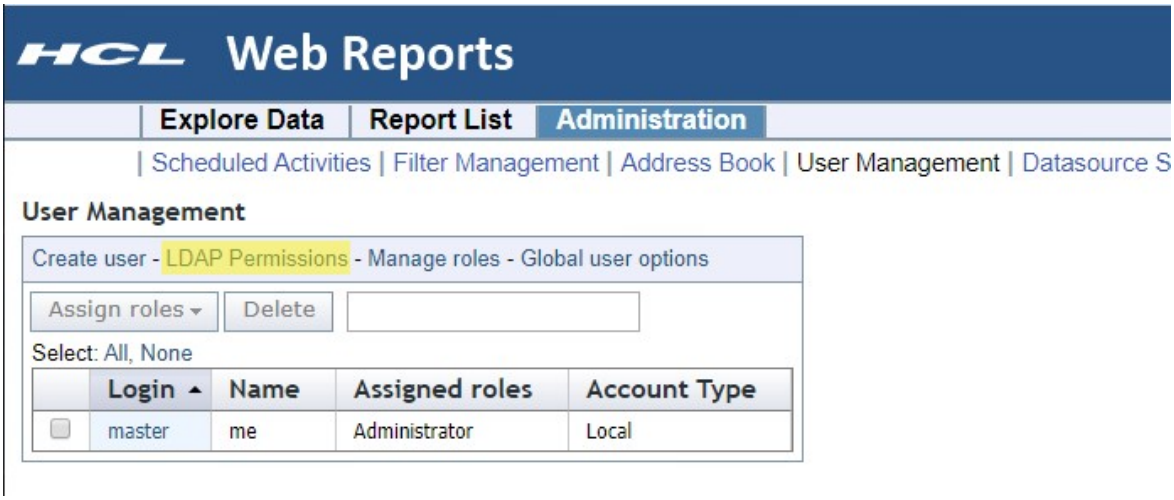


You do not need to add any LDAP console operators at this time.

Step 2: Assign a Web Reports role to LDAP users or groups

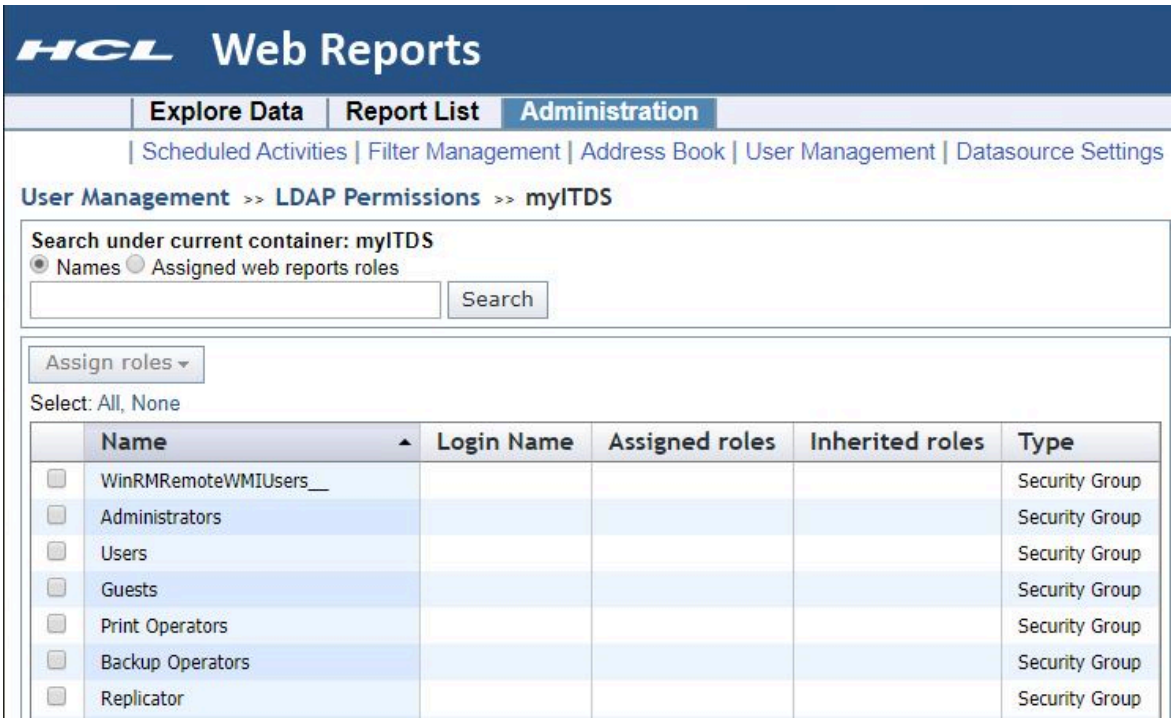
How to assign a Web Reports role.

1. Log in to the Web Reports using a user with Administrator privileges, and navigate to **Administration > User Management**:

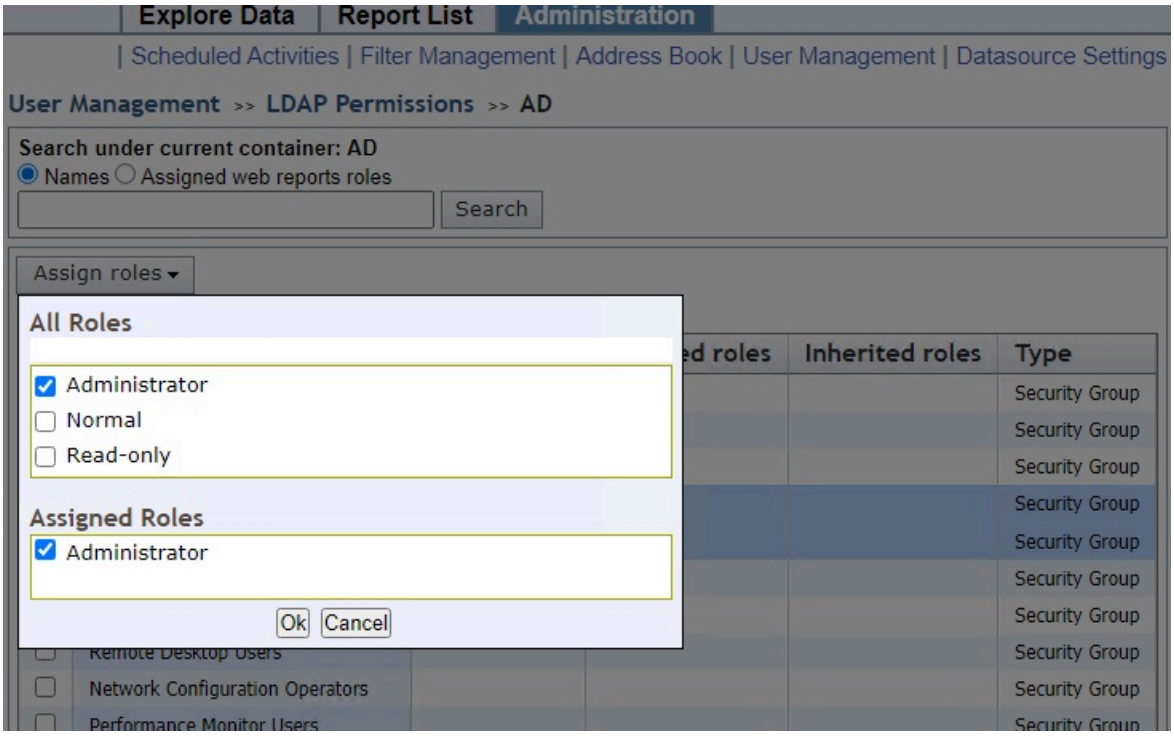


2. Click the LDAP Group permissions to see the list of the available directories among the known datasources:

3. In the previous solution you see the list of AD containers. Click a directory to list all its users and groups:



4. Select users or groups and assign them the Web Reports roles like that (after clicking the **Ok** button, you will need to reauthenticate to complete the operation as described in Performing the reauthentication *(on page 40)*):



The new LDAP user will be created in the Web Reports database when this user performs the login for the first time.

Step 3: Log in with an LDAP user

You can now log in with one of the LDAP users belonging to the group associated to the role Administrator.

To enter the Web Reports login credentials, follow the syntax used for entering Active Directory and Generic LDAP users from the Console.

When performing the first log in, the Web Reports uses the BigFix server to send the login credentials to the LDAP server. If the credentials are accepted, the Web Reports server creates the entry on the database and then logs in the LDAP user.

Integration with Active Directory

You can enable Active Directory users to access the BigFix **Web Reports** server.

Note: This configuration is not supported on the BigFix **Web Reports** server running on Linux and it is maintained only for backward compatibility reasons.

To integrate Active Directory with the **Web Reports** server running on Windows, perform the following steps:

1. Enable SSL support in Web Reports, to protect user Active Directory credentials.
2. If the permissions on Active Directory are set so that only some users are able to read the Active Directory data or if the **Web Reports** server does not belong to the Active Directory domain, you must configure your Web Reports Server service to run as a domain user with permissions to query Active Directory. This user does not need to be a domain administrator or have any permissions to make changes to Active Directory.

Note: Automatic Fixlet upgrades are enabled only if Web Reports service runs with the local system account.

3. Log in to Web Reports as a Web Reports administrator.
4. Navigate to **Administration > User Management**.
5. Click the **Active directory permissions** link.

Note: To display this link and start configuring Active Directory authentication over LDAP for Web Reports, you must enable LDAP user authentication from the BigFix console.

LDAP integration after Windows upgrade

If you upgrade Windows BigFix, the Active Directory solution is kept for compatibility with the existing environment.

Warning: When passing from the legacy mode (`UseLegacyADLogin` = 1) to the new Web Reports working mode (`UseLegacyADLogin` = 0), the data remains in the database but it will no longer be accessible by the old AD/LDAP operator definitions, unless it is public data. Therefore, in addition to the steps described below, it is required to manually create new AD/LDAP operators and not public data (i.e. reports, filters, favorites) and eventually update the scheduled activities and the user email. In the same way, AD/LDAP operators and not public data visible with `UseLegacyADLogin` set to 0 are not available when returning to the legacy mode.

To switch to the new Web Reports and LDAP integration functionality, perform the following steps:

1. Log in to Web Reports.
2. From **User Management** remove all the Active Directory users.
3. Change the `BES Web Report Server` service from Active Directory account to Local System account.
4. Set `UseLegacyADLogin` value in `HKLM\Software\WOW6432Node\BigFix\Enterprise Server\BESReports` from `1` to `0`.

5. Restart the `BES Web Report Server` service.
6. From the console, add Active Directory or LDAP by selecting **Tool -> Add LDAP Directory**.
7. Log in to Web Reports and from **User Management** assign Web Reports roles to LDAP users and groups. For more information see Assigning a Web Reports role to LDAP users or groups *(on page 8)*.

Setting the Number of LDAP Entries to Display

The default number of LDAP entries displayed in Web Reports is `1000`.

If you want to change the maximum number of LDAP entries to display within Web Reports, perform the following steps:

On Windows systems:

1. Stop the `BES Web Report Server` service.
2. Run Regedit.
3. Under the `HKEY_LOCAL_MACHINE\Software\BigFix\Enterprise Server\BESReports` key (on 32-bit Windows systems) or `HKEY_LOCAL_MACHINE\Software\Wow6432Node\BigFix\Enterprise Server\BESReports` (on 64-bit Windows systems), create a REG_SZ keyword named `LDAPSearchMaxResults` and set it to the number of LDAP entries to display in Web Reports.
4. Restart the `BES Web Report Server` service.

On Linux systems:

1. Open the `/var/opt/BESWebReportsServer/beswebreports.config` configuration file.
2. Add the `LDAPSearchMaxResults` in the `[Software\BigFix\Enterprise Server\BESReports]` section as follows:

   ```
   LDAPSearchMaxResults = <max_number_LDAP_entries>
   ```

   where `<max_number_LDAP_entries>` is the maximum number of LDAP entries to display within Web Reports.

Note: The value assigned to the `LDAPSearchMaxResults` keyword applies to the query for users and to the query for groups. For example, if you defined in your LDAP 2000 users and 5000 groups and you set `LDAPSearchMaxResults = 1000`, then your queries about users and groups display up to 1000 users and 1000 groups.

SAML integration

Starting from V9.5.5, BigFix supports SAML V2.0 authentication via LDAP-backed SAML identity providers for the Web Reports and the Web UI components.

This support can be used to enforce two-factors authentication for BigFix with Common Access Cards (CAC), Personal Identity Verification (PIV) cards, or other factors. This configuration uses a web based Single Sign-On authentication method from the identity provider login URL. Logged on users are automatically redirected to the components supporting SAML V2.0 authentication without the need to log in again.

Be aware that, if you implement this configuration, LDAP operators must login from the identity provider login URL and not from the usual Web Reports and Web UI login pages. Access to the BigFix Console is not affected by this enhancement.

For more information about SAML V2.0 authentication support, see Enabling SAML V2.0 authentication for LDAP operators and https://bigfix-wiki.hcltechsw.com/wikis/home?lang=en-us#!/wiki/BigFix%20Wiki/page/SAML%20V2.0%20Authentication%20Support.

Compatibility with NT domains

The information contained in this topic allows your user ID to login to Web Reports with the role assigned if:

- The user ID is defined on both the NT domain and the Active Directory.
- The name of the domain used for NT authentication is different from the name of the domain specified in Active Directory.
- You integrated the Active Directory with the Web Reports in your BigFix environment.

If all the conditions are true, run the following configuration steps on the system where the Web Reports component is installed:

On Windows systems:

1. Open the registry.
2. Select:

   ```
   HKLM -> Software -> Wow6432Node -> BigFix -> Enterprise Ser
   ver -> BESReports
   ```

3. Specify the file converter as follows:

   ```
   NTDomainFilePath = FullPathConversionFile
   ```

   where *FullPathConversionFile* is the path name to a file containing a row for each domain name conversion that must be applied to the domain names, for example:

   ```
   my_NT_Domain|my_LDAP_domain
   ```

4. Restart the Web Reports service.

On Linux systems:

1. In the configuration file `/var/opt/BESWebReportsServer/beswebreports.config`, specify under `[Software\BigFix \Enterprise Server\BESReports]` the file converter:

   ```
   NTDomainFilePath = FullPathConversionFile
   ```

   where *FullPathConversionFile* is the path name to a file containing a row for each domain name conversion that must be applied to the domain names, for example:

   ```
   my_NT_Domain|my_LDAP_domain
   ```

Note: Ensure that each row of the file ends with a line break of the same type as used in Windows systems (CRLF).

2. Restart the Web Reports process.

After you complete these steps, the user can log in using the NT domain credentials, for example *my_user@my_NT_domain.com*, and successfully access the Web Reports.

Chapter 3. Using the Program

The Web Reports interface is simple and straightforward.

You can create a specialized report and then print it or email it in only a few minutes, as the following tutorials demonstrate. These are quick step-by-step explorations of some of the most popular features in Web Reports, which can help you appreciate the scope of the program. Although brief, they explore a large fraction of the program functions.

First Login

Depending on the operating system where the BigFix Server is running you can have a different type of login to Web Reports.

To login to Web Reports running on Windows use the local browser to point to local host as follows: `http://localhost/webreports` and define the first Web Reports userid. After the userid definition, you can use a remote browser.

To login to Web Reports running on Linux use the userid and password of the BigFix administrator, defined at installation time. With this userid you can specify the Web Reports address in a remote browser such as: `http://HostnameWebReportsServer/webreports`

Note: If you enabled BigFix to use SAML V2.0 authentication, the LDAP operators will log in to Web Reports at the following URL `https://<bigfix_server>:8080`, where 8080 is the port number used by Web Reports, and their authentication will be managed by the Identity Provider. For more information, see What changes from the BigFix user's perspective.

Starting Web Reports

Web Reports is a stand-alone program available from the Start Menu.

You can also start it from within the console by selecting **Tools > Launch Web Reports**. The interface is divided into three main sections, which you access by clicking items in the navigation bar at the top of the window.

When you first log in to the Web Reports program, you see a startup window with several options.

In the main window you can see at least two icons:

- **Starred:** This option shows a list of the reports that you have starred as important.
- **My Authored:** This option shows a list of reports that you have personally authored.

Other possible icons are:

- **Domain Icons:** These icons can be selected to view the list of Web Reports associated with the selected domain, such as Endpoint Protection or Security Configuration.

At the top of the window you can see a search box and two user selections:

- **Search Computers:** The search box, top right, allows you to select computers by name, IP Address, OS, CPU, and Last Report Time.
- **Preferences:** For your personal login, you can set preferences including your opening splash page and the number of results you want to print on each page. For more information, see Setting Your Preferences *(on page 37)*.
- **Logout:** Click this to exit from the program.

Below this are the three main section headers in tab form:

- **Explore Data:** This option lets you filter and view your data on your BigFix clients, Fixlet messages, tasks, actions, operators, and more. This option also allows you to create your own custom reports as well as graphical charts. For more information, see Part Three, **Exploring**.
- **Report List:** This option shows all the reports, built-in and custom, that are available to you. You can filter the reports, modify their visibility, and set up schedules for printing them out. For more information, see Part Four, **Reporting**.
- **Administration:** This option lets you manage scheduled activities, database settings, and user databases. For more information, see **Administering the Program**.

The Explore and Report headers represent the primary functions of Web Reports. **Explore Data** lets you view your data with various filters. When you have narrowed your focus to the ideal data set, you can save it as a report that you can reuse or customize with just a few mouse clicks.

The reports that you author are shown in the **Report List** for easy selection. When you create and customize your favorite reports, this is where they are listed.

In the next sections of this guide, you can see how to use this program to create focused reports customized to suit your particular corporate network and policies.

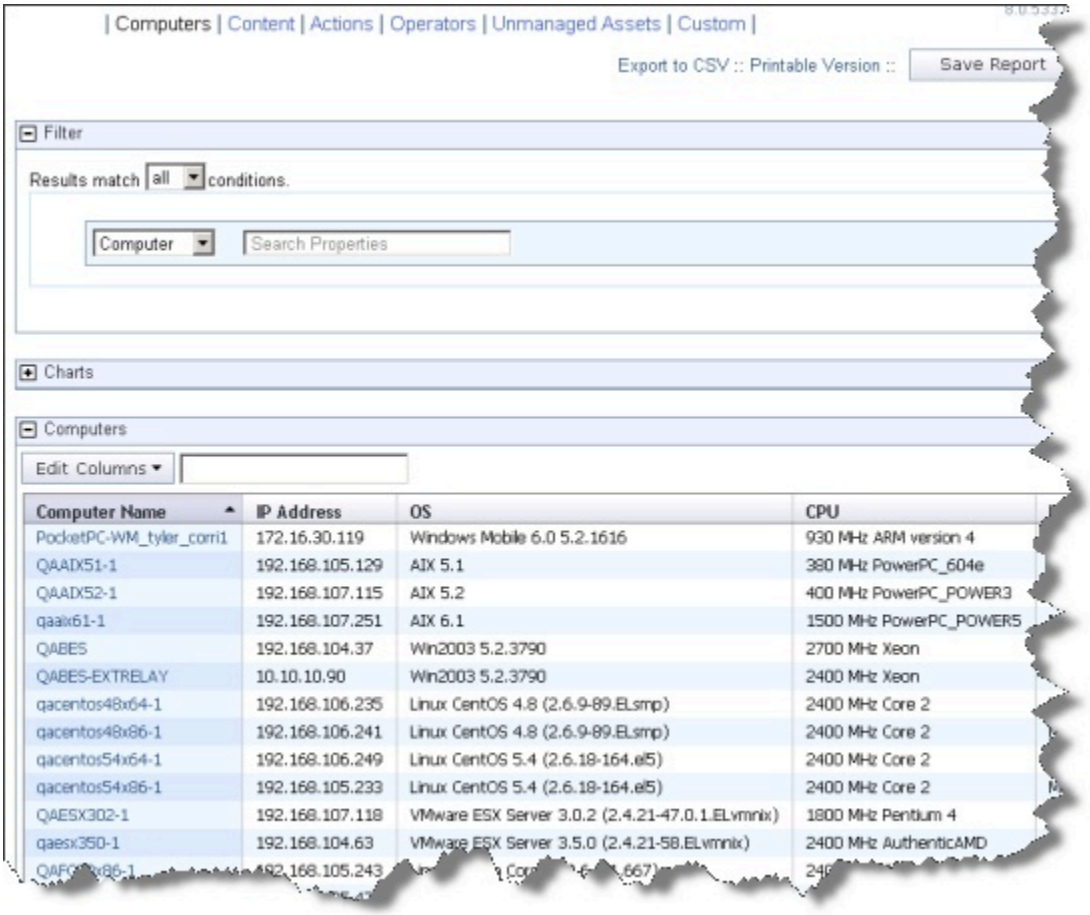
Viewing the Data

The first thing you might do is simply to view the data that Web Reports has aggregated from your BigFix databases.

To do this, follow these steps:

1. Click **Explore Data** from the top tab bar.

2. The default is the **Computers** report, and it is already displayed for you.



This important report is only one click away. Notice at the top that you can explore other data sets, including Fixlet **Content**, **Actions**, **Operators,** and more.

Also notice the Filter section above the report. The next topic describes how to use the filter to narrow your focus.

Filtering the Data

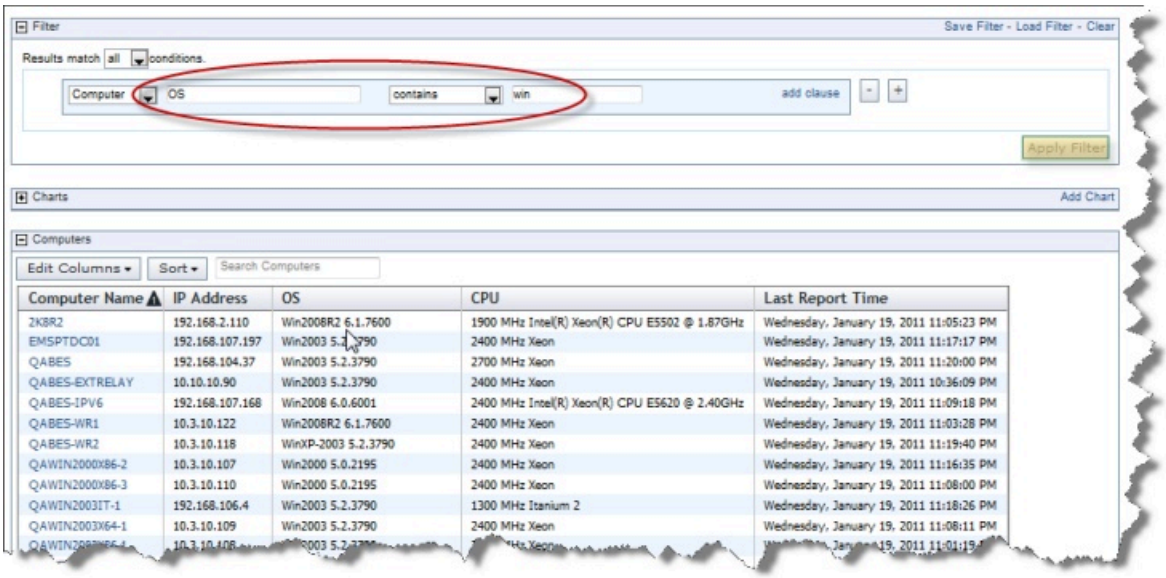
The Filter section is a key component of both exploring data and creating reports.

With effective filtering, you can highlight just that segment of the data that is most important to you. Filters are essential for creating relevant reports.

For example, to view just Windows computers, you might filter your computers like this:

1. Click **Explore Data** from the top tab bar.

2. The default **Computers** report is displayed. It displays all the computers in the database.



3. Click in the box next to the pull-down menu that says **Computer**. A pull-down menu opens, allowing you to select from the hundreds of computer properties defined across your network.
    a. Select **OS** from the menu, or simply type it in and hit Enter.
    b. Another pull-down opens with a list of operators. Select **contains.**
    c. A text box opens. Enter **win** to narrow the report down to Windows computers only.

Note: Another way to locate and select the property you need is entering the partial name of the property. To refine your search, you can use the characters ^ and $ as described in the following examples.

To search for the **OS** property (exact match), enter:

```
^OS$
```

Or to search for the property named **Subnet Address** (exact match), enter:

```
^Subnet Address$
```

To search for all properties starting with **Last**, enter:

```
^Last
```

To search for all properties ending with **Time**, enter:

```
Time$
```

Note: Starting from Patch 9, the box next to the pull-down menu does not display more than 1000 properties.

4. Click the **Apply Filter** button to get an instant view of the impact of your filter.

Saving Reports

When you have filtered a listing down to its essential core (as described in Filtering the Data (on page 21)), you can save your filter as a proper report.

Simply click the **Save Report** button at the top of the window and provide a name for your specialized report.

The name you provide is entered into the Report List, and labeled with you as the author.

Warning: The custom reports store some files in the following directories:

on Windows

```
BES Server\BESReportsServer\wwwroot\ReportFiles
```

on Linux

```
/var/opt/BESWebReportsServer/wwwroot/ReportFiles
```

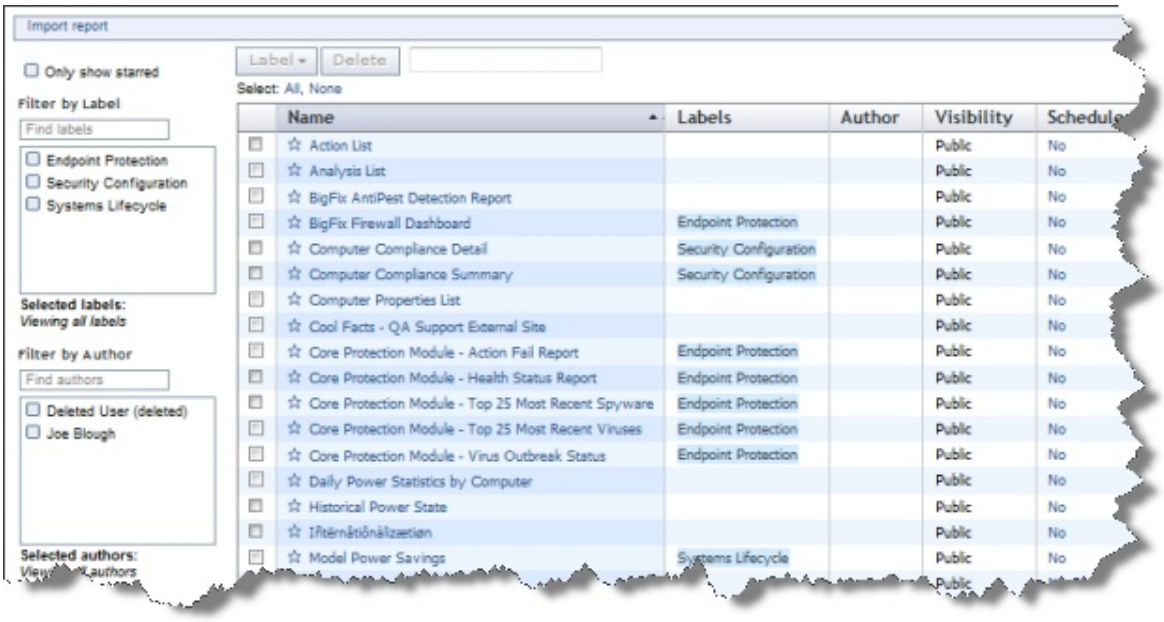
These folders might require a big amount of disk space, depending on the amount of custom reports activated in the deployment. Take into account that these folders are used also by some official sites, when they deliver these types of reports.

Viewing Reports

How to view reports.

1. Click Report List from the top tab bar.

2. The list of reports is displayed.



Simply click one of the links to see the associated report.

These reports are available by default:

- Action List
- Analysis List
- Computer Properties List
- Open Vulnerabilities List
- Operating System Distribution
- Operator List
- Overview
- Progress of 10 Fixlets from Recent Actions
- Progress of 10 Fixlets Recently Relevant
- Vulnerability Trends Over Time

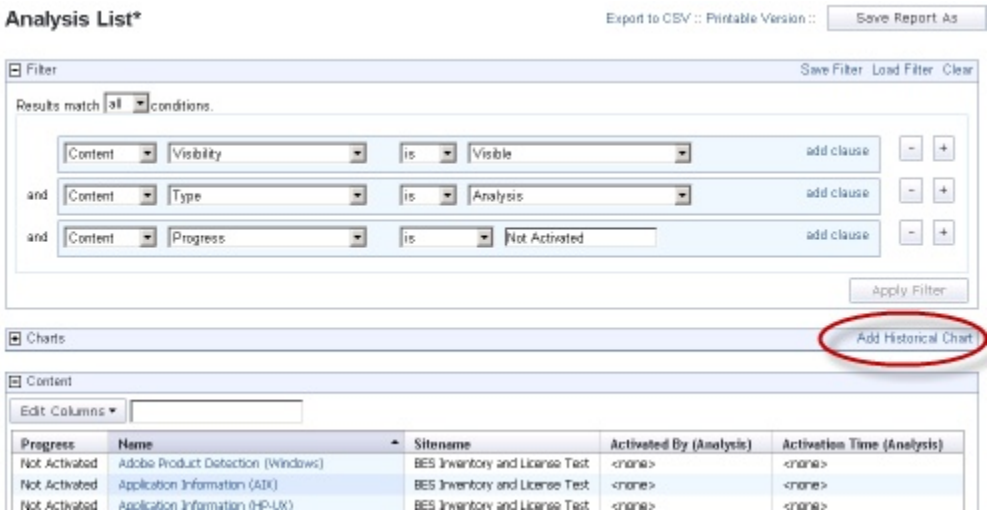
3. Note the boxes at the left of the window that allow you to filter the reports by label and author to help you keep your report list short and uncluttered. Simply click the check box in front of the filter. Multiple filters are ORed together.

There are several useful features in this section. For more information, see the Report List main page.

Creating Charts

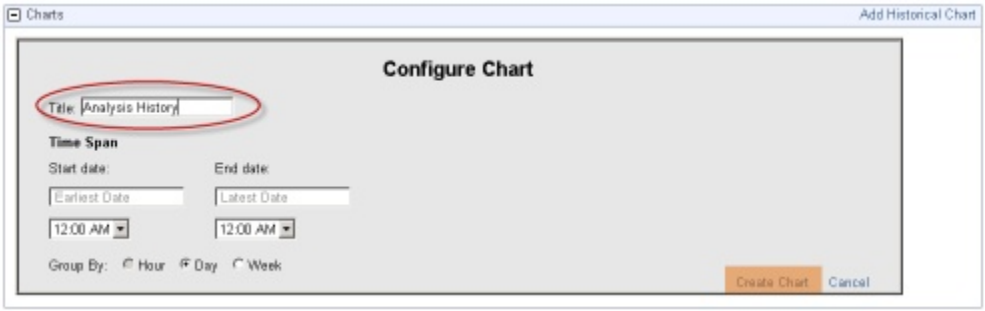
Most data views and reports can display the data graphically.

From Explore Data or a Report listing, if a chart is possible, it is shown in a section just below the filter section.

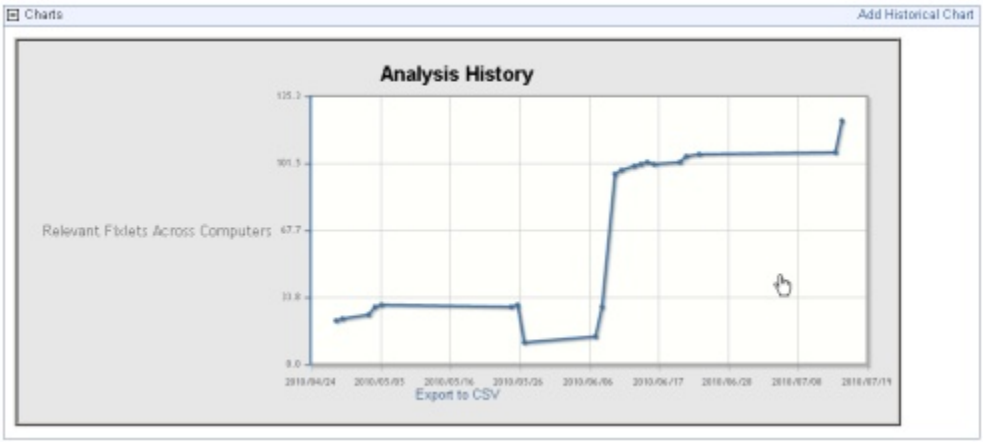


There are two basic chart types: ordinary and historical.

1. Click the link to create a new chart. You can attach multiple charts to a report.
2. Enter the title for a historical chart and click **Create Chart**.



3. Your chart is generated immediately.



Charts are useful for distilling a huge list of data into a simple graphic, and are extremely useful for busy administrators.

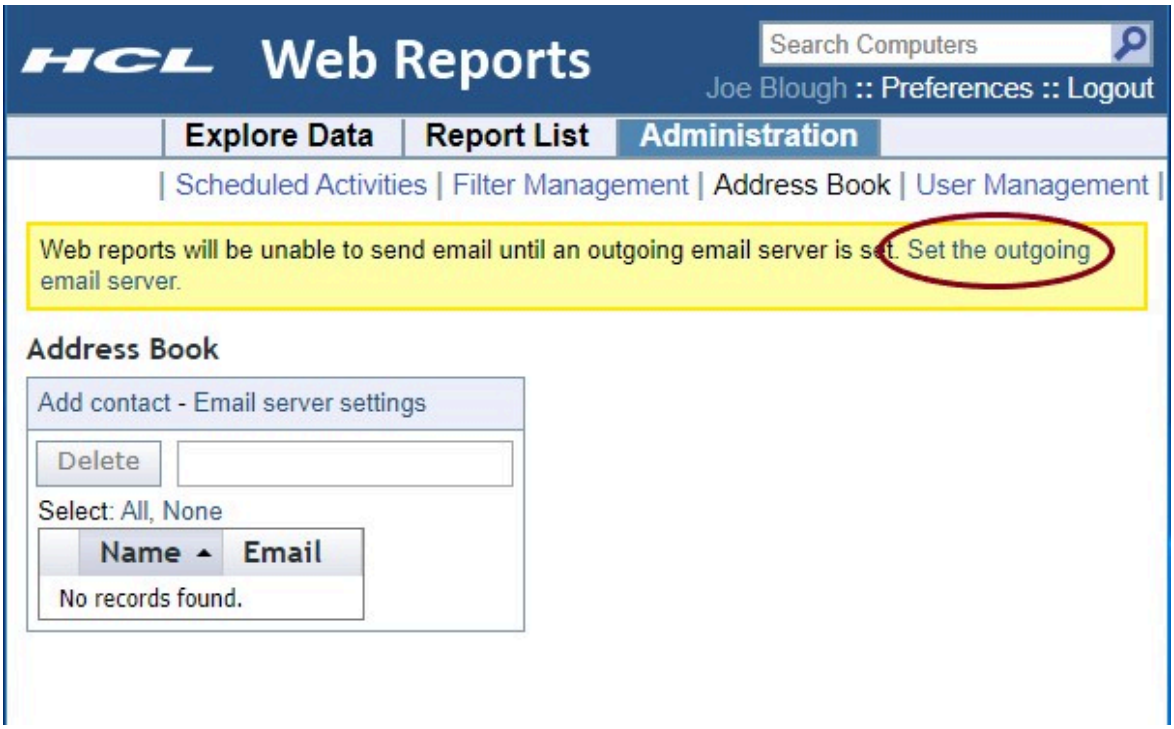
Setting Up Email

A common need is to have a report mailed to an operator or an administrator who can then easily examine various aspects of your BigFix network at their leisure.

Set up your email accounts and server as follows:

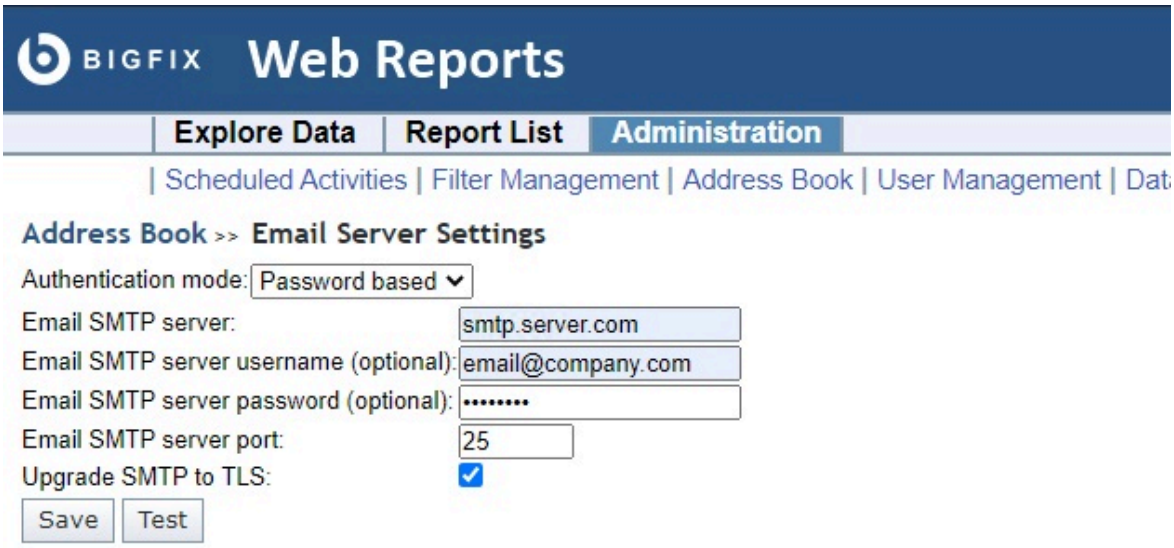
1. Click **Administration** from the top tab bar.

2. Click **Address Book** from the sub tabs.
3. If you have not yet set your outgoing SMTP server, click the link in the yellow reminder message.



4. For Version 10 Patch 1, specify which authentication mode you intend to use. Depending on the authentication mode you select, the Email Server Settings panel changes and requires different information.

   If you choose **Password based** as authentication mode:



Enter your SMTP server name.

Enter your SMTP server port. It must be a value between 1 and 65535. Before upgrading to Version 9.5 Patch 10, this value was hard-coded and set to 25.

Specify if you want to upgrade the SMTP connection to TLS by selecting the related check box.

(Optional) Enter your SMTP server user name and password if your SMTP server requires authentication. The authentication methods used are:

- PLAIN
- LOGIN
- DIGEST-MD5
- CRAM-MD5

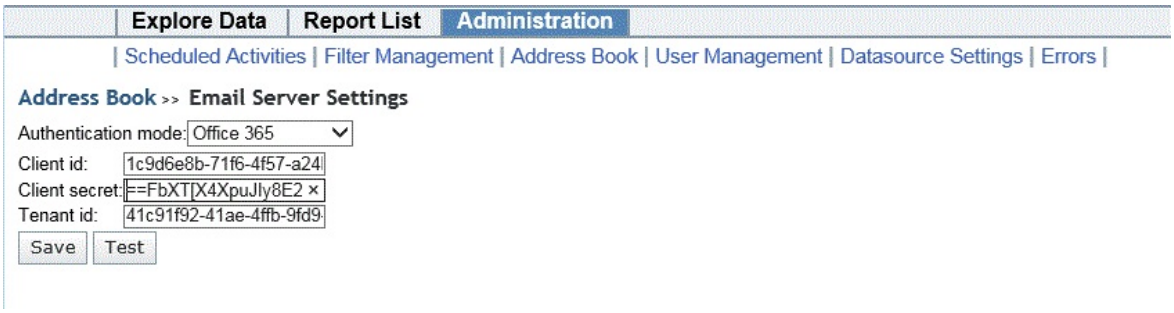
The specified user name and password are saved in the Web Reports settings named `EmailServerUser` and `EmailServerPassword` respectively.

In a FIPS mode, do not configure your SMTP server to use the following authentication methods:

- CRAM-MD5 only
- DIGEST-MD5 only
- CRAM-MD5 and DIGEST-MD5 only

Test the SMTP server before saving it.

If you choose **Office 365** as authentication mode:



Enter your Client ID, Client secret, and Tenant ID provided when registering the application on the Microsoft Azure portal.

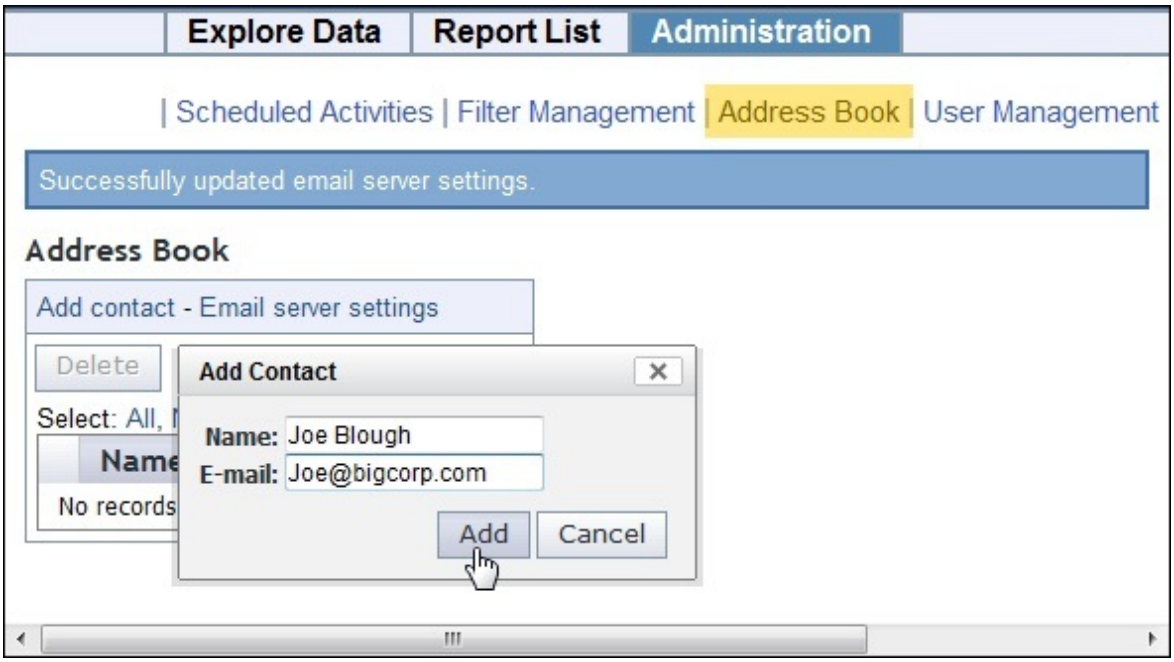
Note: When registering on the portal, you must request the ***Mail.Send*** permissions for the Microsoft Graph API.

Note: You should specify a default "From:" address for emails sent from Web Reports, using the related configuration option, otherwise the email setup test will not work. This option can be set in the Windows Registry or in the Linux configuration file under the `<BigFixMachineKey>\Enterprise Server \BESReports\EmailFromAddress` path.

Note: If you configured **Office 365** as SMTP server in Web Reports, the following known limitation applies: you cannot send emails containing attachments larger than 3 MB.

Test the Email server before saving it.

5. Click the link labeled **Add contact** to add name(s) to the Address Book.



6. Continue to add contacts. If you need to delete a contact from the Address book, check the box in front of the name and click the **Delete** button.

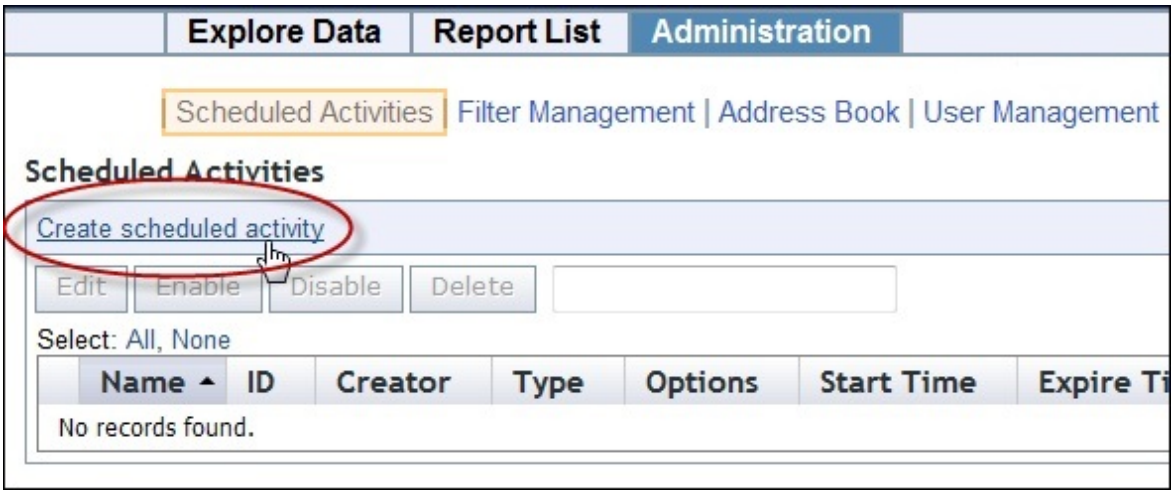
You are now set up for emailing from Web Reports.

Scheduling Reports

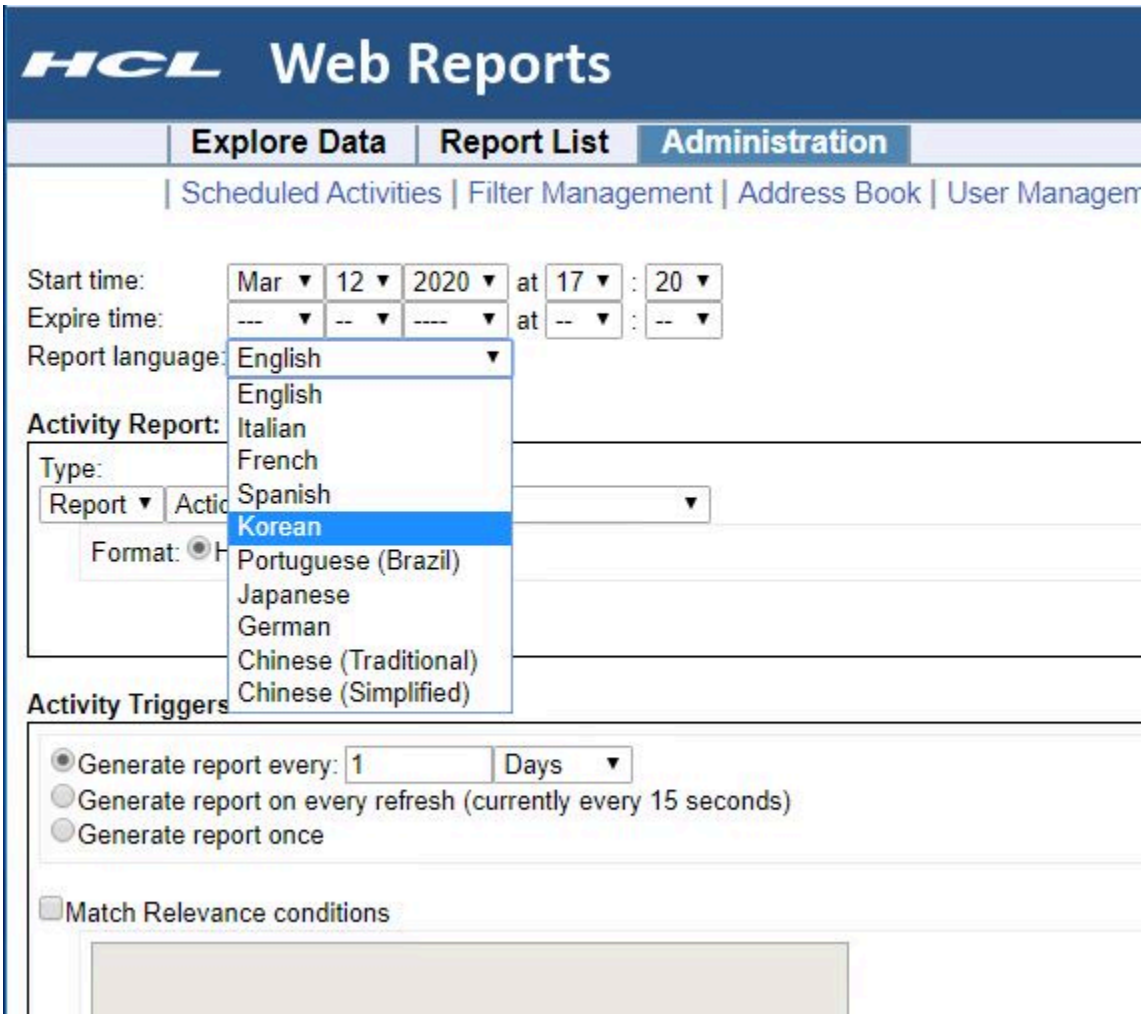
When you have your email server set up and your Address book populated, you are ready to schedule a report and email it to yourself or another operator.

1. Click **Administration** from the top tab bar.

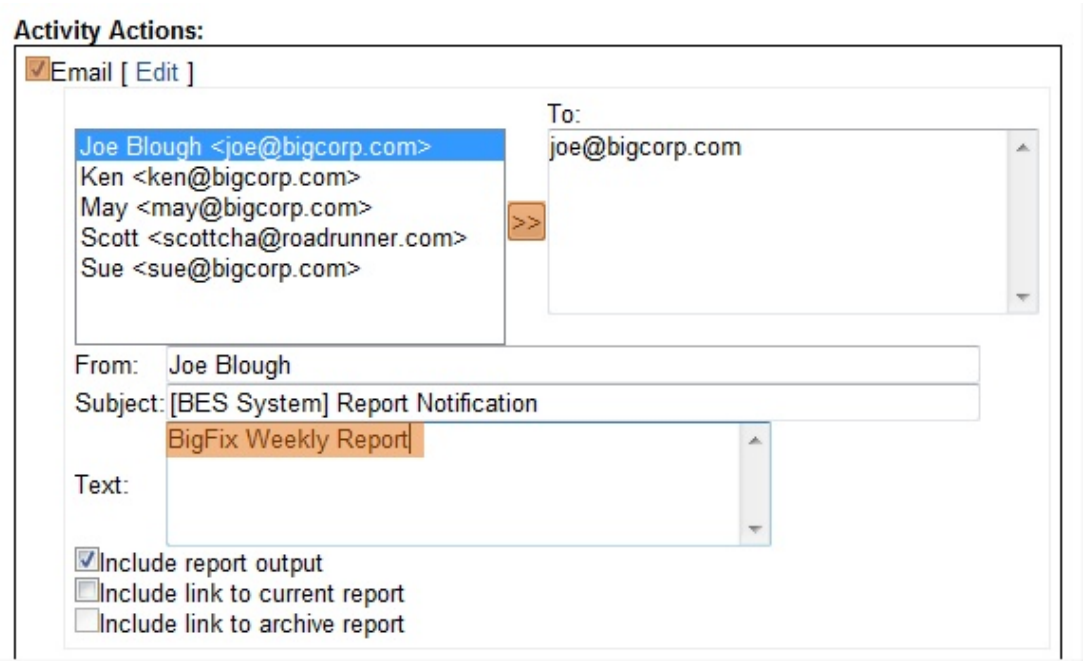
2. Click **Scheduled Activities** and click the **Create scheduled activity** link to create your custom event.



3. In the linked page, you can create triggers for your events as well as the actions that you want to trigger.



4. The Start time defaults to the current time, and is often what you want.
5. From the Report language choose the language of your report.
6. Complete the following sections:
    a. The **Activity Report** section is where you select the report you want to schedule, as well as its format. From the pull-down menu, select the report you want.
    b. The **Activity Triggers** section is where you specify how you want to trigger your event. The most popular technique is to set a time period, such as every day or week, to trigger the report (or other activity). However, there are many other useful ways to trigger a report, as described later in this guide.
    c. The **Activity Actions** section is where you select the action you want to trigger.



Typically that is just to email your report. To do this, click the Email check box, add contacts from your Address book, and set the subject line for the emailed report.

7. When you have finished, click Submit.

You can now set up reports and alerts to be sent or archived on your schedule.

Adding a Datasource

You can add other BigFix datasources to your reports.

This allows you to create aggregate reports covering hundreds of offices, each with thousands of computers. Note that, it is not possible to aggregate datasources whose Web Report servers have a different FXF encoding.

Ensure that the schema versions of the aggregated datasources are the same. You can see the schema version of every `BFENT` database, by running the following query:

```
select version from dbo.DBINFO
```

To add a datasource, credentials of a Master Operator must be provided. These credentials are required only once per datasource, and are not saved.

To add a new datasource, follow these steps:

1. Log in as an administrator.
2. Select **Administration > Datasource Settings > Add New Datasource**.

3. The Add Datasource page is displayed.

Enter a descriptive **Name** for your datasource.

4. Enter the URL of the root server you wish to connect to. The URL must also include the appropriate port number.
5. Enter **Master Operator Credentials**. These credentials are used only once, and are not saved.

Editing a Datasource

To edit a datasource, follow these steps.

1. Log in as an administrator.
2. Select **Administration > Datasource Settings > Edit**.

3. The **Edit Datasource** page is displayed.

Enter the URL of the root server to which to connect. The URL should also include the appropriate port number.

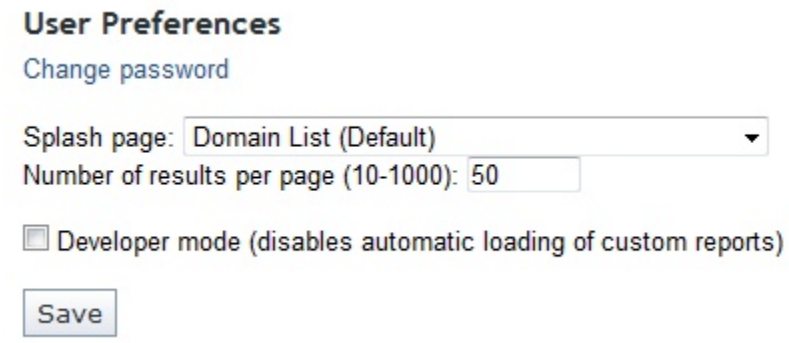
Note: You cannot change the name of your datasource.

4. Enter the Master Operator Credentials if the URL is changed.
5. When you have finished, click **Submit**.

Setting Your Preferences

At the top right of the Web Reports interface is the Preferences link.

Click it to edit your personal user preferences.



1. Use **Change password** to change the password of the currently logged on user. After clicking **Save**, you are automatically redirected to a new page where you must perform again the current user authentication as described in Performing the reauthentication *(on page 40)*.
2. Change your splash page by selecting a new page from the pull-down menu. As well as the default Domain List, you can select from a list of reports to appear in the starting splash page.
3. When you view a report, the number of rows is typically limited to 50 per page. You can change that number here.
4. You can check the box to run in Developer mode, which disables the automatic loading of custom reports.
5. Click **Save** to set your preferences.

Enabling FIPS cryptography on Web Reports

After installed, you can set up your Web Reports server to encrypt using FIPS cryptography.

To enable FIPS encryption, follow these steps:

1. From the **BigFix Management** Domain, open the **Computer Management** folder and click the **Computers** node.
2. Select the computer where the Web Reports server is running.
3. From the right-click context menu, select **Edit Computer Settings**.
4. From the **Edit Settings** dialog, click **Add**.
5. In the **Add Custom Setting** dialog, enter the setting name as

   _BESClient_Cryptography_FipsMode

   The values for this setting are:

   required

   Causes the client to encrypt using FIPS cryptography.

   none

   FIPS cryptography is not used.

Note: The client setting **_BESClient_Cryptography_FipsMode** overrides the FIPS setting specified in the masthead for the BES Client and the Web Reports components. When setting the value to **none**, the BES Client and the Web Reports components will not use the FIPS libraries. When setting the value to **required**, they will use the FIPS libraries.

6. Click **OK** to accept the value and **OK** again to complete the setting. You must enter your private key password to deploy the setting action.

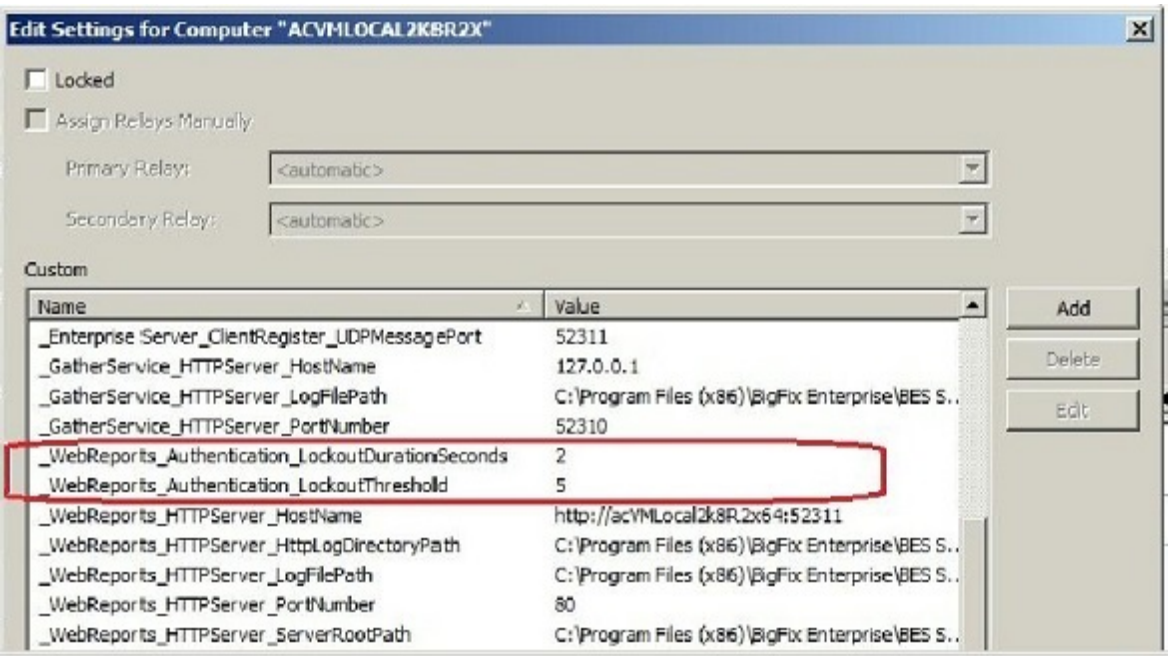
Setting the login lockout

You can set the number of invalid Web Reports login attempts that are allowed before an account is locked out.

If you are locked out, before attempting to log in again, wait for the lockout duration to expire.

To set the lockout, complete the following steps:

1. Click the **Computers** icon in the Domain Panel navigation tree to open the List Panel of client computers.
2. Select the computers on which to set the Web Reports login lockout.
3. Right-click and select **Edit Computer Settings** from the pop-up menu, or select **Edit Computer Settings** from the **Edit** menu. The Edit Settings dialog opens.



4. Change the lockout settings by editing the following keywords:

   `_WebReports_Authentication_LockoutThreshold`

   The number of invalid password attempts that are accepted before the user is locked out. Default value: 5

   `_WebReports_Authentication_LockoutDurationSeconds`

   The number of seconds for which a user is locked out after reaching the lockout threshold. Default value: 900

Note: Restart the Web Reports service to reset the lockout state for all users.

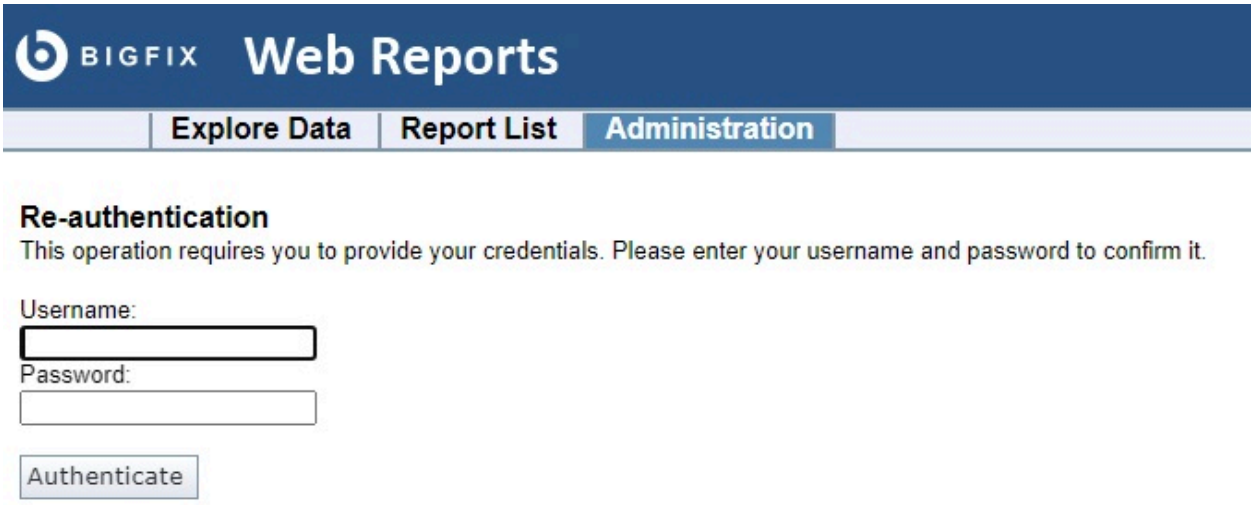
Performing the reauthentication

To enhance security for Web Reports, changes to some specific pages now require to re-authenticate using your current credentials.

You are now requested to re-authenticate when updating information on the following pages:

- Edit User *(on page 88)*
- Global User Options *(on page 86)*
- Step 2: Assign a Web Reports role to LDAP users or groups *(on page 8)*
- Setting Your Preferences *(on page 37)*

When this happens, you will be prompted to a new web page like the one shown below:



You must insert your login credentials, username and password, to permit the application to fullfill your request.

Chapter 4. Exploring

The **Explore Data** section of the program allows you to look at data collected from your entire BigFix network to filter it, and to create reports.

Click the **Explore Data** tab, upper left.

Want a quick peek at your network? This section of the program lets you instantly visualize your data with both charts and reports. It also allows you to filter that potentially huge data set down to something concise and useful.

Want to record your custom view? At any time you can press the **Save Report** button to save your filters, charts, and layouts, which are added to the **Report List** (available from the next tab to the right). Now you can reuse your custom template to quickly provide you with unique portraits of your network at any given moment.

There are several options for exploring Data. They make up the secondary tabs on this page:

- **Computers:** This option allows you to examine properties of your networked BigFix clients and filter the list into a specialized report.
- **Content:** This option allows you to examine and create specialized reports based on Fixlet messages, baselines, tasks, and analyses.
- **Actions:** This option allows you to list and report on actions taken on any of the BigFix clients in your network.
- **Operators:** This option allows you to list subsets of your BigFix operators.
- **Unmanaged Assets:** This option allows you to examine the states of all your unmanaged assets, such as printers, scanners, faxes, and more.
- **Custom:** This option allows you to create free-form listings and reports.

These options are described later in this section. However, many of these options have commonalities that represent core utilities of Web Reports. These are described in the following section.

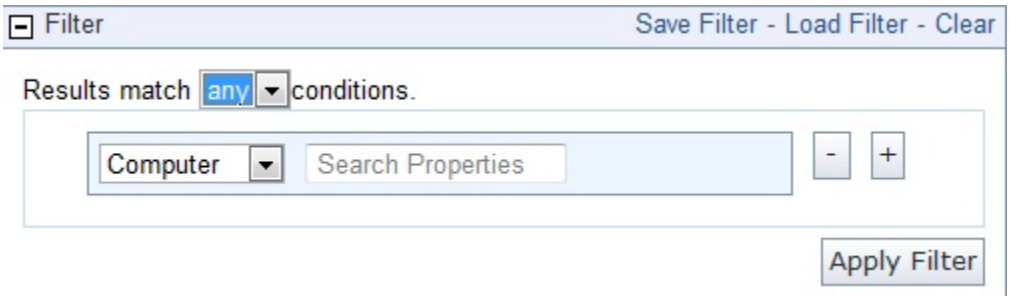
Filters

Filters are a key part of most reports.

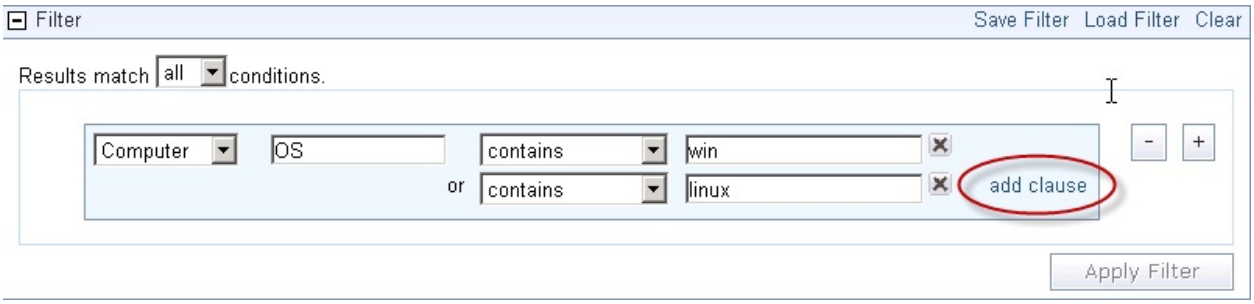
They allow you to view just one facet of the data at a time. Data fields can be filtered individually, limiting the data that is displayed. This technique is a form of Facet Navigation, and is a powerful way to reduce a huge data set to something easily tractable.

The Filter interface is nearly the same wherever you see it. This section highlights the essentials of designing powerful and effective filters, and is referred to elsewhere in this guide.

The **default filter** specifies nothing, allowing all data records to be listed.

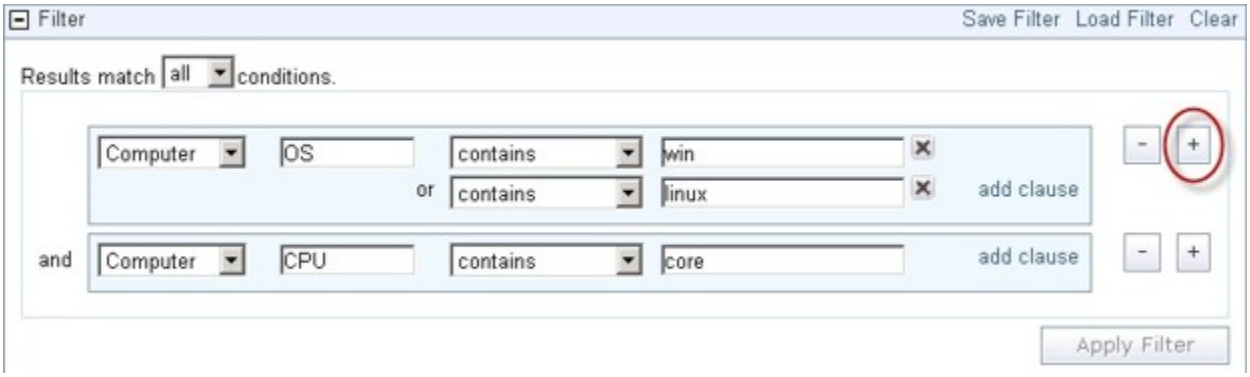


To view a subgroup of the data, pull down the menu to filter by **computer**, **content**, **site** or a previously saved filter. The choice you make determines the secondary fields of the filter. For example, you might want to view computers that have specific operating systems. Click in the box labeled **Search Properties** and enter "OS". There might be a pause while the system collects the properties and verifies the existence of the OS property.



Click the link labeled **add clause** to add extra qualifiers to a filter. Click the associated X to delete any of these clauses.

Click the plus sign to the right of the filter to add a new one.



These filters are ANDed together if you choose **all conditions**. They are ORed together if you choose **any conditions**. Click the minus sign next to a filter to delete it from the set.

Click the **Apply Filter** button to see how your custom filter affects the subsequent computer reports and charts.

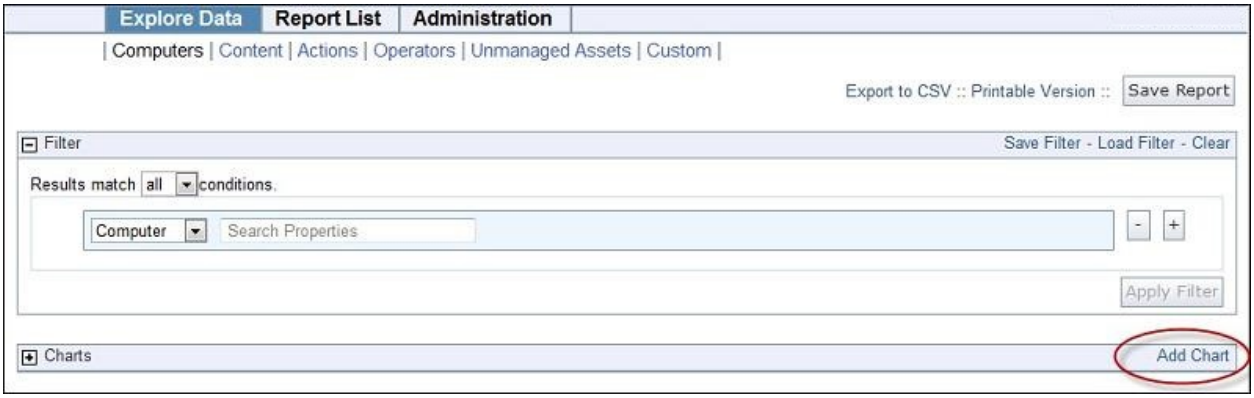
When defined, click the **Save Filter** link at the upper right if you want to save your work as a custom named filter. Later you can use this filter in other circumstances by clicking the **Load Filter** link or by selecting it from the conditions pull-down menu.

Charts

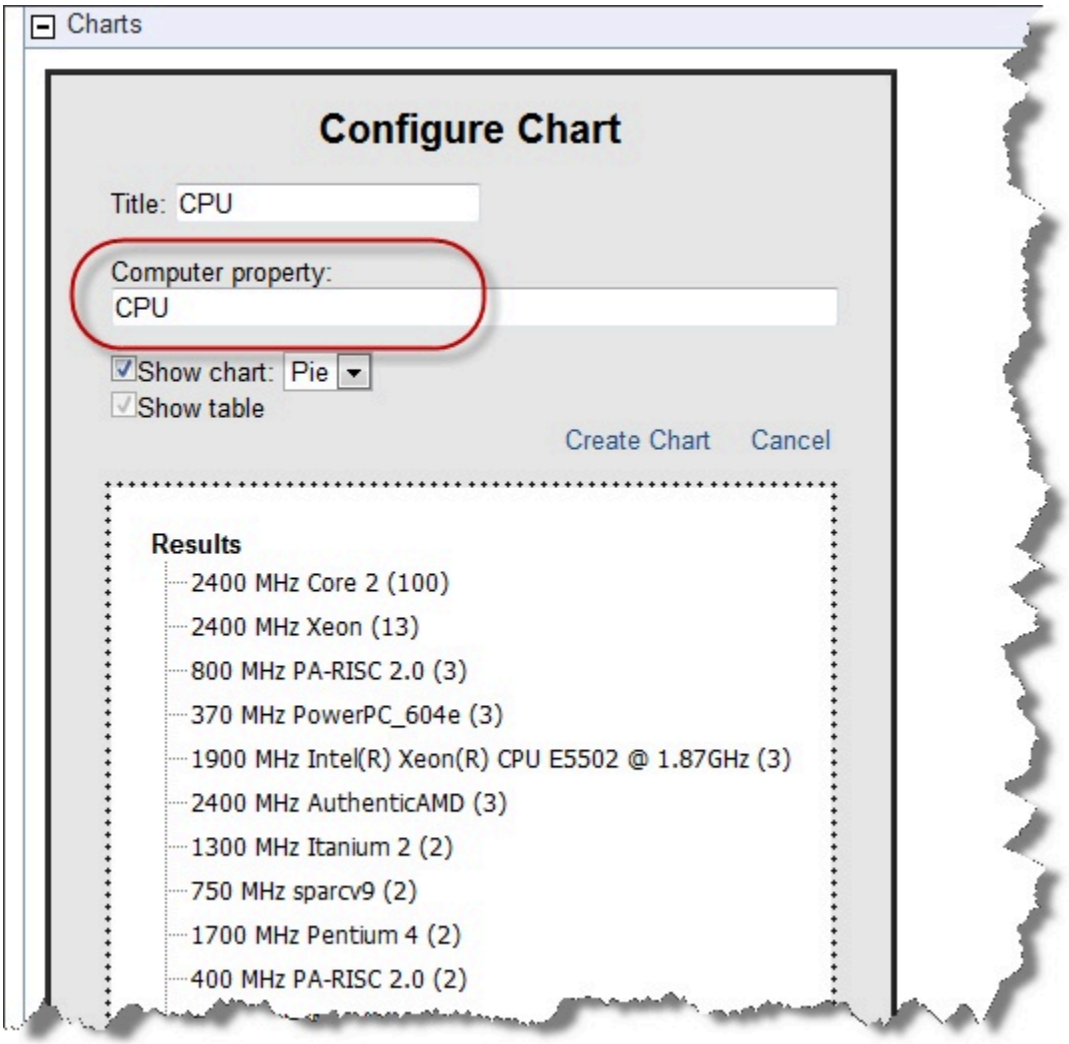
Reports often include a chart to summarize the data. Charts and graphs help to clarify major trends hidden in a detailed list.

Depending on the data, you can make pie charts, columnar graphs, or historical trend sheets with just a few mouse clicks.

If a chart is available, the interface can be found immediately beneath the Filter interface. Click the **Add Chart** link.



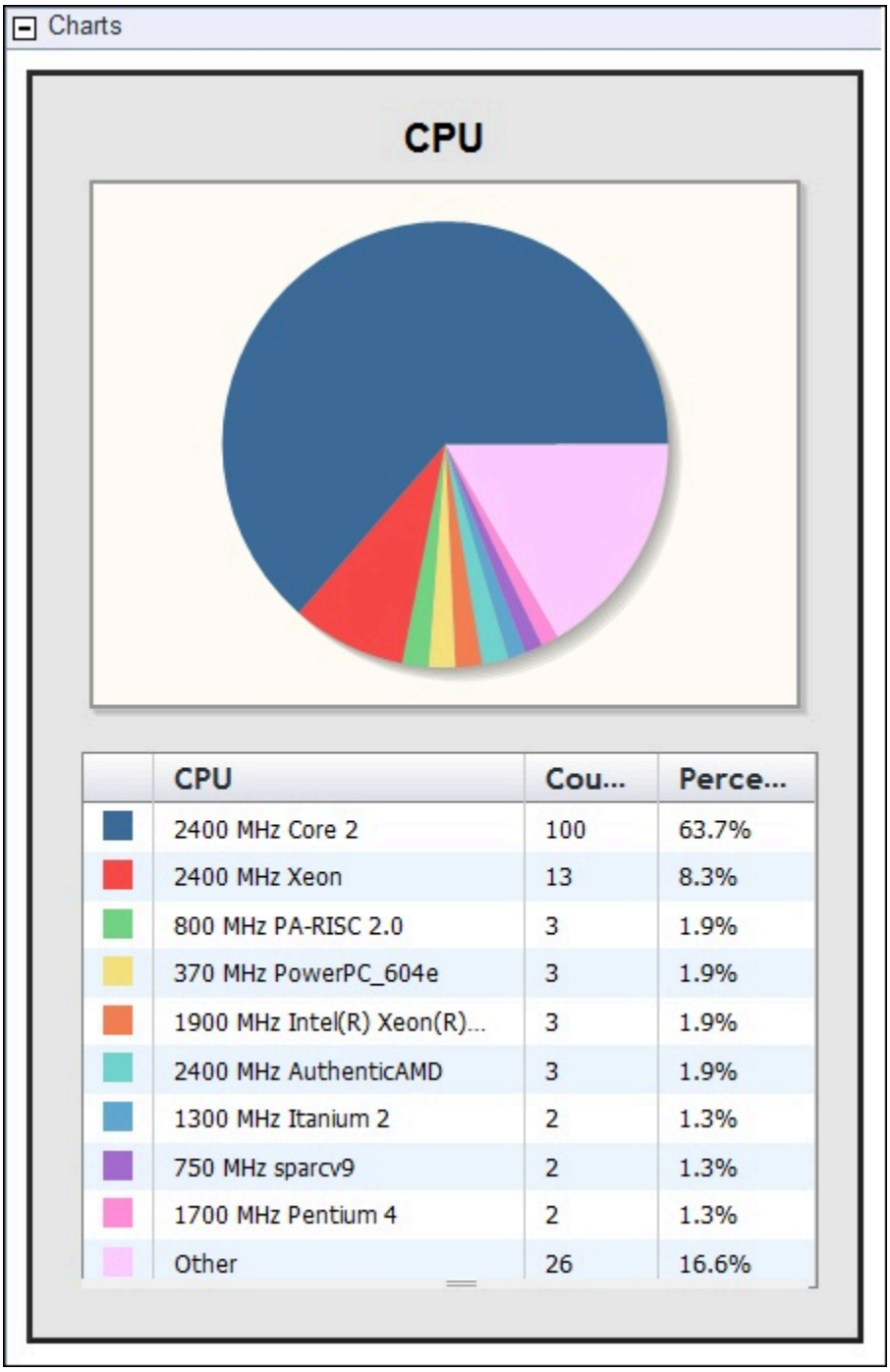
Depending on the data set you are looking at, the Chart Wizard has a default setup that is appropriate. For a chart on computers, the wizard prompts you for a computer property.



Here we have used the pull-down menu to chart CPUs on our network. The title is automatically filled in to reflect our choice of computer property. You can change it if you want. Note that a typical chart includes a table below it. Use the check boxes to specify whether you want a chart, a table, or both.

We have kept the default pie chart, but we could have chosen a bar chart instead. In the dotted box at the bottom of the wizard, you can choose to give some extra order to the data by grouping records together.

When you are ready, click the **Create Chart** link.



	CPU	Cou...	Perce...
	2400 MHz Core 2	100	63.7%
	2400 MHz Xeon	13	8.3%
	800 MHz PA-RISC 2.0	3	1.9%
	370 MHz PowerPC_604e	3	1.9%
	1900 MHz Intel(R) Xeon(R)...	3	1.9%
	2400 MHz AuthenticAMD	3	1.9%
	1300 MHz Itanium 2	2	1.3%
	750 MHz sparcv9	2	1.3%
	1700 MHz Pentium 4	2	1.3%
	Other	26	16.6%

Note that we created this chart simply by selecting a single item (CPU) from a pull-down menu.

When you mouse over a chart, a tool bar appears.

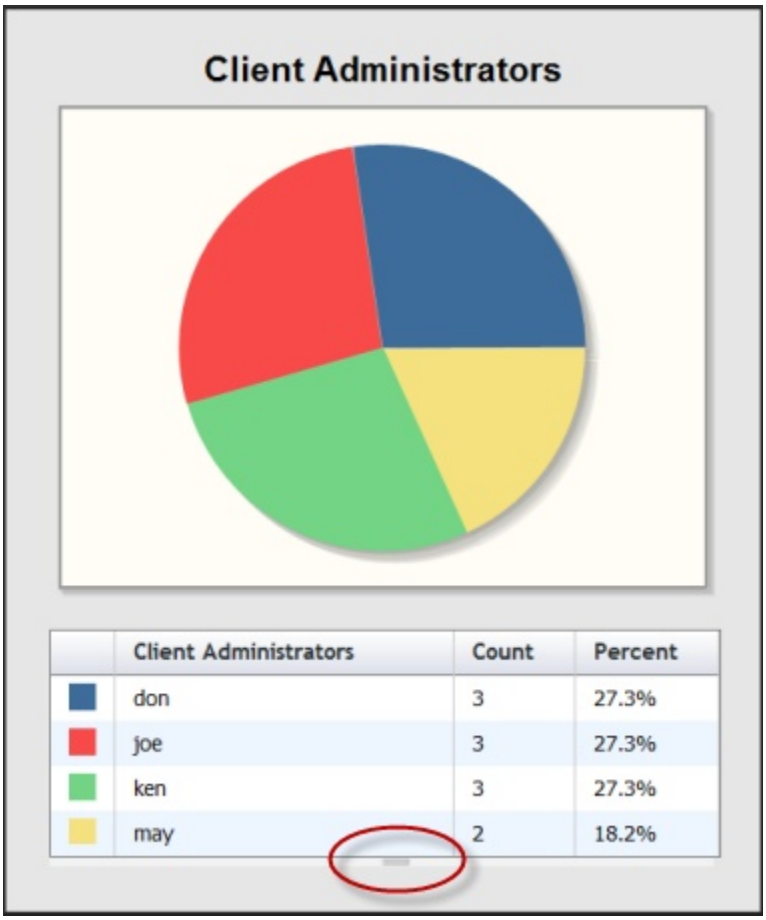
The top icon lets you delete the current chart, and the wrench lets you edit the chart.

Note: After creating the chart, you can no longer move it.

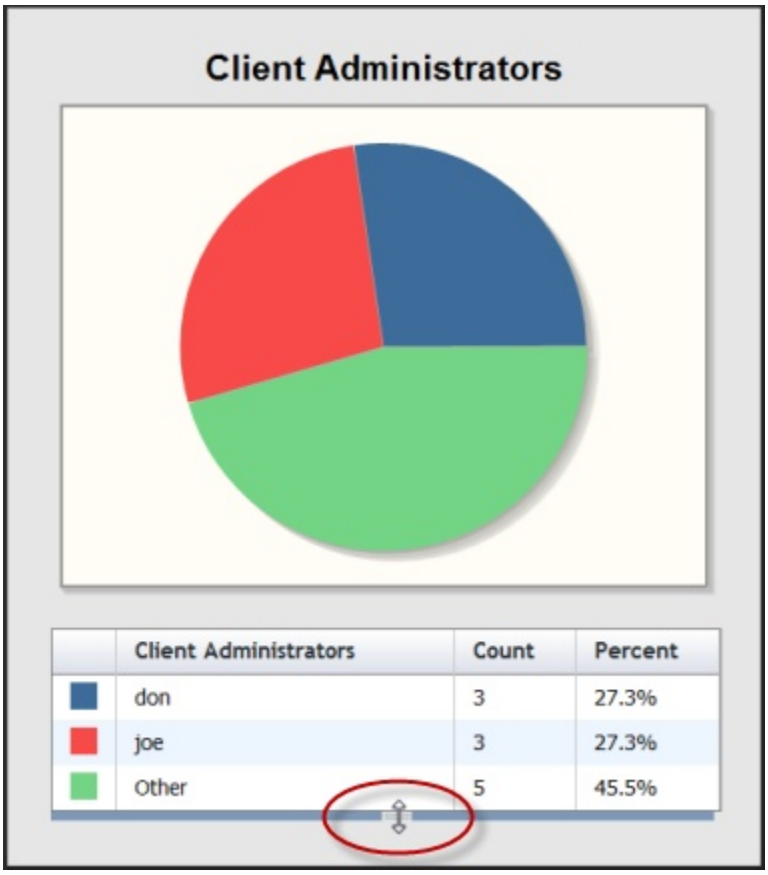
Collapsing the Table

When a chart is complete, you have another final option for editing.

A small handle is available at the bottom of the list and you can drag it up or down to truncate the list.



When you change the list, the truncated items get summed into an "Other" category and the chart is dynamically updated to reflect the change.



Here, Ken and May are collapsed into the **Other** category. You can continue to **Add Charts** by clicking on the link at the top of the UI.

Columnar Report

This section is directly below the Charts section.

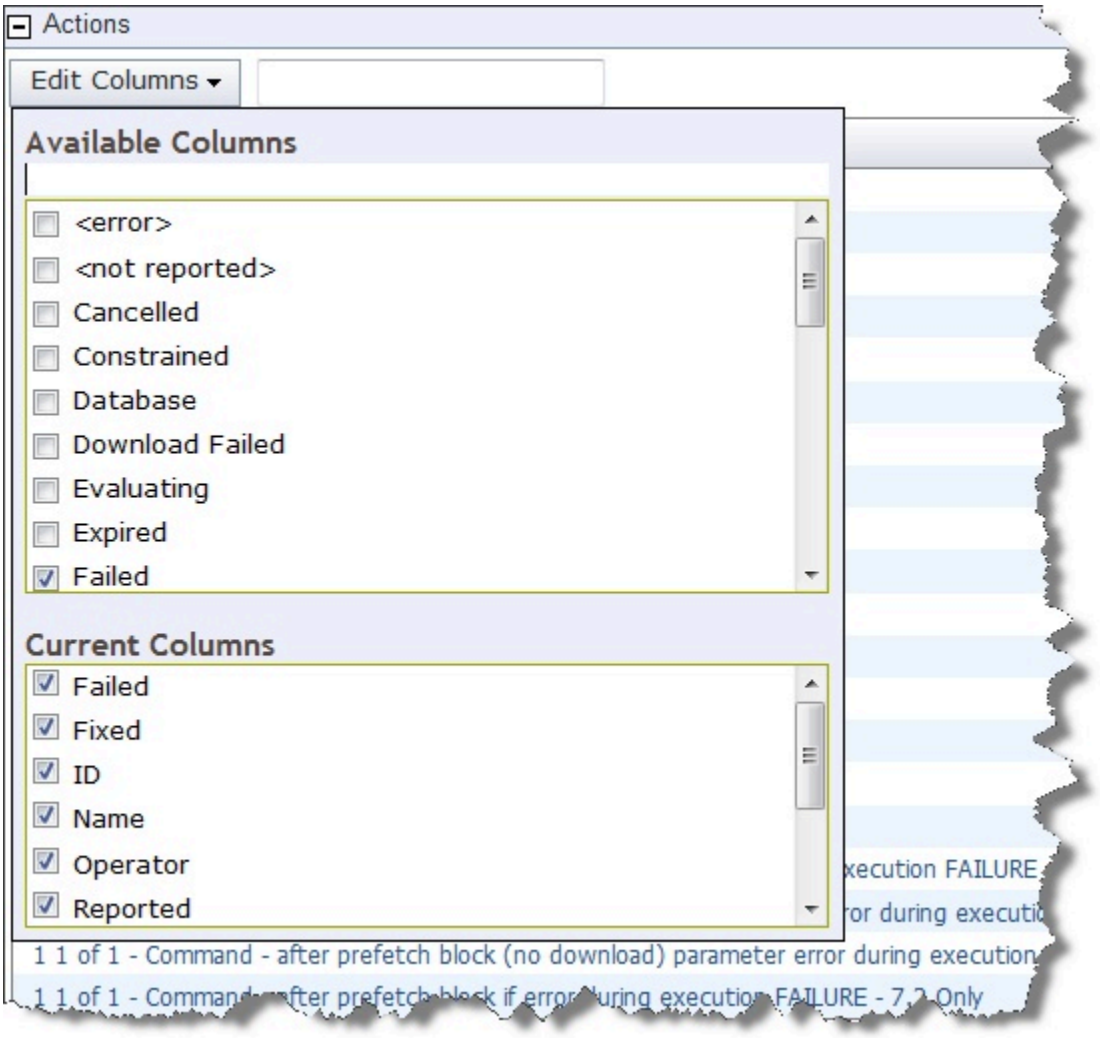
It is named after the data set under review, such as Computers, Content, or Actions.

Edit Columns

Click the **Edit Columns** button (at the top of columnar views and reports) to change which columns you want to display in your report.

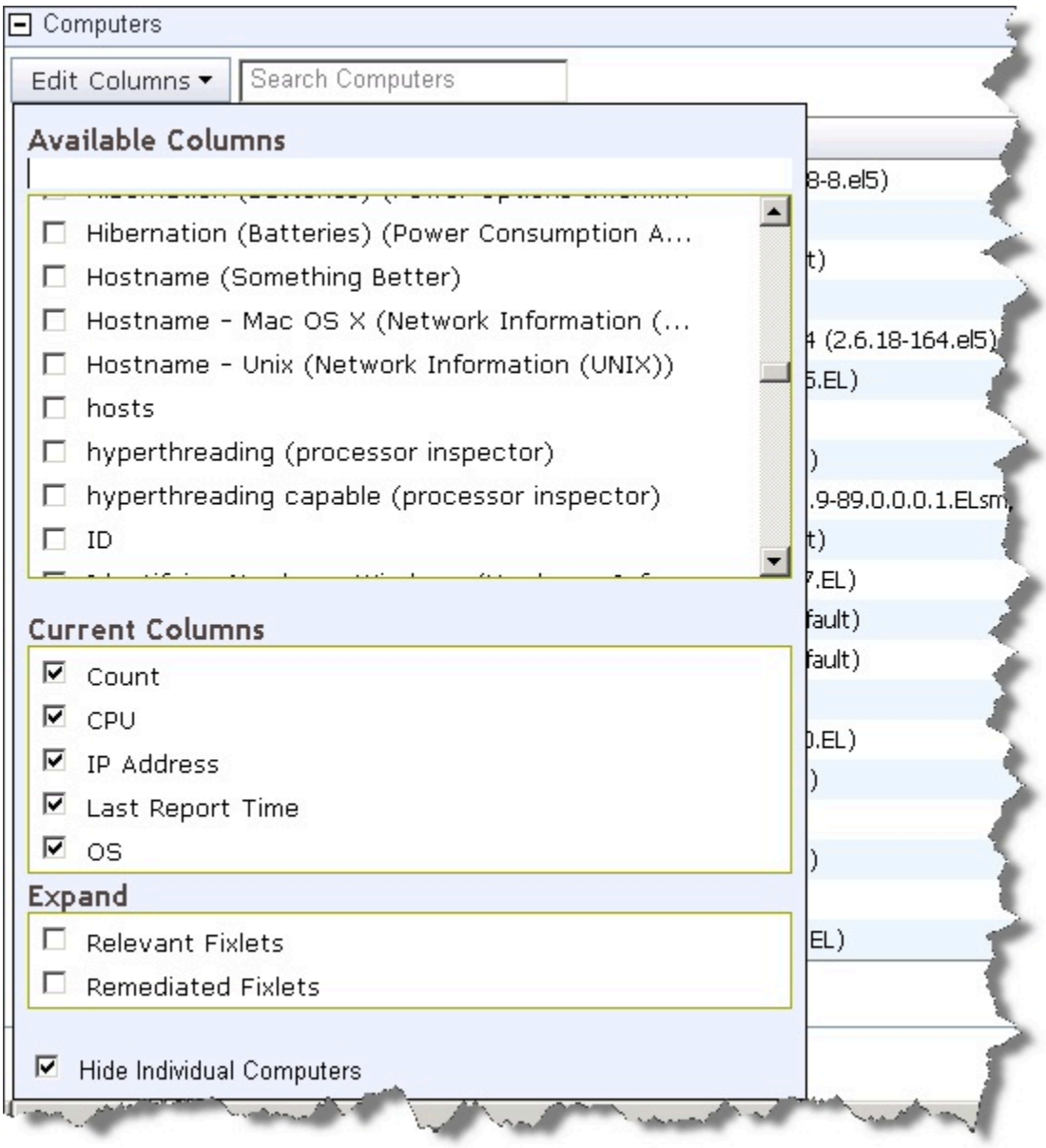
It shows a menu of column headers that you can add and delete to create the most information in the least number of columns.

It shows the first 1000 properties. If the property you need is not among the first 1000 properties, you must search for it. You can refine the search using the characters ^ at the beginning and/or $ at the end of the string that you are searching for.



This example is from an Action report, so the headers all refer to fields in the Action database. When you check an item in the Available Columns box, it is added to the Current Columns box. When you clear an item, it becomes cleared in both boxes. The Current Columns box is generally smaller, letting you see the column layout at a glance, without having to scroll through the lengthier list of Available Columns.

The options for columns depend on what you are looking at. For computer columns, there are more possibilities.



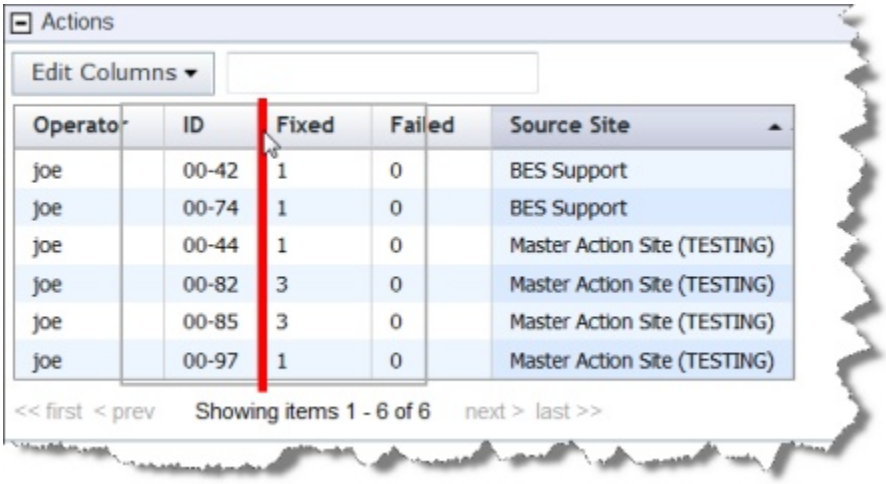
The Expand section lets you add Relevant or Remediated Fixlet messages to the Computer list. Note that there is a check box to **Hide Individual Computers**, which lists the computer count instead of individual computer names.

The Expand section for Content lets you add Applicable and Remediated Computers to the list.

Changing Column Order

To change the order of any column in your report, simply click and drag the column to where you want it.

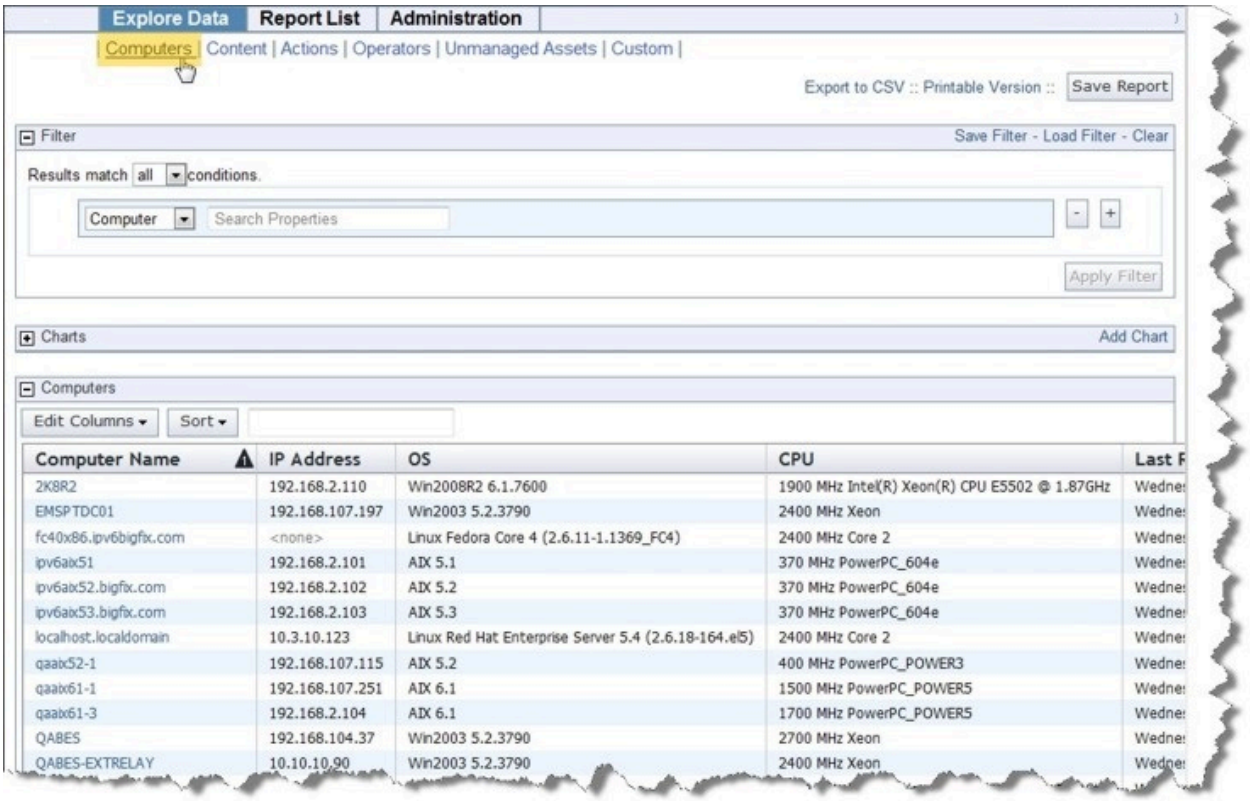
A red line indicates legitimate targets as you drag the column.



Both editing and moving columns are available when exploring data or viewing a columnar report, allowing you to customize the output to your particular needs. To keep your changes, be sure to save your report when you are finished.

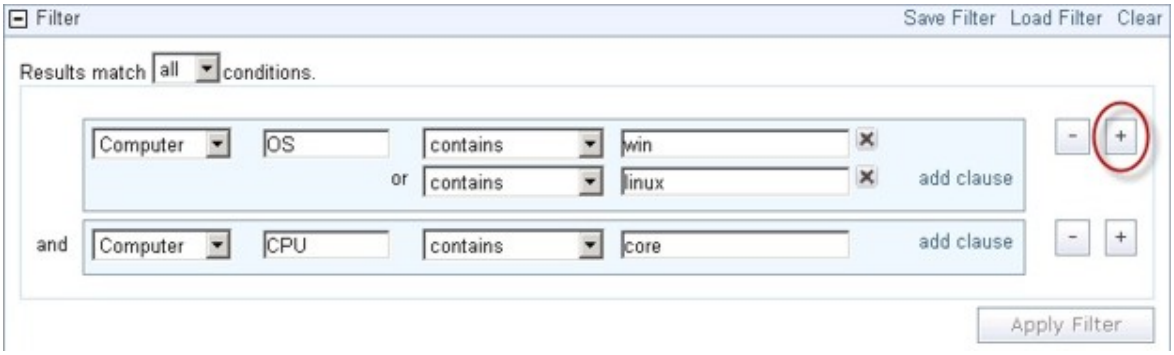
Computers

Click the Computers tab to see the default Computer report.



There are three sections on this page.

- **Filter:** View just the subgroup of the database you want to view by specifying a filter. Pull down the menu to filter by computer, content, site, or a previously saved filter. The choice you make determines the secondary fields of the filter. For example, you might want to view just those computers that have the specified properties.



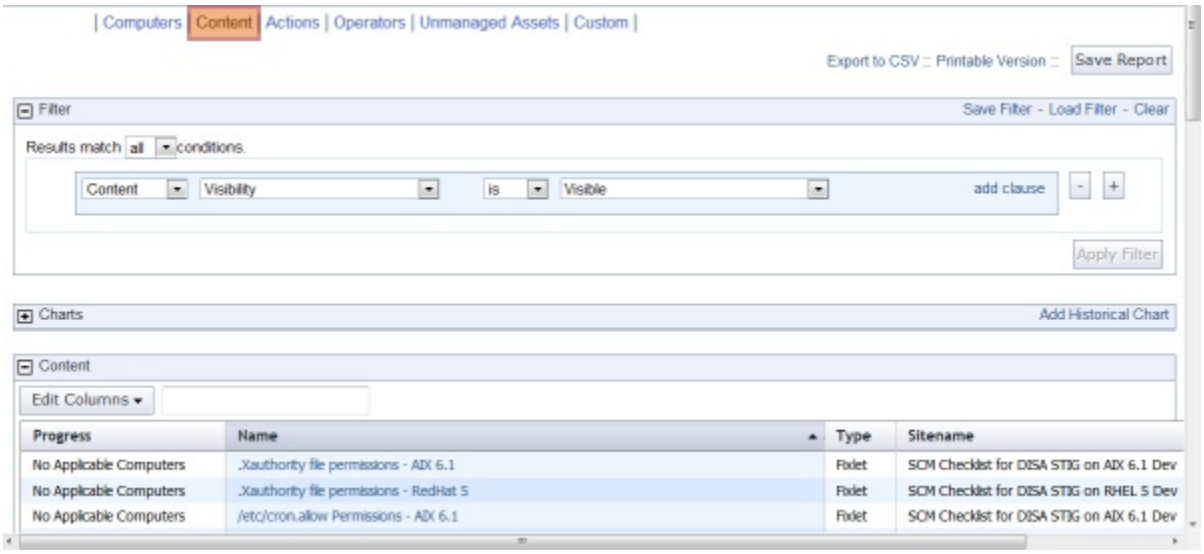
Click the link labeled **add clause** to add extra qualifiers to a filter. Click the **X** to delete any of these clauses. Click the plus sign to the right of the filter to add a new filter. These filters are ANDed together if you choose **all conditions**; they are ORed together if you choose **any conditions**. Click the minus sign (-) to delete a filter from the set. Click the **Apply Filter** button to see how your custom filter affects the subsequent computer reports and charts.

When defined, click the **Save Filter** link at the upper right if you want to save your work as a custom named filter. Later you can use this filter in other circumstances by clicking the **Load Filter** link.

- **Charts:** The typical computer chart is a pie or a bar chart. As described in the Charts *(on page 44)* section, you can select any computer property to graph.
- **Computers:** This section contains the data of the report. As described in the Columnar Report *(on page 50)* section, you can edit and rearrange the columns to suit your needs.

Content

Click the Content tab to view the default contents view.

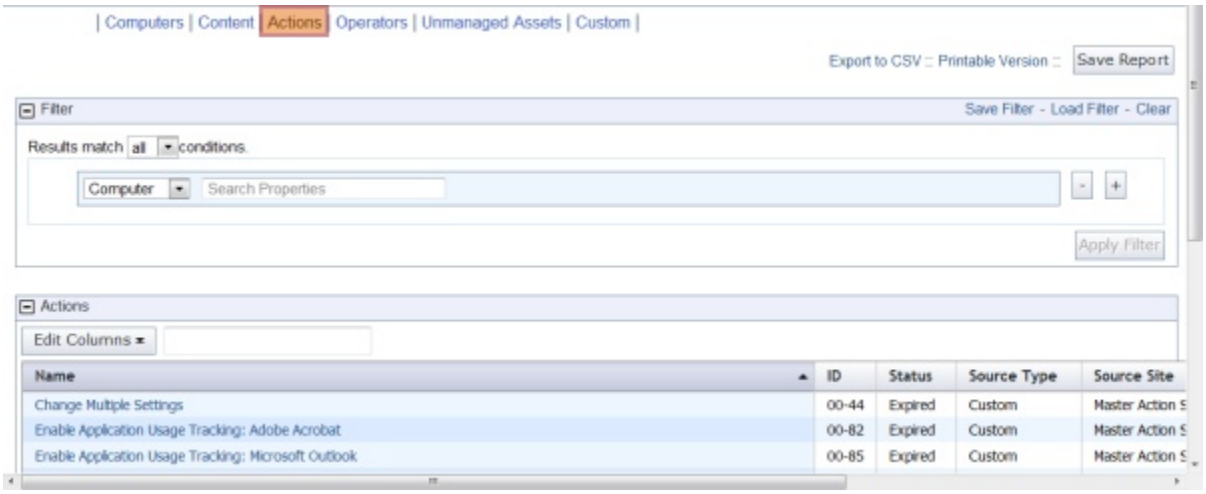


BigFix content consists of Fixlet messages, tasks, analyses and baselines. If you want, you can create a filter to separate these categories, for example, **Content Type is Fixlet**.

As with all typical views and reports, you can click a column header to sort the data (click again to change the direction of the sort). You can also edit the columns to display, set filters, and create charts.

Actions

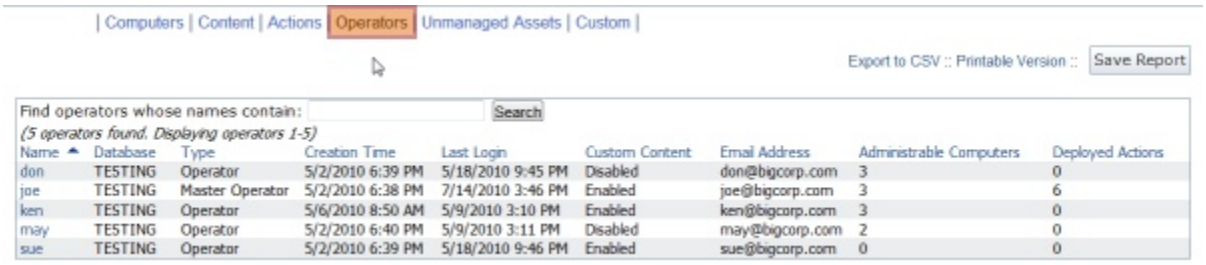
Click the Actions tab to view the default Actions view.



Actions are the consequence of clicking an Action link in a Fixlet or task. Actions propagate throughout your BigFix network, during which time they are marked as open. They can also be stopped and they can expire. A typical view includes the status, so you can watch the progress of your actions over time.

Operators

Click the Operators tab to view the default Operators view.



The Operator list is simple and straightforward. It contains a list of all the operators of your BigFix deployment, displaying the type and management rights of each. This list cannot be edited, although you can filter it by the name of the operator.

Unmanaged Assets

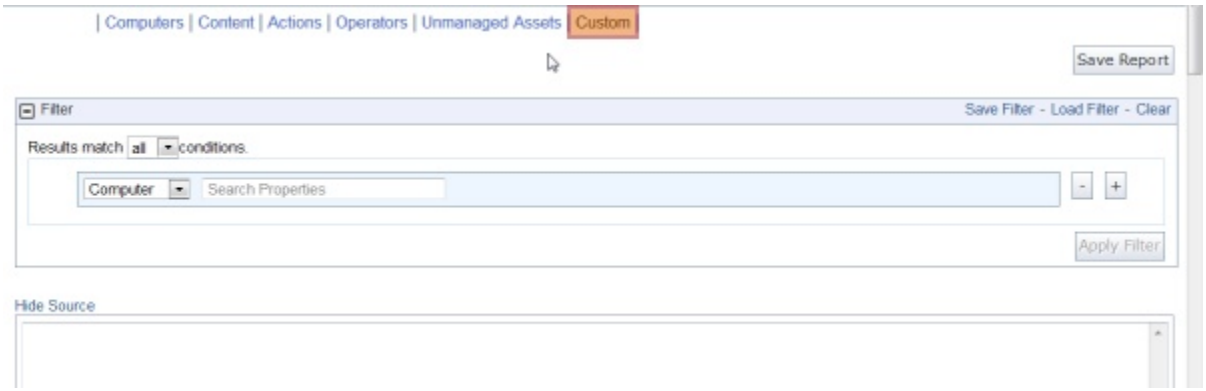
Click the Unmanaged Assets tab to view the unmanaged assets in your network.

For the unmanaged assets in your network, you can click, shift-click or ctrl-click the properties that you want to display. Click Next to see the report.

The Unmanaged Assets report cannot be customized, except for your choices in the original property list.

Custom

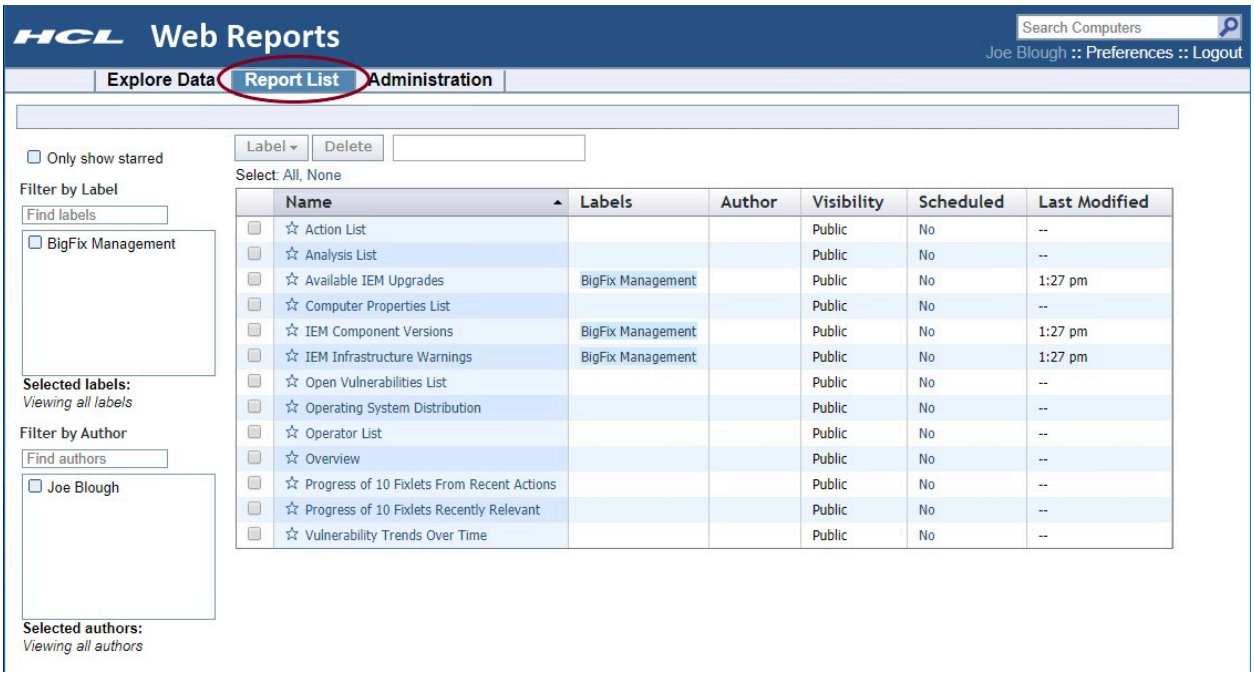
Click the Custom tab to create a new report from scratch.



For more information about custom reports, see the Resource section Creating a Custom Report (on page 96). A complete description of how to write your own custom reports is beyond the scope of this guide, but you can find more information in the **Session Inspector Guide** and the Web Reports and Custom Reports.

Chapter 5. Reporting

The **Report List** section of the program is accessed by clicking the appropriate tab from the top tab bar.



There are several parts to this page that allow you to customize your view of the available reports.

Report List Main Page

Import Report

The top link on the Report List page allows you to **import** a report.

It opens a new panel allowing you to browse for the report and specify the format and visibility.

- You can enter a **filename** in the text box, or use the file browser to find the report.
- The input can be an **XML** or **HTML** file.
- The imported file can be treated as a **Private** file that only you can view, or a **Public** report that is available to everyone.
- Click the **Import** button to load in the selected report.

Only Show Starred

Click this box to limit the report list to the starred reports.

You set which reports get a star by clicking the empty star next to their names in the list. The star is then filled with yellow. You can select any scheme you choose for starring a report. Most users star their favorite or most-used reports. Uncheck the box to display the entire list of reports.

Filter by Label

You can label any report by clicking the box in front of its link and then using the **Label** pull-down menu to assign an existing label.

To filter by a label, click the box in front of the appropriate label in the **Filter by Label** section. You can select multiple labels. Labels are ORed so that reports containing any of the labels selected are displayed.

Filter by Author

In the same way as you filter by label, you can filter the report list by author.

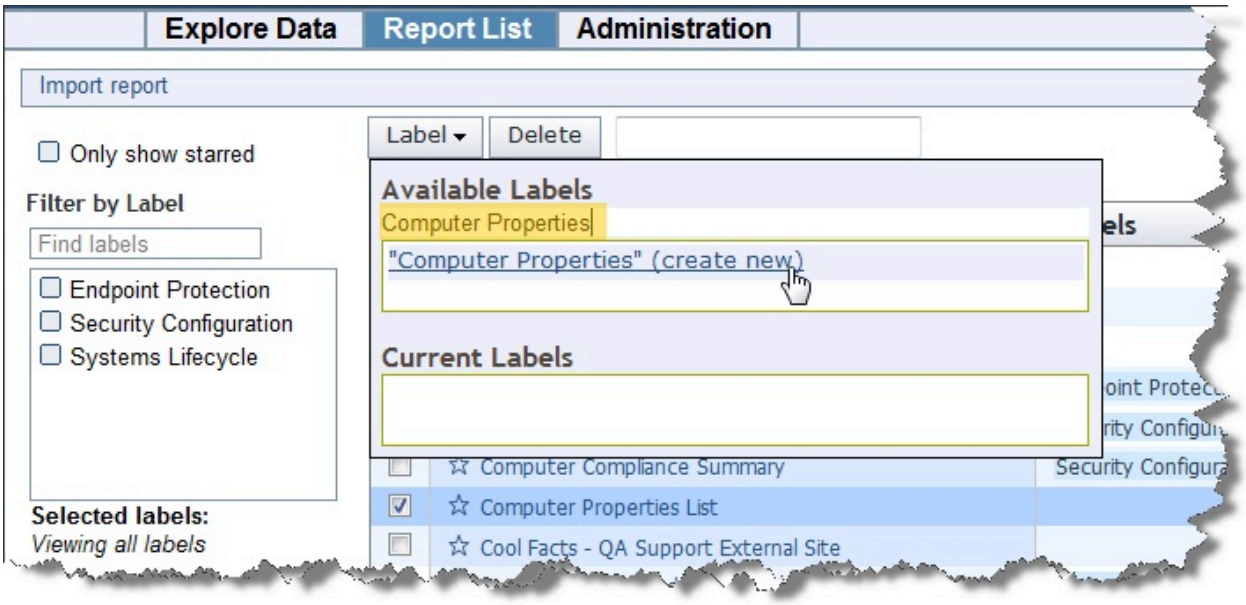
Click the box in front of the authors that you want and all the reports that were created by the chosen authors are listed.

Add, Create, and Delete Labels

When you click the box next to any report list, the Label button becomes available.

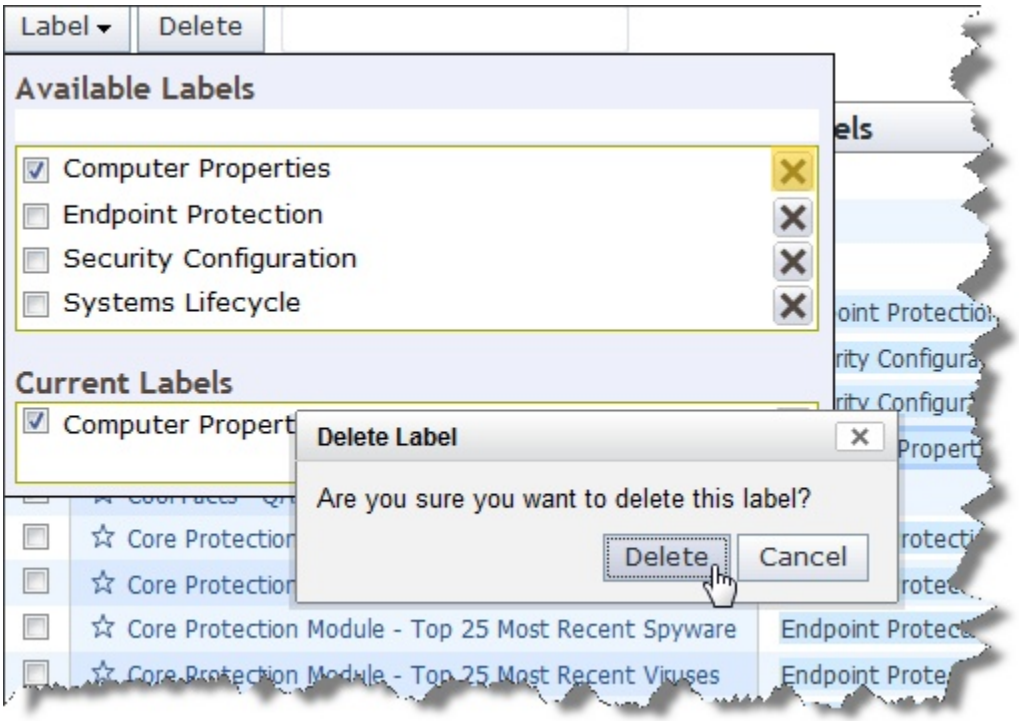
From this pull-down menu, you can select a label to attach to the chosen reports. You can add multiple labels to a report to allow it to be selected in multiple groups.

To create a new label, type in a name that does not already exist. The name is reprinted in the box below as a link.



Click the link to create the new label, which is then applied to the reports.

To delete a label, use the X button to the right of the label.



Delete

When you click the box next to any report list, the Delete button becomes available.

Click it to delete the specified report from your list.

Main List

There are several columns that describe reports in this list.

- **Select:** This column consists of check boxes allowing you to apply a function to several reports at a time. For example, if you want to delete a report, click the appropriate check boxes, then click the **Delete** button. This is also how you can attach a label to a report or group of reports.
- **Stars:** This column consists of unfilled stars directly to the left of the report name. Click them to fill them with yellow and highlight them as starred reports. These reports can then be filtered by clicking the **Only show starred** check box at the top left of the page.
- **Name:** This column contains the name or title of the stored report.

- **Labels:** This column contains the labels that have been assigned to the particular report. A report can have multiple labels, and the check boxes on the left allow you to filter the report list by labels. Domain labels might also be attached to external reports delivered by a site. Because there are multiple labels in this column, it cannot be sorted.
- **Author:** This column lists the name of the Web Reports user who created this report.
- **Visibility:** This column shows whether the report is public or private. If you are the author of a report, this column also lets you change the status of the report from the pull-down menu.
- **Scheduled:** This column indicates which reports are on a schedule.
- **Last Modified:** This column contains the dates when the report was last modified by its author.

The next sections describe specific reports that are commonly used.

Overview Report

The **Overview** report contains graphs and tables that visually represent the general state of your network, as well as the effectiveness of your BigFix deployment.

Next to the title of each report, there is a bracketed question mark **[?]**, which you can click for additional information.

Note: To print the overview report with the graphs and tables use the PDF version of the report.

Important: Reports are disabled if a user is logged in without sufficient privileges to view them, or if the report is filtered. Users are not considered to have sufficient privileges unless they have full rights to all the computers on the server.

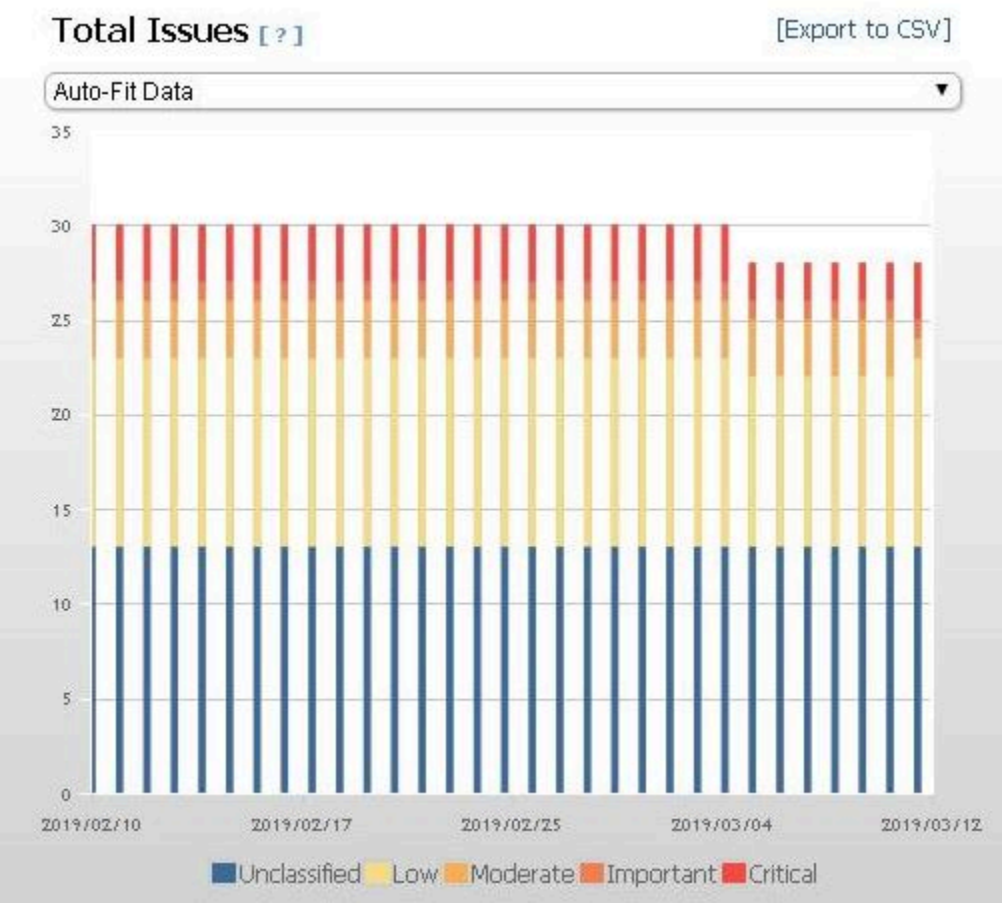
The following sections describe each of the graphs, charts, and tables presented in the Overview.

Total Issues

The **Total Issues** graph adds the number of relevant issues for each computer and then groups them by their severity rating.

An issue is a Fixlet message that is relevant on any computer in your network. For example, if you have a computer with five relevant Fixlet messages and a second computer with three relevant Fixlet messages, the total number of issues is eight, even if some of those messages are the same.

This graph can be set to different time granularities by selecting from the pull-down menu above the graph. The **Auto-Fit Data** option automatically groups the data in the graph for up to the last 12 months of your BigFix installation. **Last 7 Days** groups the data by day and shows the last seven days. **Last 30 Days** groups the data by day and shows the last 30 days. **Last 26 Weeks** groups the data by week and shows the last six months. **Last 52 Weeks** also groups the data by week and shows the last year.

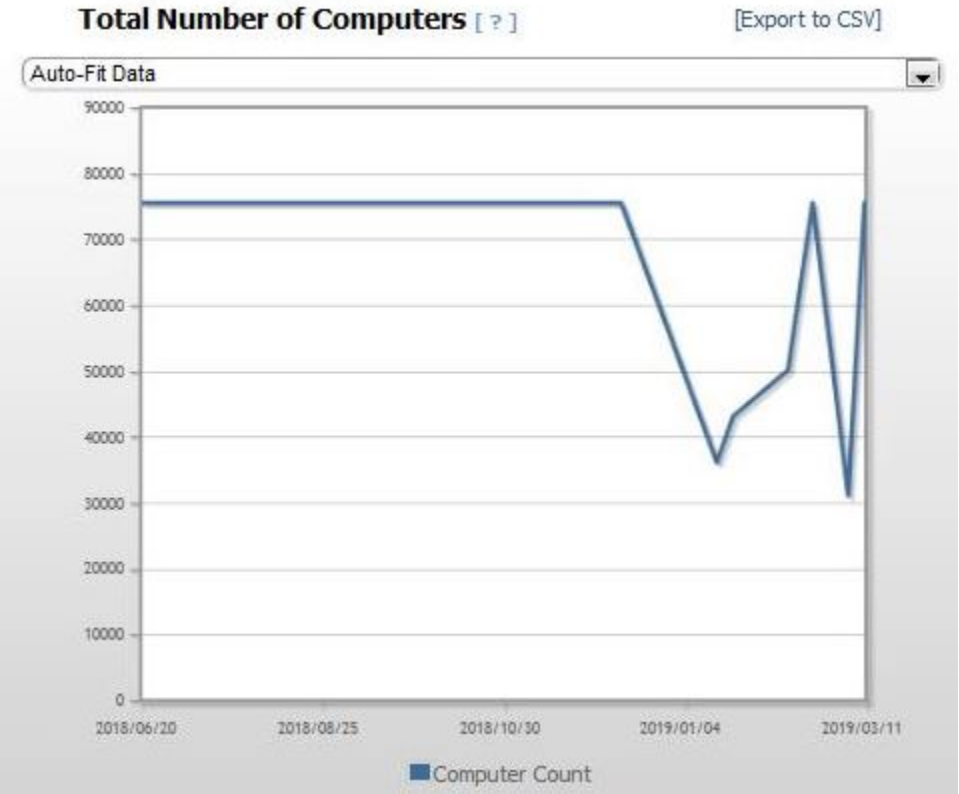


Different colored bars represent different issue severity. The height of each bar represents the number of issues for a particular bar. For example, if a bar for important issues starts at 300 and ends at 500, the total number of important issues is 200. Move your cursor over any point in the graph to see a pop-up containing more detail.

Total Number of Computers

The **Total Number of Computers** graph displays the number of computers that have been under BigFix management in a given period of time.

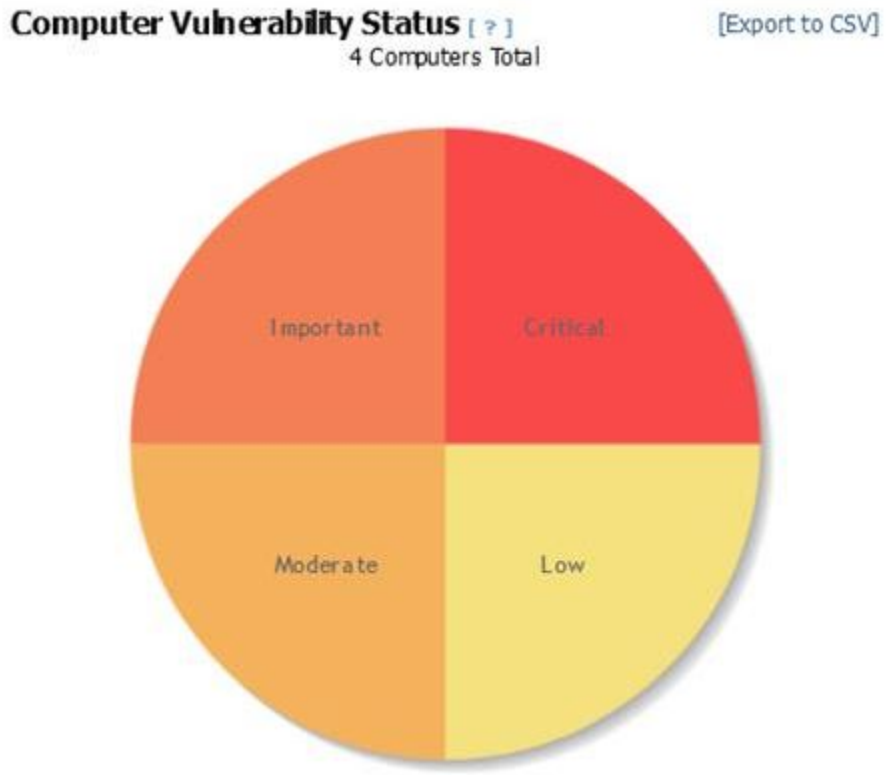
This graph offers a way to monitor additional deployments of the BigFix Client over time.



In the same way as the Total Issues graph, this graph is disabled if a user logs in without sufficient privileges. Select the time scale you want from the pop-up menu above the chart. Move your cursor over specific data points for more information.

Computer Vulnerability Status

The **Computer Vulnerability Status** pie chart computer groups according to their most severe vulnerability.

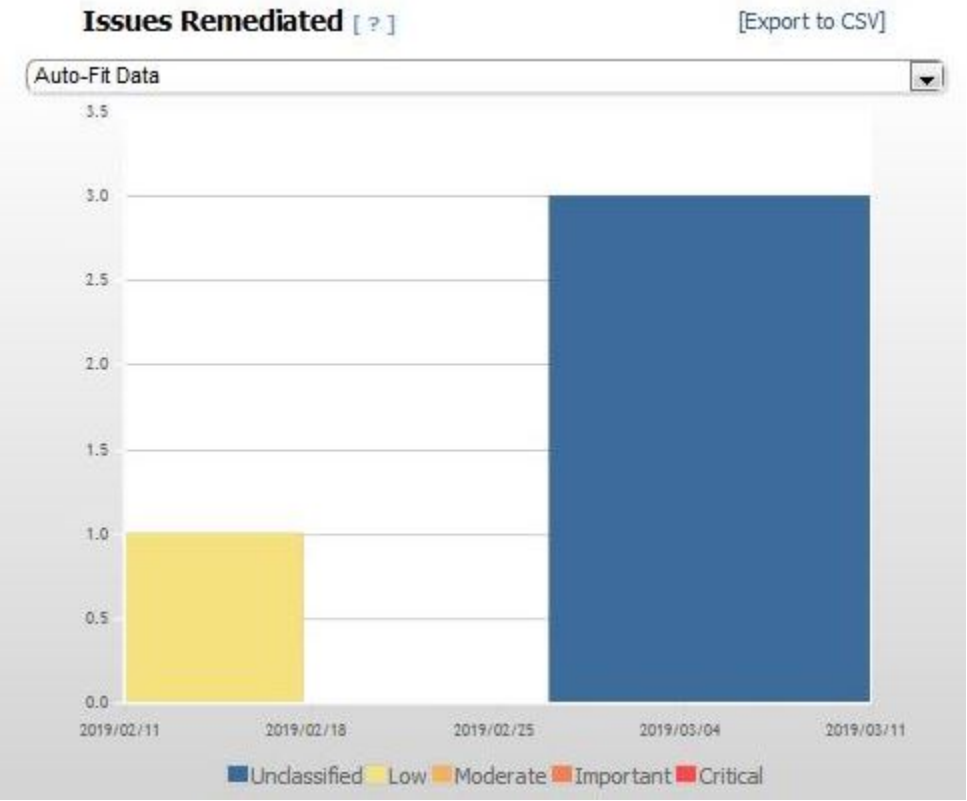


If a computer has a **Critical** vulnerability, it is considered to have critical status, regardless of other vulnerabilities it might have. If a computer has no critical vulnerabilities, but has an **Important** vulnerability, it is considered to have important status, providing you with a general sense of how your network is doing. Initially, the vulnerability pie is mostly red (critical), and as you continue to use BigFix, it becomes green (no vulnerabilities). Move your cursor over each pie slice to see the actual number of computers with each vulnerability status, and the percentage of network computers they represent.

Issues Remediated

The **Issues Remediated** graph shows a count of the number of computers that have returned **Fixed** in response to an action.

The time segment for an action is attached to its start time, not its completion time (which might occur in a subsequent time segment). This graph gives you a picture of remediation rollouts across your enterprise as BigFix finds and fixes vulnerabilities.



This is a historical graph. Select a time scale from the pop-up menu above the chart. This graph displays colored bars representing the severity of remediated issues, and lets you highlight data with your cursor.

Overall Statistics

The Overall statistics table displays important facts about your network.

Overall Statistics

Total Number Of Computers:	79	Relevant Fixlets Per Computer (average):	162.77
Total Number Of Fixlets:	29756	Total Number Of Fixlet Sites:	48
Total Number Of Tasks:	3792	Total Number Of Analyses:	237
Total Number Of Actions:	990	Mean Time To Remediate:	No information.

- **Total Number of Computers**: The current number of BigFix Clients.
- **Relevant Fixlets per Computer**: The average number of relevant Fixlet messages per computer, or the total number of relevant issues divided by the total number of computers.
- **Total Number of Fixlets**: The current number of Fixlet messages that exist on the BigFix system. Note that if Web Reports is looking across multiple databases in the network, the number of Fixlet messages corresponds to the union of all the Fixlet messages in all the databases.
- **Total Number of Fixlet Sites**: The total number of sites to which the BigFix system is currently subscribed.
- **Total Number of Tasks**: The current total of relevant tasks on your BigFix network.
- **Total Number of Analyses**: The current total of analyses that exist on the BigFix system.
- **Total Number of Actions**: The current total of actions issued so far by the BigFix system.
- **Mean Time to Remediate**: The average time it took for every relevant issue to become non-relevant on all computers. Note that issues can become non-relevant by methods other than actions. For example, users can manually update their computers, making those relevant issues no longer relevant.

Top 10 Critical/Important Issues Detected

The **Top 10 Critical/Important Issues Detected** report displays Fixlet messages that are currently affecting the largest number of computers in the network.

Top 10 Critical / Important Issues Detected

	Name	Source Severity	Affected Computers	Patch Completion
1.	Version of Dbmslpcn.dll May Cause Handle Leak on BES Client/Server Components	Important	10	0.00%
2.	Updated BES Client Now Available! (Version 7.0.1.356) - WinNT/2000/2003/XP	Important	8	52.94%
3.	MS07-012: Vulnerability in Microsoft MFC Could Allow Remote Code Execution - Windows XP/2003 (x64) (v2, re-released 6/12/2007)	Important	6	0.00%
4.	MS06-078: Vulnerability in Windows Media Format Could Allow Remote Code Execution - Windows Media Player 6.4 (re-released 7/10/2007)	Critical	5	0.00%
5.	MS07-031: Vulnerability in the Windows Schannel Security Package Could Allow Remote Code Execution - Windows XP SP2	Critical	5	0.00%
6.	MS07-035: Vulnerability in Win 32 API Could Allow Remote Code Execution - Windows XP SP2	Critical	5	0.00%
7.	MS07-034: Cumulative Security Update for Outlook Express and Windows Mail - Windows XP SP2	Important	5	0.00%
8.	MS06-068: Vulnerability in Microsoft Agent Could Allow Remote Code Execution - Windows XP SP2	Critical	4	0.00%
9.	MS07-008: Vulnerability in HTML Help ActiveX Control Could Allow Remote Code Execution - Windows XP SP2	Critical	4	0.00%
10.	MS07-009: Vulnerability in Microsoft Data Access Components Could Allow Remote Code Execution - Windows XP SP2	Critical	4	0.00%

Show Progress of Top 10 Critical / Important Issues

There are four columns in this list:

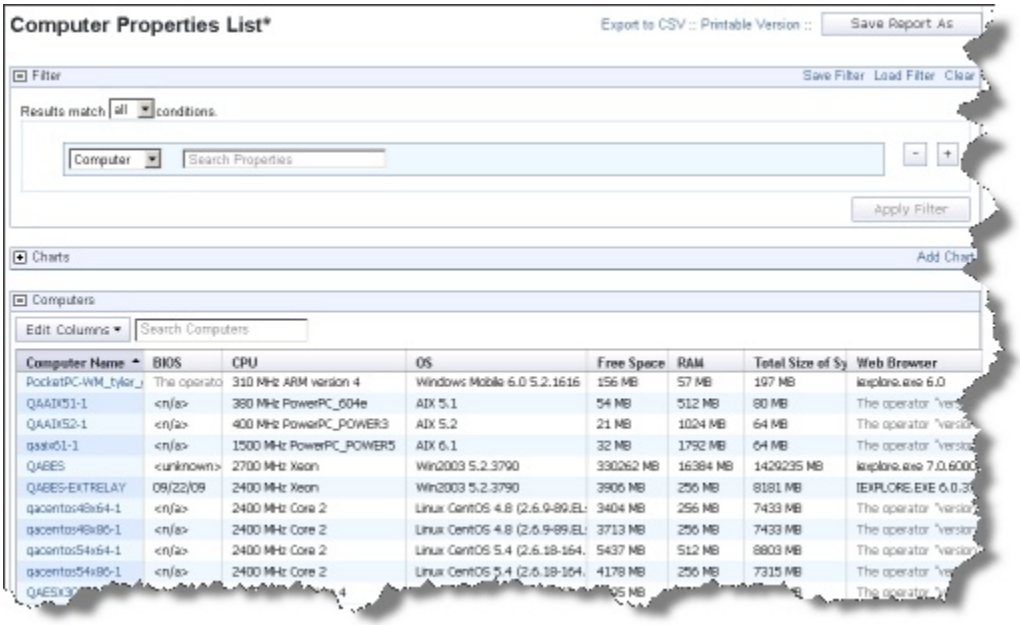
- The **Name** column lists the name of the Fixlet message.
- The **Source Severity** column lists the severity of each common Fixlet.
- The **Affected Computers** column displays the number of computers that currently have the Fixlet relevant. The Fixlet list is sorted by the Affected Computers count.
- The **Patch Completion** column is the percentage of fixed computers out of the total number of computers that have ever been affected by the listed Fixlet.

Beneath the list of the top 10 most common issues, the **Show Progress of Top 10 Critical/ Important Issues** link opens a progress report that you can view in Explore Data.

Computer Properties List

This report provides you with a list of certain properties of your BigFix Client computers.

Like many of the listed reports, this is derived from Explore Data, with specific filters and charts. These exist for your convenience, but you can also re-create them yourself with just a few mouse-clicks.

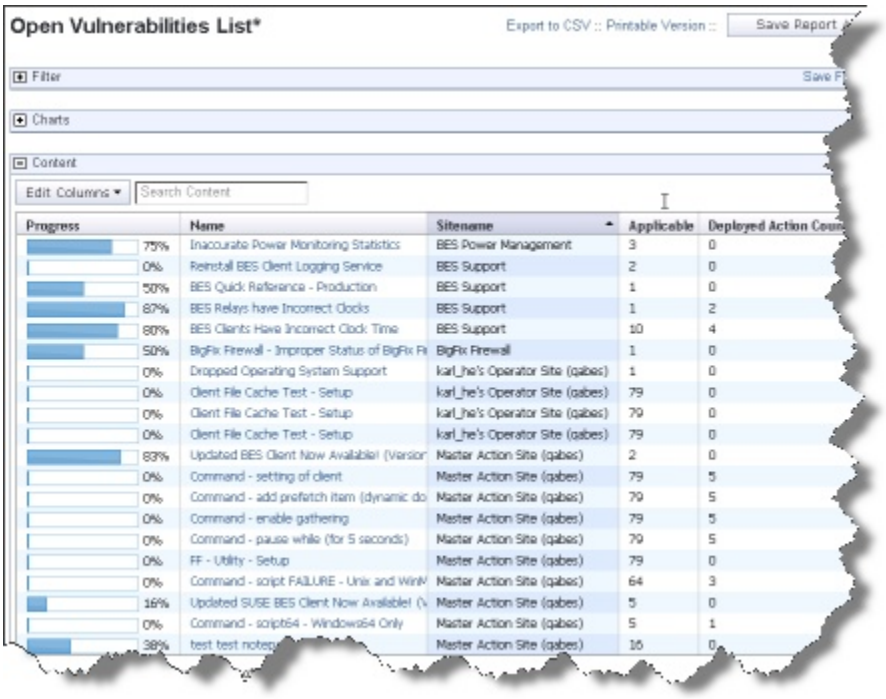


Select **Computer Properties List** from the Report List. You can select a filter to reduce the size of the list. The headers refer to important computer properties, such as the BIOS date, the CPU type, free hard disk drive space, the operating system, memory, and user name. These properties are standard for out-of-the-box BigFix clients. However, from the console, you can create new computer properties using relevance expressions, and they are also available here.

Open Vulnerabilities List

This report displays Fixlet messages that are currently relevant.

You can also filter this report to view only Fixlet messages that have at least one applicable computer.



Select **Open Vulnerabilities List** from Report Lists. The first column provides a quick visual representation of the progress of each vulnerability. In addition, the report shows the name, site applicable computer count, and deployed action count to complete the report. This

report is useful to help you track those issues that can expose your network to potential problems.

Other Reports

As well as the reports you create yourself, there are several other pre-installed reports included with Web Reports.

- Action List
- Analysis List
- Operating System Distribution
- Operator List
- OS Vulnerability Summary. (This report, along with a few other built-in reports and some customer-created reports, is loaded in the 7.2 Computer Properties Report format. Reports in this format can be viewed, but new ones in this format cannot be created.)
- Progress of 10 Fixlet messages From Recent Actions. (This report is special because it generates an ad-hoc filter to list only the 10 Fixlet messages with the most recent actions in the deployment.)
- Progress of 10 Fixlet messages Recently Relevant. (Similar to the above, this report generates an ad-hoc filter.)
- Vulnerabilities by Console Operators. (This report is in the 7.2 format.)
- Vulnerabilities by OS. (This report is in the 7.2 format.)
- Vulnerability Trends Over Time. (This is a special historical report, and cannot be filtered.)
- Average Vulnerability Trends Over Time. (This is a special historical report, and cannot be filtered.)

These reports are easy to examine by clicking them from the Report List. Many reports can be further customized by using filters, adding charts, and editing the columns.

Showing non-relevant results

By default the Web Reports mark as `<not reported>` a property that is not relevant or that is no longer relevant.

The console, instead, always shows the property with its latest retrieved results. If you want that the Web Reports show the same type of information as the console, configure them as follows:

BigFix Server with Windows OS

1. In the `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node` registry section under `HKLM\Software\WOW6432Node\BigFix\Enterprise Server\BESReports`, create the `ShowNotRelevantResults` registry key.
2. Set the `ShowNotRelevantResults` value to `1`.
3. Restart the Web Reports service after modifying the registry.

BigFix Server with Linux OS

1. In the `beswebreports.config` file, under the section named `[Software\BigFix\Enterprise Server\BESReports]`, insert the `ShowNotRelevantResults` keyword.
2. Set the `ShowNotRelevantResults` value to `1`.
3. Restart the Web Reports service after modifying the configuration file.

Chapter 6. Administering the Program

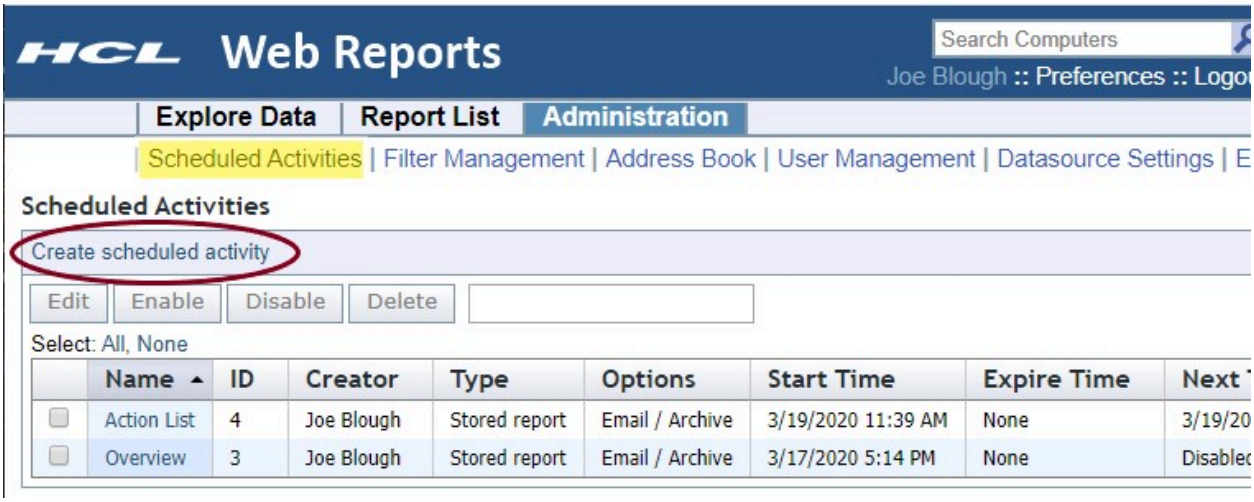
The **Administration** section of the program lets you manage activities, filters, addresses, users, and databases.

This part of the Guide describes these functions. Click the **Administration** tab, at the top of the window.

Scheduled Activities

The Schedule section allows you to run reports at a given time or when certain conditions are met.

The report results can then be emailed to you or archived for later viewing. This allows you, for example, to receive automatic updates of critical Fixlet messages via email, or to regularly back up audit reports.



When you open this page, a list of your currently scheduled reports is opened. Click **Create Scheduled Activity** to add to the list.

Below the create link are some buttons. These are grayed out until you select one or more activities in the list below. The buttons include:

- **Edit:** Allows you to edit the properties of the scheduled activity.
- **Enable:** Allows the selected activity to perform on schedule. Used to reactivate an activity that you previously disabled.
- **Disable:** Prevents the activity from running until enabled again. This allows you to preserve the functions of an activity without actually running it.
- **Delete:** Deletes the selected (checked) activities.

You can select the items in the list by individually clicking them. You can also use the links at the top of the list to Select **All** or **None**.

The list has several columns, including:

- **Name:** The name of the activity, derived from the underlying report.
- **ID:** An incremental number assigned to each activity when it is created.
- **Creator:** The name of the activity author.
- **Type:** The type, either report or alert.
- **Options:** Describes the action, either email, archive, or custom.
- **Start Time:**The starting time of the activity, which is typically when you created it.
- **Expire Time:** The ending time of the activity, if you set one. Otherwise, it is open-ended and this column displays **None**.
- **Next Time:** The time when the activity runs next, unless the activity has been disabled.
- **Period:** The time period between scheduled activities. This can be any time from one minute to two years.

Creating Scheduled Activities

A scheduled activity creates a report or an alert on a specified schedule.

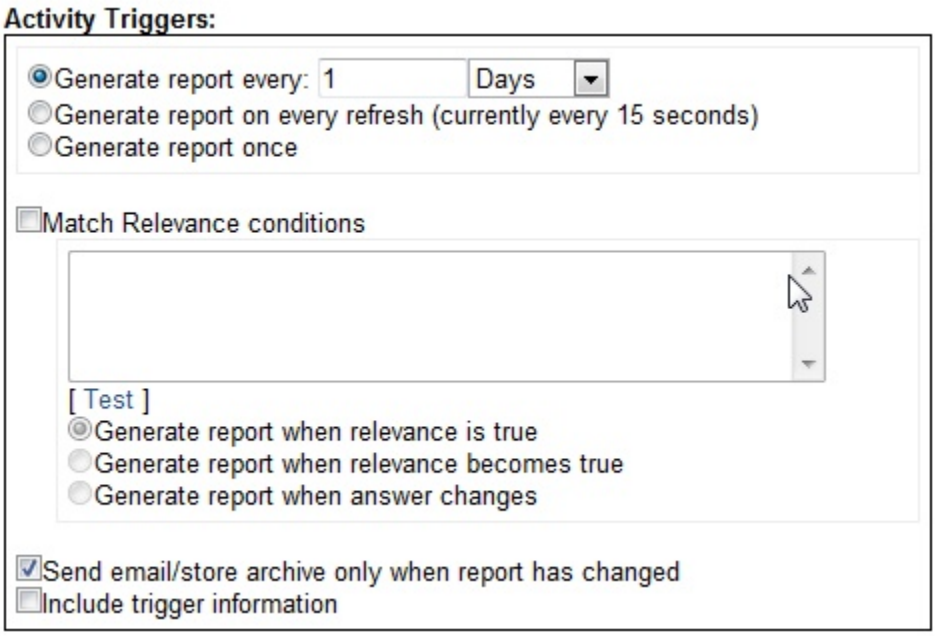
The interface has four sections, specifying the **time range**, the **activity report**, the **activity trigger** for the schedule, and the **activity actions** to be taken.

To schedule an activity, follow these steps:

1. Click **Administration > Scheduled Activities**, and then click the **Create scheduled Activity** link.
2. From the requested Creation page, select a time range for the scheduled activity.

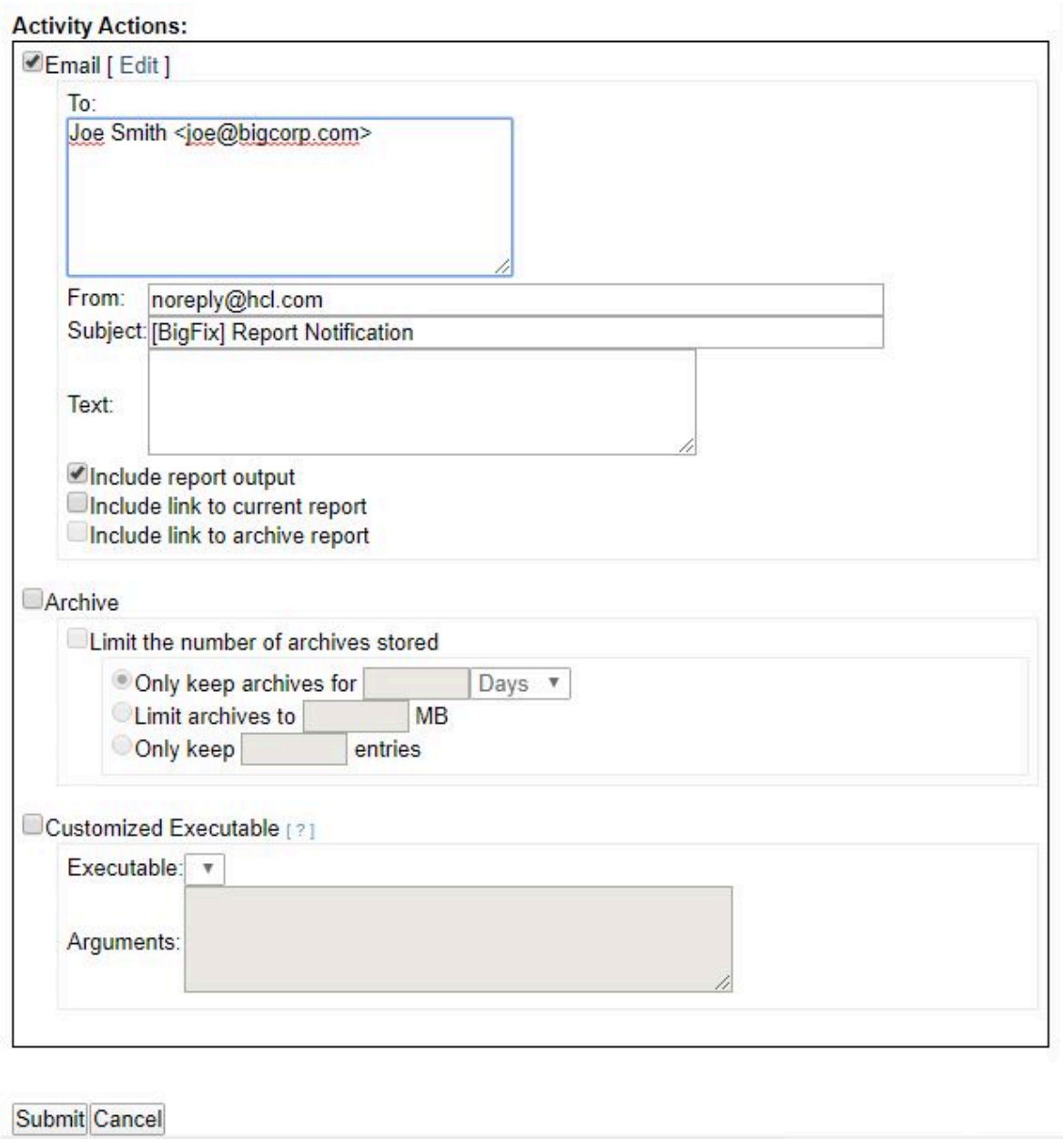
   This setting defines the window during which the schedule remains in effect. It consists of a **Start time** and an **Expire time**. The default start time is now. If you do not select an expiration time, the activity stays open-ended.
3. In the Activity Report box:

   a. Select a report type: **Report** or **Alert**. A report produces a detailed graphic/tabular output and an alert typically sends a report as an email.
   b. Select a stored report from the pull-down menu. The menu includes all public and private reports to which you have access.
   c. Select either HTML or CSV format for your report. The PDF format is also available if PDF generation was enabled in Web Reports.
4. In the Activity Triggers box:



a. **Generate:** Select how often to generate the report: during a specified interval, after every data refresh, or once.
b. **Match Relevance conditions:** Enter any relevance conditions necessary for the report to run.
c. Select whether to email or archive the report only when it has changed.
d. Check the box labeled **Include trigger information** to embed the trigger criteria in the report itself.

5. In the Activity Actions box:



a. Select to whom you want to **email** the report. Write a subject line and some accompanying text. Check the boxes to include the **output** of the report, a **link** to the report, or a link to the archive.
b. Select whether or not to **Archive** the report. You can limit the number of archives, and you can limit each archive by time, disk space, or number of entries.

c. You can specify a customized executable that is triggered when the activity runs. Customized executables must be located in the correct directory. On Windows Web Reports server the default path is: `C:\Program Files\BigFix Enterprise\BES Server\BESReportsData\CustomExe`. On Linux Web Reports server the default path is `/var/opt/BESReportsServer/BESReportsData/CustomExe`.

   The executable runs as the Web Reports service user through the shell. It runs in the background, without a user interface. Select an executable from the pull-down menu. There are some reserved words that can pass variable information to the executable:

   <activityname>

   Passes the scheduled Activity name.

   <reportfile>

   Passes the generated report file.

   <activitycreator>

   Passes the name of the Activity creator.

6. Click **Submit**.

You have now scheduled an activity. It is shown in the Schedule Activity list, named after the report you chose to schedule.

Filter Management

Filters are used to customize reports, allowing you to highlight any particular subset of the database.

You can save your custom filters, allowing you to reuse them in other reports. You can then view, delete, and change the Private or Public status of your custom filters from this interface.

Click the **Filter Management** option from the **Administration** tab. You can see a list of the existing filters, allowing you to modify any of them. All administrators, not just the creator of the filter, can edit, delete, or change the visibility of any filter in this list.

Click the check boxes in front of a filter to use the **Delete**, **Make Public,** or **Make Private** buttons. You can also specify a search string to narrow down the list of filters.

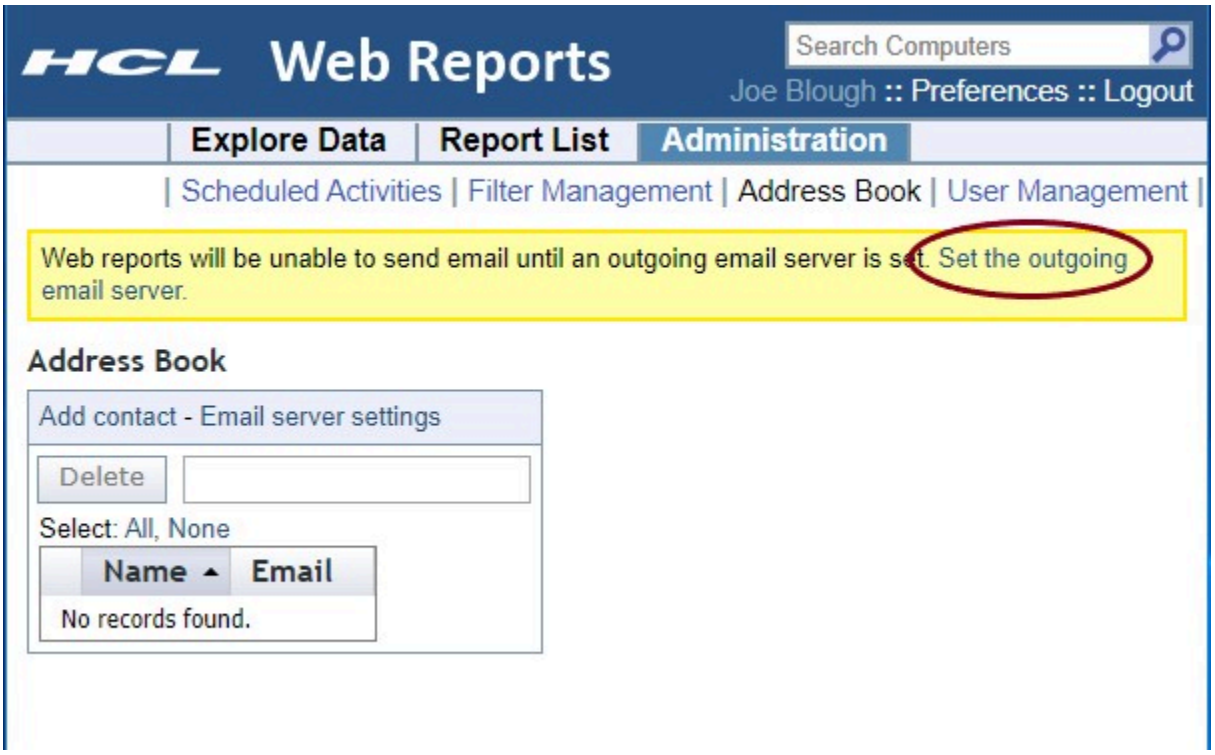
Note: If you delete a filter that is a part of an existing report, you might change the interpretation of that report and generate a larger than expected listing.

Address Book

The Address Book section allows you to configure the email server settings, and to edit your list of email addresses.

Click the **Address Book** option from the **Administration** tab to manage your address book.

If you have not yet configured your email settings, a warning box opens, allowing you to identify the outgoing email server.



For more details about how to set the outgoing email server, see step 4 in Setting Up Email (on page 27).

Note: Only a Web Reports administrator can edit email settings.

After you save the server settings, you are returned to the Address Book.To add a new contact to the book:

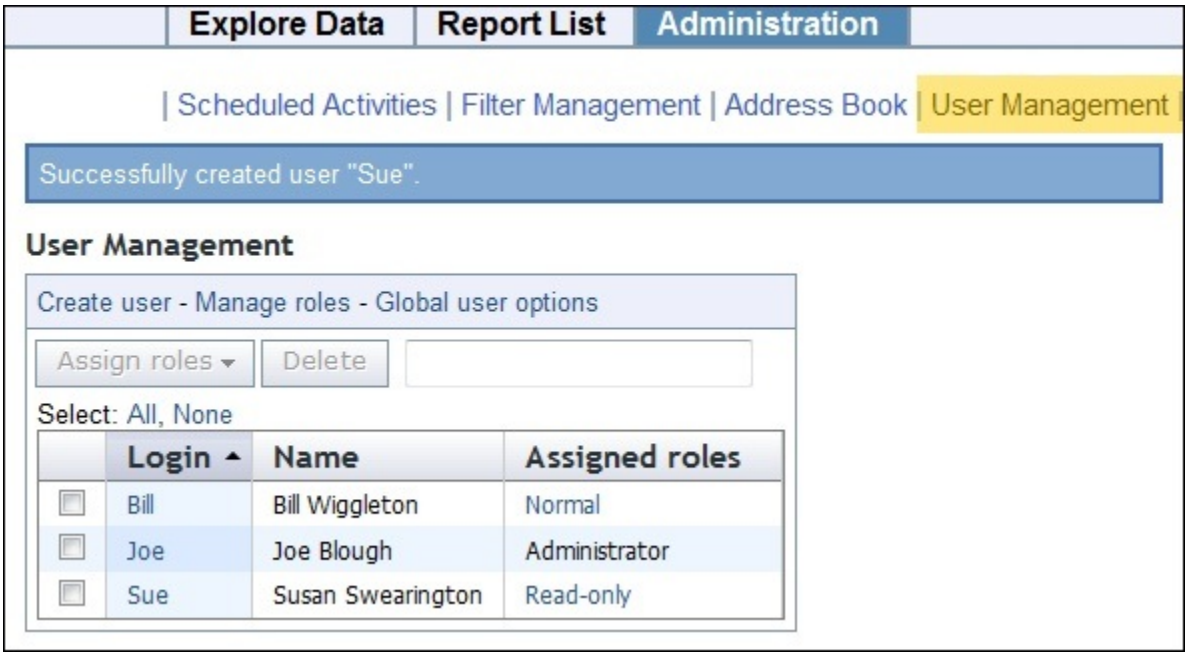
1. Click **Add Contact**. From the pop-up dialog, enter the name and email address.
2. Click the **Add** button to store the contact information.
3. This page also allows you to delete addresses: check the box next to the name and click **Delete**.

You have now set up your Address Book, which you can use to send scheduled activities to anyone on your list.

User Management

The **User Management** page allows you to add, delete, and edit the properties of your web users.

Each user can have more than one role. When you log in, your roles are ORed together and your status is determined by the union of your permissions. If the sum of your roles does not grant you Administrator status, then you cannot see the User Management section. If you have Administrative privileges, click the **User Management** option from the **Administration** tab.



The User Management page lists users in a table, which contains **Login**, **Name**, and **Assigned roles** information.

There are other links on this page:

- **Create user:** Opens the Create User page, which prompts you to provide a name, login, password, and define any user roles. For more information, see Create Users *(on page 83)*.
- **Manage roles:** Allows you to define and manage the roles that you want to assign to your users. For more information, see Manage Roles *(on page 84)*.
- **Global user options:** Allows you to set some management parameters that are shared by all users. For more information, see Global User Options *(on page 86)*.

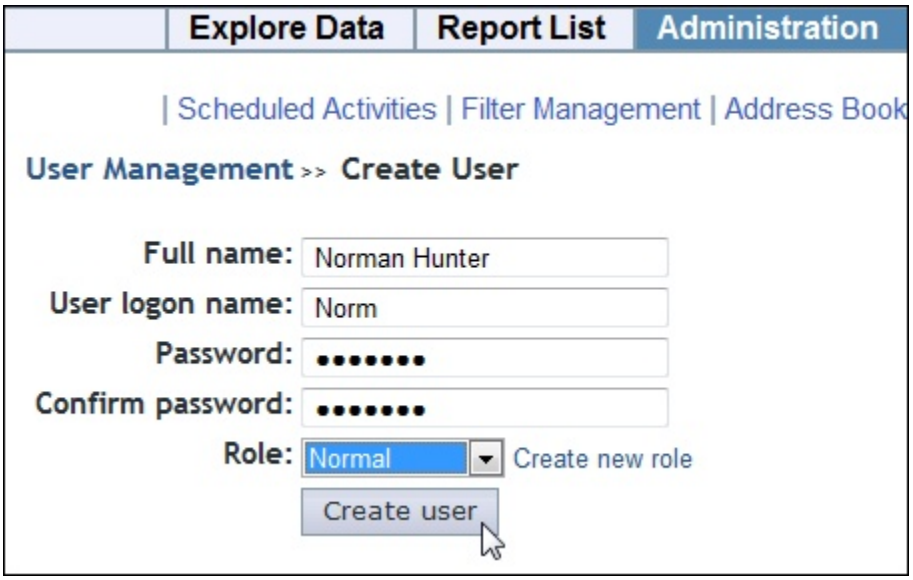
As you create new users, they are added to the list. In front of each entry is a box that you can check. When you do, the **Assign Roles** and **Delete** buttons become available. You can then assign a group of users a new role or delete them

You can also click the links in the Login column to **edit** a user. For more information, see Edit User (on page 88).

Create Users

How to create users.

This page is available from **Administrator > User Management > Create User**. It prompts you to provide a **name**, **login**, **password,** and define the user **roles**.



The built-in **Roles** include:

Administrator: Grants top-level privileges, with the ability to create additional users, schedule activities, and set database configurations.

Normal user: Grants ordinary privileges allowing the user to view the data, but not to create other users or set database configurations.

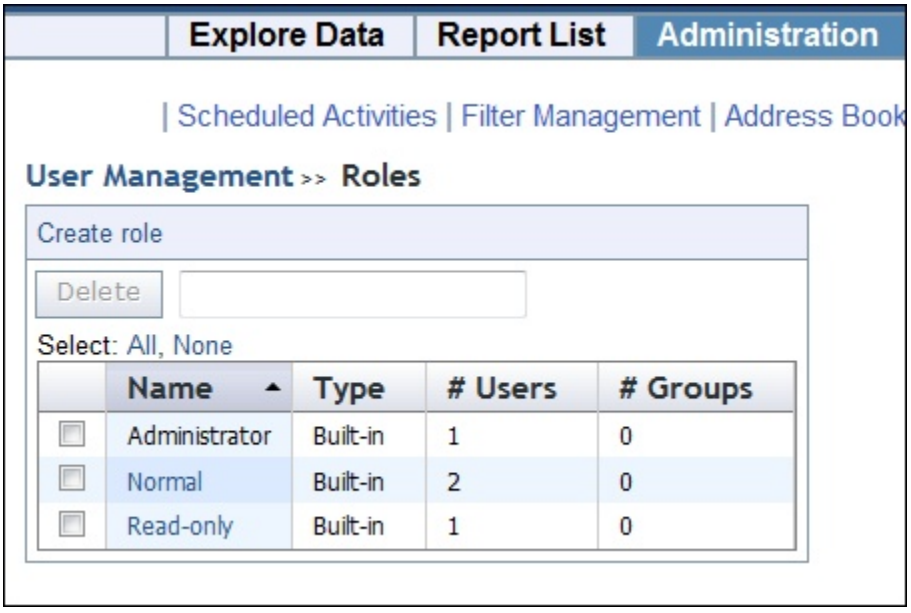
Read-only: Restricts a user from editing public filters and reports.

Enter the information required and click **Create User**.

Manage Roles

This page is available from **Administration > User Management > Manage Roles**.

On this page, you define and manage the roles that you want to assign to your users.



Delete roles by clicking the box to the left of the role and then clicking **Delete**.

There are three built-in roles:

Administrator

Grants top-level privileges, which allow the user to create additional users and set database configurations.

Normal user

Grants ordinary privileges, which allow the user to view the data, but not to create other users, set database configurations, or schedule activities.

Read-only

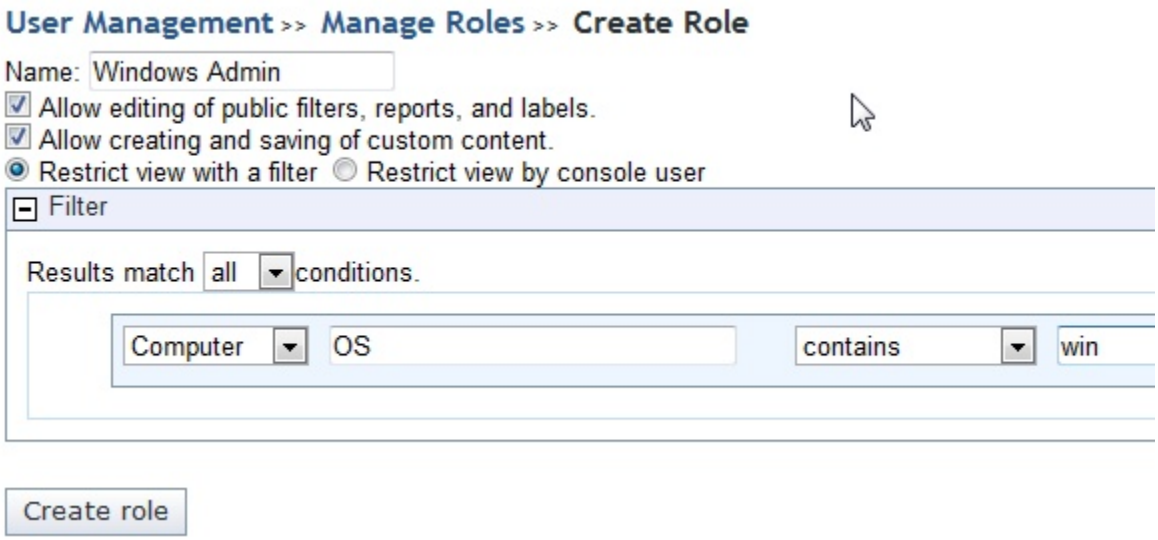
Restricts a user from creating or modifying public filters, reports, and labels or anything belonging to or visible to any other user. A user with the Read-only role can create, save, and edit only private custom reports.

Click the **Create Role** link, to define your own custom role, allowing different permissions and scopes.

Create Roles

This page is available from **Administration > User Management > Manage Roles > Create role**.

It allows you to create a new role with just the specific permissions you want to grant This role then becomes visible in the list of roles, available for you to assign it to the appropriate users.



A role requires a name, and then there are some check boxes to define permissions:

Allow editing of public filters, reports, and labels. Check this box if you want this defined role to include editing permissions on these objects.

Allow creating and saving of custom content. Check this box if you want this role to allow content creation.

Restrict view with a filter. Click this button to use a filter that constrains what this role can view. When you click this button, a filter panel opens allowing you to create a filter that is applied to computers or content to only allow subsets of the data to be viewed by this role.

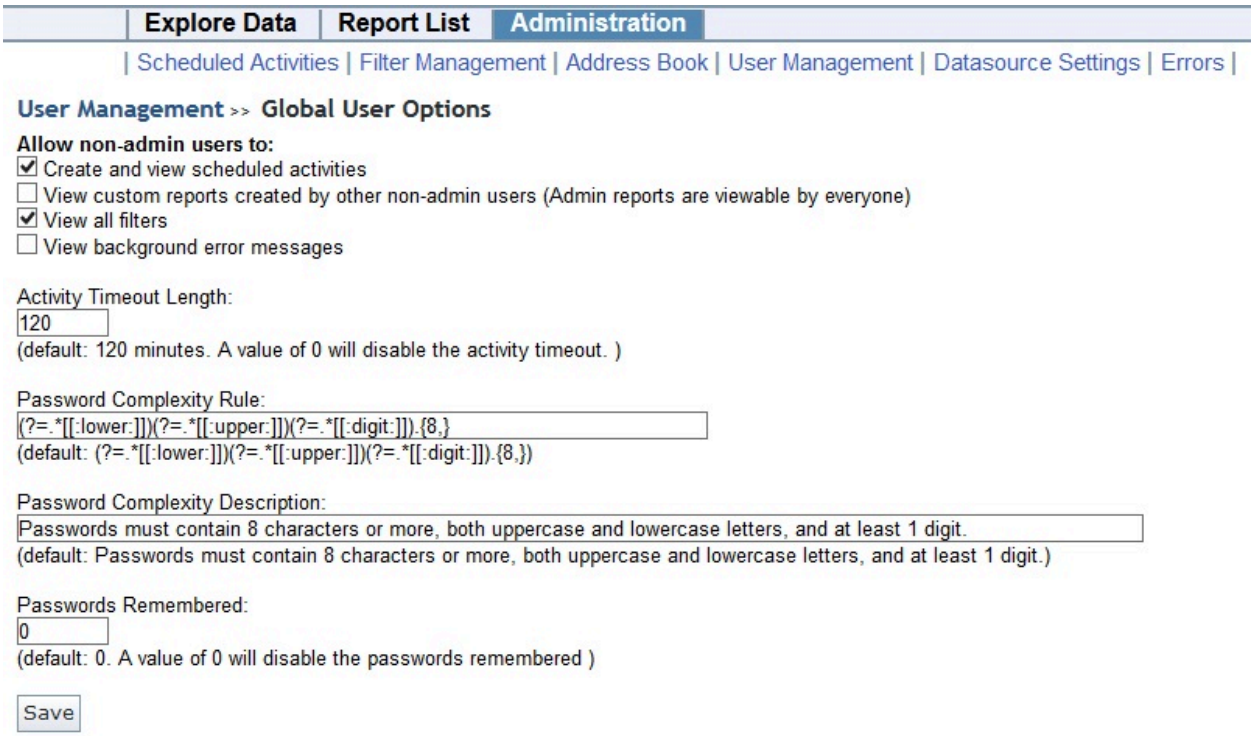
Restrict view by console user. Click the button to select a user from a list. This allows you to create a role just for a specific user. When you click this button, a list of console users opens from which you can choose a name.

The example above creates a Windows Administrator who is limited to accessing Windows computers. Click **Create Role** when you have finished your definition.

Global User Options

This page is available from **Administrator > User Management > Global User Options**.

It allows you to set some management parameters that are shared by all users.



From this interface, you can refine user rights for **non-administrative** users and **console operators**. Check the appropriate boxes to add and delete the specific permissions you want. The options include:

Allow non-admin users to:

- **Create and view scheduled activities.** This is set to on by default. If it is turned off, the non-administrator user cannot view the schedule of activities.
- **View custom reports created by other non-admin users**. This is set to on by default. Custom reports created by the administrator are always viewable.
- **View all filters.** This is set to on by default. If turned off, non-administrative users can only view filters they have created themselves.
- **View background error messages.** This is set to off by default. Turn it on if you want non-administrative users to view error messages**.**

Allow user restricted by Console operators to:

- **View all operators.** This is set to on by default. If turned off, restricted Web Reports users cannot view other operators.
- **View all local analyses.** This is set to on by default. If turned off, restricted Web Reports users cannot view analyses that were created by another non-master operator.

Password Complexity Rule:

- You can also define the **Password complexity**, which specifies the minimum and maximum length of acceptable passwords. The default is to allow passwords between 6 and 256 characters. The password complexity rule is defined using a regular expression.
- Below the rule is the text that is printed when a password is out of these bounds.

Passwords Remembered:

- You can specify the number of unique new passwords that can be set for a user account before an old password can be reused.
- The default value is zero (0). Setting the value to 0 disables the passwords remembered.

Click **Save** to record your global options.

After clicking **Save**, you are automatically redirected to a new page where you must perform again the current user authentication as described in Performing the reauthentication (on page 40).

Edit User

When editing user accounts, different options are presented depending on whether you are editing your own settings or those of someone else.

If you are not logged in as an administrator, you cannot edit other users' accounts. To change the parameters of a user, select the **Users** tab, and then click the **Login** link for the user you want.

Regardless of administrative privileges, if you are editing your own settings, you can:

- **Change name**. Click this link to enter a new user logon name. After clicking **Save**, you are automatically redirected to a new page where you must perform again the current user authentication as described in Performing the reauthentication *(on page 40)*.
- **Change password**. Click this button to open the **Change Password** page. Enter your old password, then enter your new password and confirm it. After clicking **Save**, you are automatically redirected to a new page where you must perform again the current user authentication as described in Performing the reauthentication *(on page 40)*.
- **Change preferences**. You can only access your own personal defaults, not those of other users. This opens the same dialog as when you click the **Preferences** link at the very top of the page.

If you are logged in as an administrator, and editing a user other than yourself, you can change everything except the preferences.

Datasource Settings

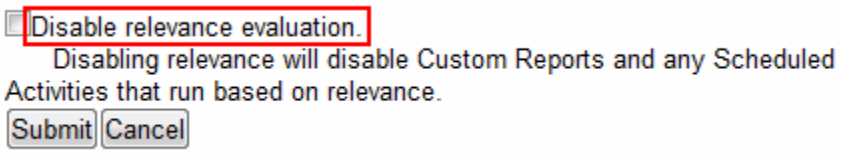
You can manage the datasources from which Web Reports aggregates information.

The Datasource section is used for BigFix datasource management. This includes adding, deleting, and editing datasource connections and settings.

Click **Administration > Datasource Settings**.

These are the links you can select on this page:

- **Disable** (Enable): Allows you to remove a datasource from aggregation, without deleting the datasource. In this way it can be re-enabled at a later time.
- **Edit**: Allows you to edit the settings for a selected Datasource (to the left of the row). For more information, see *Edit Datasource*.
- **Delete**: Lets you delete the selected datasource from the Web Reports aggregation. To ignore the datasource but keep the datasource connection information available, you can disable the datasource by clicking **Disable**.
- **Add New Datasource**: Allows you to add a new datasource into the aggregation group. For more information, see *Add New Datasource*.
- **Datasource Options**: Allows you to set options for datasources. One option exists on this page: **Disable relevance evaluation**.



It is cleared by default. If checked, all relevance evaluation in custom reports and in any scheduled activities is disabled. Click **Submit** to set the option.

- **Cache Settings**: Displays information about the datasource cache in memory. It displays the last time the cache was written to a file on disk for each datasource. It also allows you to change how often the cache is refreshed. Finally, it gives the option of writing the cache to disk, and if so, how often to write it to disk.

- **Refresh Cache**: Starts a full refresh of the datasource cache. To delete the datasource cache you can also restart the BigFix BES Web Reports Server service.
- **View Errors**: Allows you to view all recent errors that have occurred in the Web Reports system. These errors usually occur in the background and can affect the integrity of the data. They are usually related to connection problems or other problems with the datasource. Only an administrator can clear these errors.
- **Local Database Settings:** Shows the local database DSN and the local BigFix Reporting Server.

Note: In case you have defined multiple datasources for aggregation by Web Reports and the name of the LDAP directory for each BigFix Root Server is the same, then the LDAP user login for Web Reports is authenticated by either of the BigFix Root Servers only. For a successful login, ensure that both the BigFix Root Servers are up and running. If either of them is down (for example, for maintenance), the LDAP user login fails.

Add New Datasource

This page allows you to add a new datasource for aggregation by Web Reports.

To reach this page, select **Administration > Datasource Settings > Add New Datasource**.

Datasource Name: Enter a descriptive name for this new datasource.

URL: Enter the URL of the root server to which to connect. The URL must also include the appropriate port number.

Master Operator Credentials: Enter the Master Operator credentials. These credentials are used only once, and are not saved.

Note: In case you have defined multiple datasources for aggregation by Web Reports, all datasources must have Enhanced Security at the same level: a mixed condition is not managed.

Edit Datasource

This page allows you to edit the settings for a selected datasource (to the left of the row).

To reach this page, select **Administration > Datasource Settings > Edit**.

URL: Enter the URL of the root server to which to connect. The URL must also include the appropriate port number.

Note: You cannot change the name of your datasource.

Master Operator Credentials: Enter the Master Operator credentials if the URL is changed.

Errors

This page is available by selecting **Administration > Errors**.

It shows any current errors based on the last action taken.

Appendix A. Tasks for advanced users

This section presents tasks unlikely to be needed by the typical user, but which can be of use to advanced users with specific customization needs.

Understanding the Web Report File

Web Reports has a general report format using an XML wrapper. It can show reports from content sites and new reports can be added, edited, or removed.

The report file must either have the extension `.beswrpt` or `.webreport`, and is written in XML. It has the form:

```
<BESWebReport>
<Name>Report Title</Name>
<Type>[TemplateReport] | [CustomReport] | [ExternalReport]</Type>
<URLParameters>param1=value1&amp;param2=value2</URLParameters>
<Data>Custom data or external URL</Data>
<SourcePage>Source Page in Web Reports</SourcePage>
</BESWebReport>
```

The `.beswrpt` file can also contain multiple reports in one xml file:

```
<BESWebReports>
 <BESWebReport>




 </BESWebReport>
 <BESWebReport>




 </BESWebReport>
</BESWebReports>
```

Most of the tags are self-explanatory. The Name tag provides the title of the report. URLParameters and Data depend on the Type tag. The Type tag can be one of three strings

- TemplateReport
- CustomReport
- ExternalReport

These strings are case-sensitive.

Creating a Custom Report

This page lets you create a custom report. A report like this is actually code that generates a printable report.

It typically consists of HTML with embedded Relevance and JavaScript commands. You can choose to make this report public or private.

Take note that, if you have a brand new installation of the product, the import or save of custom reports is disabled by default. To import or save custom reports, the product administrator must set the value of key `AllowCustomReportCreation` to 1. Also the view of custom reports to non-administrator users is disabled by default. To allow any user to view custom reports, the product administrator must set the value of key `AllowUserViewCustom` to 1. Depending on your installation, these registry keys can be found in:

On Windows operating systems:

`HKLM\Software\WOW6432Node\BigFix\Enterprise Server\BESReports`

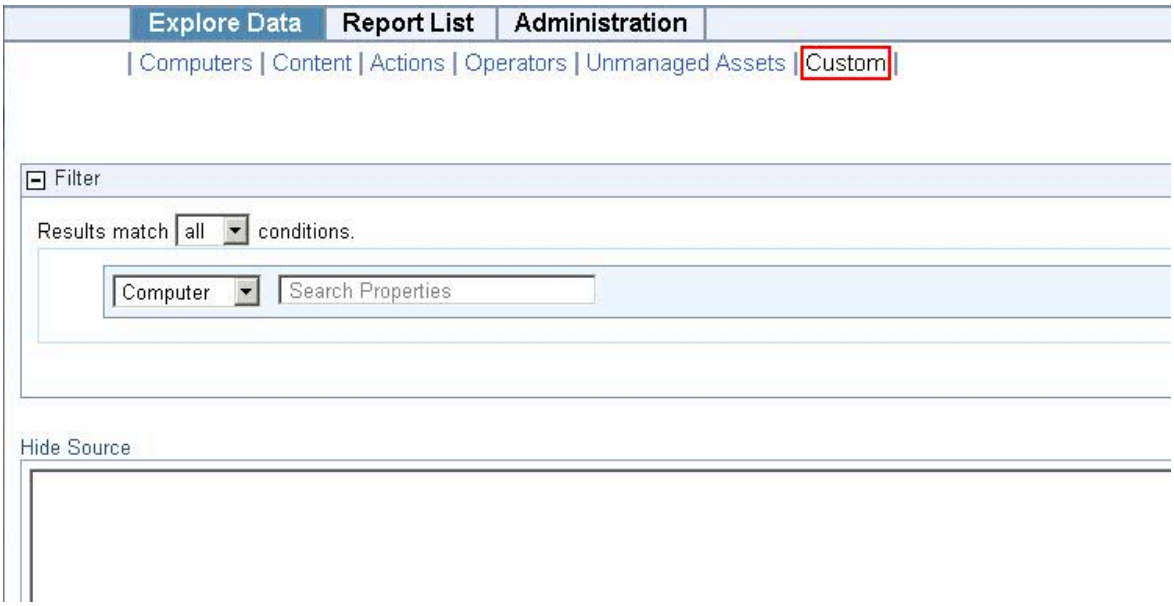
On Linux operating systems:

In the configuration file `/var/opt/BESWebReportsServer/beswebreports.config`, section `[Software\BigFix\Enterprise Server\BESReports]`

If you modify any of these registry keys, to enable the change, you must restart the Web Report server.

To create a custom report:

1. Select **Explore Data > Custom**.



2. There is a **Filter** box. Set it to apply to just the subset of data you want your custom report to be based on.
3. Fill in the text box by specifying the full report request. For example you can specify to list the names of your BigFix computers as follows:

```
<div>Computer Names</div>
    <?Relevance names of bes computers?>
```

   Note: In the corresponding XML file this information is displayed in the character data (CDATA) block of the Data tag

4. When you like what you see, click the **Save Report** button to add your custom report to the list.

When in the list you can change its visibility, label it, and schedule it, as with any other report. The following section describes in more detail how to create a custom Web Report using XML.

Web Reports XML

A custom report is made of HTML, Relevance, and JavaScript, embedded in an XML file.

In the Data tag specify the full report request using the character data (CDATA) block. The XML parser does interpret the CDATA block as markup, so you do not have to escape your included HTML or JavaScript. You can also include an optional parameter tag such as URLParameters tag for extra information to use.

For more information about the specific set of parameters available, see the BigFix support site.

The following is an example of custom web report:

```
<BESWebReport>
  <Name>Example Custom Report</Name>
  <Type>CustomReport</Type>
  <URLParameters>computerID=computerRecord</URLParameters>
  <Data>
   <![CDATA[
    <div>Computer Names</div>
    <?Relevance names of bes computers?>
   ]]>
  </Data>
  <SourcePage>ExploreComputers</SourcePage>
 </BESWebReport>
```

This report lists the names of your BigFix computers.

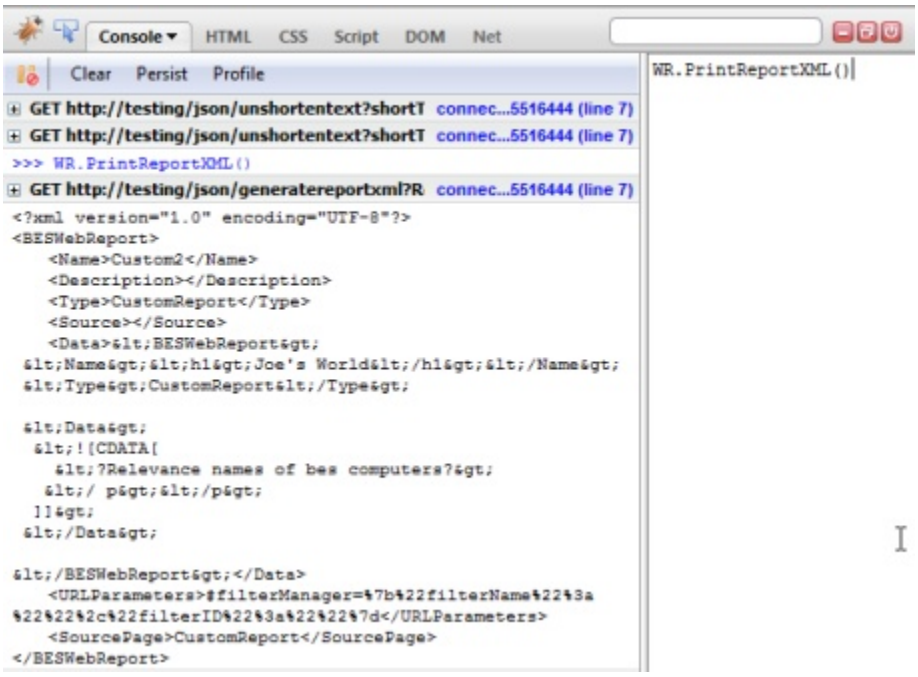
Creating a Portable Report for Propagation

As you explore data, you can save a report at any time. In general, if you want to share the report with other users, you can set its visibility to **Public** in the **Report List**.

However, there is an advanced technique that can be used if you are a site creator. You might notice that an abbreviated description of your report is shown as a part of the URL, as seen in the address bar of the browser. That, however, is a compressed version designed

to stay within the 2048 character limit in Internet Explorer, and is not portable. To make a portable report, follow these steps:

1. Click the **Explore Data** tab at the top of the Web Reports window.
2. Configure the columns you want to display as well as any filters you want to apply.
3. Click the **Save Report** button.
4. Open a JavaScript™ debugger, such as Firebug for Firefox.
5. In the console area of the debugger, enter the command **WR.PrintReportXML()**.



This example uses Firebug. WR.PrintReportXML is an embedded JavaScript™ that prints a portable XML version of the current report.

It might look like this code sample:

```
<?xml version="1.0" encoding="UTF-8"?>
<BESWebReport>
  <Name>Example Report</Name>
  <Type>TemplateReport</Type>
  <Data></Data>
```

```
  <URLParameters>#wr_computerTable=%22sort%3DR-Computer%2520
    Name%26dir%3Ddesc%26startIndex%3D0%26
    results%3D50%26c%3DR-Computer%2520Name%26c%3DR-IP%2520
    Address%26c%3DR-OS%26c%3DR-CPU%26c%3DR-Last%2520
    Report%2520Time%22</URLParameters>
  <SourcePage>ExploreComputers</SourcePage>
</BESWebReport>
```

6. Copy this XML to a text editor and save it with the extension `beswrpt`.

You have now created a portable report that you can easily propagate in any content site or import into the Report List page. Note that the report is contained in the `URLParameters` tag. This listing shows line feeds for readability, but the actual XML has an uninterrupted line of text.

Note: Take into account that, if you have a fresh installation of BigFix, the import report option is disabled by default. To import a report, the product administrator must set the value of the `AllowCustomReportCreation` registry key to 1.

Exporting activity reports to CSV files

To create a hardcopy of a report generated by BigFix, export the report to a CSV file and print it.

To create the CSV report file schedule it as an activity in the Create scheduled Activity window opened from the **Administration > Scheduled Activities** menu. For additional information see Creating Scheduled Activities (on page 75).

You can also use the CSV file to create charts and statistics based on the information in the report.

A Web Report exported to a CSV file has an Excel-compatible CSV format. Any string containing characters that might be interpreted as a formula by Microsoft Excel such as `"+myfield"`, are transformed in literal strings as shown in the following example:

```
"=""+myfield"""
```

The following characters are handled in this way: `+` (plus), `-` (minus), `/` (slash), `*` (asterisk) and `=` (equal).

Exporting activity reports to PDF documents

Web Reports can generate PDF documents for printing or mailing.

PDF reports can be sent by setting the PDF format option when creating or editing a scheduled activity, or by exporting the report as a PDF document.

On Windows Systems

Important: On Windows Server 2016 and later, Microsoft Windows security patches removed the ability for the LocalSystem account to access "desktop resources", including printers. Because of that, if you are running the Web Reports service "BESWebReportsServer" as LocalSystem, you will not be able to generate reports in PDF format. Web Reports will be able to generate PDF reports only if the service is run by a *local user account* or by a *service account*.

Note: You can keep running BESWebReportsServer as LocalSystem if you do not need to use the PDF export feature. Exports in other formats are still available.

Refer to the procedure described in How to enable PDF Reports if the version of Web Reports is lower or equal to 10.0.9.

Otherwise, run the following steps to add this capability to your Web Reports installation on Windows platforms.

1. On the BigFix console click Fixlets and Tasks.
2. Search for the following task ID:
    - Task ID: 5436: BES Web Reports: Enable PDF Reports
3. Run the action in this task to automatically install the PDF generator.

Note: The Task ID 5436 could be relevant also when PDF Reports were already enabled in the past with a lower Web Reports version. In this case, it is mandatory to run the above steps to avoid malformed PDF Reports.

Registry Settings

All the following settings are under the key registry `HKLM\Software\WOW6432Node\BigFix\Enterprise Server\BESReports`.

Setup

- PDFEnable (set to `1` to enable PDF generation)
- PDFPostScriptPath
- PDFPrinterName

Logging

- PDFLogPath

Default Header and Footer

- PDFDefaultHeader
- PDFDefaultFooter

Using an unprivileged user to render the report and generate the PDF

- PDFUseUnprivileged (set to `1` to use the account specified by the values below)
  - UnprivilegedUsername
  - UnprivilegedDomain
  - UnprivilegedPassword

Timeout Settings

- PDFReportTimeout (in minutes, default `60`)
- PDFPrintTimeout (in minutes, default `60`)

Internet Explorer post-rendering pause

- PDFPause (in seconds, default `10`, gives components time to initialize before printing)

Logging PDF generation on Windows systems

The keys to enable logging are stored in the `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node` section under `HKLM\Software\WOW6432Node\BigFix\Enterprise Server\BESReports`.

Run the following steps to enable logging PDF generation:

1. Set the `PDFLogPath` registry key to `C:\webreportspdf.log`.
2. Ensure that the server machine was restarted after running the installation.
3. Verify that the following registry keys have are correct values:
    - `PDFEnable` must be set to 1.
    - `PDFPostScriptPath` must be equal to the port of the printer added during the installation.
    - `PDFPrinterName` must be equal to the name of the printer added during the installation.

Troubleshooting PDF generation on Windows systems

If charts are not displayed in the generated PDF, ensure that Internet Explorer, running under the SYSTEM account on the Web Reports server box, has the correct security settings to render Web Reports pages.

- Do the following to accomplish this task:
    - Open Internet Explorer using the **at** or the **schtasks** commands.
    - Navigate to the Web Reports Overview page.
    - Verify that the charts display. If they do not display, change the security settings to allow ActiveX plugins and JavaScript.
- On Windows platform, after the PDF Reports have been enabled, if you try to export a report as PDF, the created pdf does not contain the expected report but the following error:

```
HTTPS Error: Content BlockedContent was blocked because
         it was not signed by a valid securitycertificate.
         For more information see 'Certificate Errors' in Internet
 Explorer Help.
```

Workaround:

The certificate must be added to the Web Reports server machine so all accounts are not blocked. You can export the certificate from the **Certificate Errors** dialog that is displayed by your web browser when you connect to the Web Reports server the first time.

To add the certificate to the machine store:

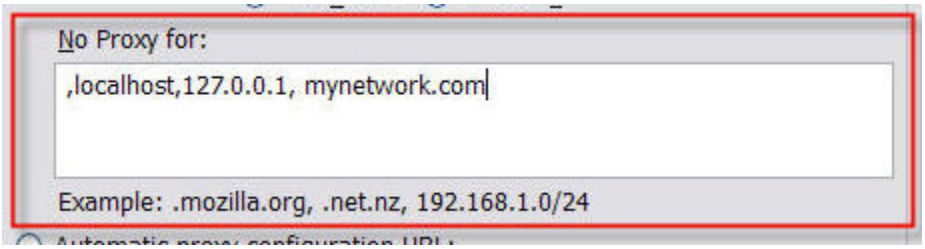
1. Right click the saved certificate and select **Install Certificate**.
2. In the Import Certificate Wizard select **Local Machine** as Store Location.
3. Select **Place all Certificates in the following Store**.
4. Click Browse.
5. Select **Trusted Root Certification Authorities**.
6. Click Next.
7. Click Finish.

On Linux Systems

If you installed Web Reports on a Linux system, you do not have to install extra components to export reports as PDF documents, but you must run some configuration steps if they apply to your environment.

If BigFix server uses a proxy connection to communicate over the Internet and you run Web Reports using Firefox on the Linux system where you installed the Web Reports.

Ensure that the Firefox browser is not configured for the system's fully qualified hostname. For example, if your network domain is mynetwork.com, configure the Firefox connection settings as highlighted in the following picture:



If the DISPLAY variable is set to a value different from DISPLAY=:0.0

Manually change the export statement in the `/etc/init.d/beswereports` file as follows:

1. Stop the Web Reports service by running:

```
/etc/init.d/beswereports stop
```

2. Edit the file `/etc/init.d/beswereports`.
3. Set the **DISPLAY** variable to correctly point to your X server.
4. Save the file.
5. Restart the Web Reports service by running:

```
/etc/init.d/beswereports start
```

If the runlevel set on your Linux system is different from 5.

Modify the runlevel and set it to 5, or use `xvfb`.

Run these steps if you decide to use `xvfb`:

1. Set up the optional channel as follows:

```
rhn-channel --add --channel=rhel-x86_64-server-optional-6
```

2. Install the packages:

```
yum install xorg-x11-server-Xvfb.x86_64
yum install gstreamer-plugins-base-XXX
yum install urw-fonts-XXX
```

where *XXX* depends on the specific version number of the packages installed, for example: *gstreamer-plugins-base-0.10.36-10.e17.x86_64*.

Note: On Red Hat Linux 8, the library to use for the `yum install` command is `urw-base35-fonts-XXX`, where *XXX* depends on the specific version number of the packages installed.

You can get the full, current name of these packages by running the following commands on your system:

```
rpm -qa | grep urw-fonts
rpm -qa | grep gstreamer
```

3. **Important:** This step is no longer required if you install or upgrade to BigFix 10.0.5.

   Modify the script that manages the PDF exports as follows:

   a. Edit the script `/var/opt/BESWebReportsServer/BESReportsData/BESExe/generatepdf.sh`

   b. Prepend:

   ```
   xvfb-run -a -s "-screen 0 1024x768x16"
   ```

   before the statement:

   ```
   $besexe_folder$athena_folder$athena_executable --ignor
   e-certificate-errors
   --delay 5000 --no-cache $arg1 $arg2
   ```

   so that it is a unique command line as follows:

   ```
   xvfb-run -a -s "screen 0 1024x768x16" $besexe_folder$a
   thena_folder$athena_executable
   --ignore-certificate-errors --delay 5000 --no-cache $a
   rg1 $arg2
   ```

   c. Save the script file.

If you cannot generate the PDF.

If the generation of the PDF does not complete successfully and the `/var/log/BESWebReportsPdfExport.log` file shows the following error:

error while loading shared libraries: libXss.so.1: cannot open shared object file: No such file or directory

Install the following library which is required on Red Hat by issuing the command:

```
sudo yum install libXScrnSaver
```

If you experience a slow rendering when the PDF is generated.

If the generation of the PDF takes longer than 5 seconds to display the Web Reports exports to the PDF only the data that were available before the 5 seconds elapsed. To bypass this limitation, increase the delay as follows:

1. Edit the script `/var/opt/BESWebReportsServer/BESReportsData/BESExe/generatepdf.sh`
2. Increase the value that is assigned to `-delay` in the statement:

   ```
   $besexe_folder$athena_folder$athena_executable --ignore-cer
   tificate-errors
   --delay 5000 --no-cache $arg1 $arg2
   ```

   The value is expressed in milliseconds and 5000 ms is the default vale.
3. Save the script file.

Logging PDF generation on Linux systems

To gather and review the output from the call to `athenapdf`, redirect the stdout and stderr from `athenapdf` to a file.

Before doing the redirection, ensure that you enabled logging for Web Reports as it is explained in Logging Web Reports (on page 113).

Run these steps to do the redirection:

1. Make a backup copy of the script

   `/var/opt/BESWebReportsServer/BESReportsData/BESExe/generatepdf.sh`
2. Update the script by changing the following line:

   ```
   $besexe_folder$athena_folder$athena_executable
    --ignore-certificate-errors
    --delay 5000 --no-cache $arg1 $arg2
   ```

   as follows:

   ```
   $besexe_folder$athena_folder$athena_executable
    --ignore-certificate-errors
   --delay 5000 --no-cache $arg1 $arg2 1>/tmp/pdfout.txt
   ```

   By doing so you redirect the stdout and stderr from `athenapdf` to the `/tmp/pdfout.txt` file.

Exporting the report output to a PDF file

If you configured Web Reports to export reports as PDF, when you run a report from the **Reports List** panel, the entry **Export to PDF** is displayed in the top right corner of the report output window.

Click it to save the output of the report in a PDF file on the system where the Web Reports is installed. Note that customized reports cannot be exported to a PDF file.

Customizing HTTPS on Web Reports

BigFix Web Reports is configured to use HTTPS by default when it gets installed and creates its own certificate during the installation. If you want to replace it, you need to configure HTTPS manually.

First steps

If you have a trusted SSL security certificate and key from a certificate authority, you can configure BigFix Web Reports to use this certificate and key to enable trusted connections. You can also use a self-signed certificate.

You can configure Web Reports to work with HTTPS by using a certificate file containing the private key or two separate files one for the certificate and another for the private key. To configure Web Reports on Windows or Linux systems manually, do the following steps:

1. Install or upgrade OpenSSL on your system to the latest available version.
2. Ensure that an OpenSSL command-line tool is available.
3. Create a Certificate Signing Request (csr) with your company and Web Reports server information.
4. **EITHER:** Generate a Self-Signed Certificate **OR** Request a Certificate from a Certificate Authority.

When an HTTPS certificate is set, the certificate is supplied by the server to connecting clients (browsers) and they present a dialog to the user containing information from the certificate. If the certificate meets all of the trust requirements, then the browser connects without any interventions by the user. If the certificate does not meet the trust requirements of the browser, then the user is prompted with a dialog that asks if it is OK to proceed with the connection, and giving them access to information about the certificate. A trusted certificate is signed by a trusted authority (such as Verisign), contains the correct host name, and has not expired.

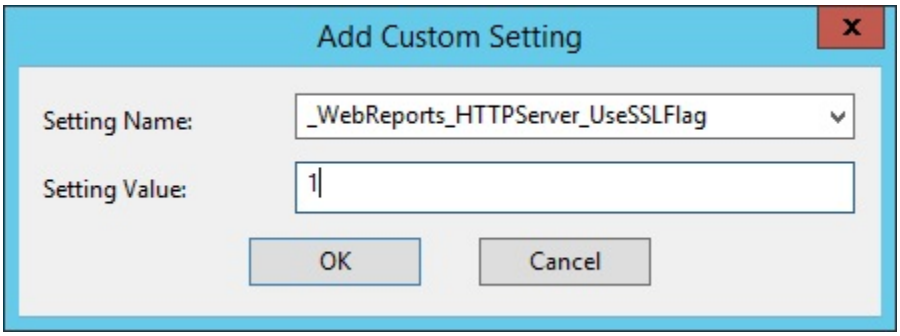
When you have a trusted SSL certificate, copy the .pvk (if you have one) and the .pem files on the computer(s) running Web Reports.

In the following sections, we show ways to implement these macro-steps:

- Specify that you are using a secure communication.
- Specify where the SSL certificate and private key files are located.
- Specify the HTTPS port number
- Specify a port to redirect to HTTPS.
- Restart the relevant services.

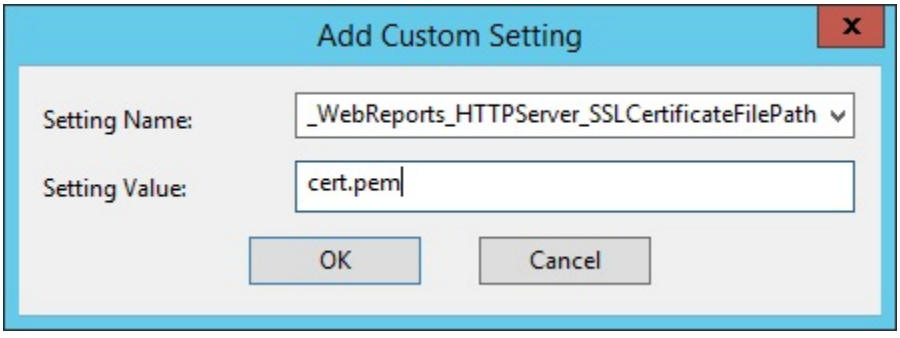
Customizing HTTPS using the BigFix Console

1. From the BigFix console, select the **Computers** tab.
2. Right click on the computer on which Web Reports runs and click **Edit Computer Settings**.
3. Look for the **_WebReports_HTTPServer_UseSSLFlag** setting. If it exists, do not create a second one, but edit its value to `1` to enable HTTPS. If it does not exist, add it.

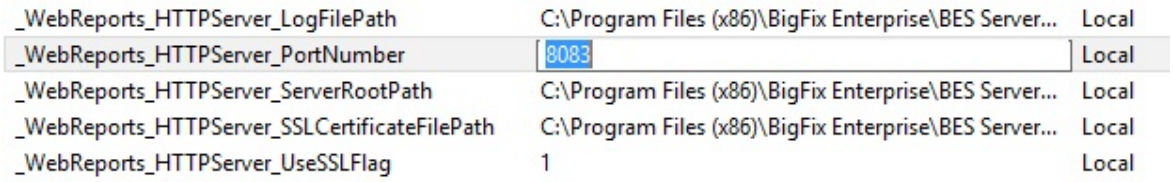


4. If you combined the private key file with the certificate file, skip this step and set only the **_WebReports_HTTPServer_SSLCertificateFilePath** setting.

   Look for the **_WebReports_HTTPServer_SSLPrivateKeyFilePath** setting. If it exists, do not create a second one, but edit its value to the full path name of the private key (`.pvk` file) which contains the private key for the server. The private key must not have a password. If it does not exist, add it.
5. Look for the **_WebReports_HTTPServer_SSLCertificateFilePath** setting. If it exists, do not create a second one, but edit its value to the full path name of the `.pem` file which might contain both the certificate and private key for the server, or only the certificate. If it does not exist, add it.



6. Look for the **_WebReports_HTTPServer_PortNumber** setting. If it exists, do not create a second one, but edit its value to the port number you would like to use. If it does not exist, add it:



7. When SSL is enabled define the forwarding port with the following settings:
   - **_WebReports_HTTPRedirect_Enabled** to 1
   - **_WebReports_HTTPRedirect_PortNumber** to the port listening for HTTP connection and redirecting the client to HTTPS.
8. To require TLS12 for web browser requests, look for **_WebReports_HTTPServer_RequireTLS12**. If it exists, do not create a second one, but edit its value to `1`. The Web Reports component always uses TLS 1.2 when communicating with the BigFix server, regardless of local settings or settings of the masthead.

   Important: Use of a TLS with a version earlier than 1.2 is deprecated.

9. Restart the **BES Web Reports Server** service:
   - On Windows, open **Services**, select **BESWebReports** and on the **Action** menu, click **Restart**.
   - On Linux run from the prompt: `service beswebreports restart` or `/etc/init.d/beswebreports restart`

Customizing HTTPS manually on Windows systems

When you have a trusted SSL certificate (a `.pem` file), place it on the computer running Web Reports (usually the server) and follow these steps.

1. Run **regedit** and locate `HKEY_LOCAL_MACHINE\Software\Wow6432Node\BigFix\EnterpriseClient\Settings\Client`

   You need to add or modify subkeys for the HTTPS flag, for the location of the SSL certificate, for the HTTPS port number, and for the redirection to HTTPS.
2. Create a subkey of **Client** called `_WebReports_HTTPServer_UseSSLFlag` (if it does not exist yet). Add a string value (reg_sz) called "value" to the key and set it to 1 to enable HTTPS.
3. Create a subkey of **Client** called `_WebReports_HTTPServer_SSLCertificateFilePath` (if it does not exist yet). Add a string value (reg_sz) called "value" to the key and set it to the full path name of the SSL certificate (cert.pem).
4. Create a subkey of **Client** called `_WebReports_HTTPServer_PortNumber` (if it does not exist yet). Add a string value (reg_sz) called "value" to the key and set it to the port number you want to use (typically 443).
5. Create a subkey of **Client** called `_WebReports_HTTPRedirect_Enabled` (if it does not exist yet). Add a string value (reg_sz) called "value" to the key and set it to 1 to enable the browser redirection of HTTP to HTTPS.
6. Create a subkey of **Client** called `_WebReports_HTTPRedirect_PortNumber` (if it does not exist yet). Add a string value (reg_sz) called "value" to the key and set it to the number of the port listening for HTTP requests and redirecting them to HTTPS.
7. Restart the **BESWebReports** service.

Customizing HTTPS manually on Linux systems

When you have a trusted SSL certificate (a `.pem` file), place it on the computer running Web Reports and customize the keywords in the applicable file.

- `besclient.config` - if a client is installed together with Web Reports
- `beswebreports.config` - if only Web Reports is installed

To define the port number you want to use:

```
[Software\BigFix\EnterpriseClient\Settings\Client\_WebReports_HTTPServer_PortNumber]
value = 443
```

To define the full path name of the SSL certificate (`cert.pem`):

```
[Software\BigFix\EnterpriseClient\Settings\Client\_WebReports_HTTPServer_SSLCertificateFilePath]
value = /tmp/CERT/cert.pem
```

Important: If you combined the private key file with the certificate file, skip this setting:

```
[Software\BigFix\EnterpriseClient\Settings\Client\_WebReports_HTTPServer_SSLPrivateKeyFilePath]
value = /tmp/CERT/pvtkey.pvk
```

To enable HTTPS:

```
[Software\BigFix\EnterpriseClient\Settings\Client\_WebReports_HTTPServer_UseSSLFlag]
value = 1
```

To enable redirection of HTTP to HTTPS:

```
[Software\BigFix\EnterpriseClient\Settings\Client\_WebReports_HTTPRedirect_Enabled]
value = 1
```

To specify the port listening for HTTP requests and redirecting them to HTTPS:

```
[Software\BigFix\EnterpriseClient\Settings\Client\_WebReports_HTTPRedirect_PortNumber]
value = 8080
```

Stop and restart the beswebreports service.

Logging Web Reports

You can keep track of your Web Reports usage by setting up a log file. In a fresh installation, Web Reports logging is disabled by default and its settings do not exist.

The settings to control Web Reports logging, if present, are stored:

- on Windows, in the registry key `HKEY_LOCAL_MACHINE\Software\Wow6432Node\BigFix\Enterprise Server\BESReports`
- on Linux, in the section [Software\BigFix\Enterprise Server\BESReports] of the configuration file /var/opt/BESWebReportsServer/beswebreports.config

The LogOn setting controls turning the logging on and off. Its default value is 0.

The LogPath setting controls the path of the active log file.

The LogFileSizeLimit setting controls the maximum log file size in bytes. When the currently used log file reaches this size, a "log rotation" is performed, the file is renamed and a new log file is used. A maximum of 10 old log files is kept, then the oldest log file is discarded. The maximum number of old log files (10) is fixed and the numbering is cyclical, from 0 to 9. If "file.txt" is the name of the log file, the old log files will be named file.txt_0, file.txt_1, ..., file.txt_9. The default value of _LogFileSizeLimit_ is 0, which means log rotation is disabled and logging is performed on a single log file that can grow indefinitely. The minimum value to enable log rotation is 1048576 (1 MB). We recommend setting LogFileSizeLimit to at least 10485760 (10 MB).

The EnabledLogs setting controls what kind of information is logged. Its value can be one of following: debug|critical|memory|store_usage|all. Its default value is "all".

To enable Web Reports logging, perform the following steps.

On Windows:

1. Run regedit.
2. Find the key `HKEY_LOCAL_MACHINE\Software\Wow6432Node\BigFix\Enterprise Server\BESReports`.
3. Create a new string value named LogPath and set it to the full path name of your log file, for example "C:\full_path\file.txt". The path must already exist.

Note: When running the Web Reports service with the custom user specified at installation time, the custom user must have read and write permissions on the directory where your log file is located.

4. Create a new DWORD value named LogFileSizeLimit and set it to the log file size in byte. We recommend a value of at least 10485760 (10 MB).
5. Create a new string named EnabledLogs and set it to "all".
6. Create a new DWORD value named LogOn and set it to 1 to turn logging on.
7. Close regedit.
8. Restart Web Reports.

On Linux:

1. Open the configuration file `/var/opt/BESWebReportsServer/beswebreports.config`.
2. Find the section [Software\BigFix\Enterprise Server\BESReports] and, under that section, add the following settings.
3. Add the LogPath setting and set it to the full path name of your log file. Like this

```
LogPath = /var/log/WebReports/WebReports.log
```

Note: When running the Web Reports service with the custom user specified at installation time, the custom user must have read and write permissions on the directory where your log file is located.

4. Add the LogFileSizeLimit setting and set it to a value of at least 10485760 (10 MB). Like this

```
LogFileSizeLimit = 10485760
```

5. Add the EnabledLogs setting and set it to "all". Like this

```
EnabledLogs = all
```

6. Add the LogOn setting and set it to 1 to turn logging on. Like this

```
LogOn = 1
```

7. Close the file.
8. Restart Web Reports.

The next time you launch Web Reports, a log of the session is saved to the specified file.

Changing the temporary files on Linux

You can specify a directory for your temporary files of Linux Web Reports by setting up a parameter in the Web Reports configuration file.

On Linux

To specify a directory for your temporary files on Linux, perform the following steps:

1. Stop the Web Reports component.
2. Open the following configuration file: `/var/opt/BESWebReportsServer/beswebreports.config`
3. Add the parameter named `TemporaryDirPath` in the `[Software\BigFix\Enterprise Server\BESReports]` section.
4. Specify the directory for your temporary files of Linux Web Reports.
5. Restart the Web Reports component.

If the setting is not configured, Web Reports will now use the default temporary directory /var/opt/BESWebReportsServer/BESReportsData/Temp.

Querying Using HTTP GET

You can query and access Web Reports by using HTTP GET. Provide the URL and port for the Web Reports program, and then pass the command you want in your browser address line.

If you are already logged in to the program, you can access the main page with a URL:

```
http://bigco.com:80/webreports?page=Main
```

If you have installed BigFix 9.5, the URL to the main page is:

```
http://bigco.com:80/webreports?page=Main
```

In this example, **bigco.com** is your domain, **80** is the default BigFix port, and **page=Main** describes the part of the program you want to access. If you have not yet logged in, you can pass your **Username** and **Password** on the same line:

```
http://bigco.com:80/webreports?Username=myName&Password=myPassword&page=Main
```

If you have installed BigFix 9.5, the URL is:

```
http://bigco.com:8080/webreports?Username=myName&Password=myPassword&page=Main
```

Querying Using SOAP

You can also access Web Reports using SOAP. Most client libraries require the location of a Web Services Description Language (WSDL) file, a method name, and parameters to pass into the method.

The WSDL file describes the network endpoints required to query the BigFix Database using Web Reports. The WSDL can be accessed from the Web Reports server as in the following example: `http://server/webreports?wsdl`.

Alternatively, you can find a sample file, `relevance.wsdl`, in the BigFix installation directory. This WSDL file defines `relevanceExpr`, which allows you to evaluate a relevance expression. If you installed BigFix to a folder named `BigFix Enterprise`, you can find the file in this directory:

```
BigFix Enterprise\BES Server\BESReportsServer\wwwroot\soap
```

The registry location for your installation is `HKLM\SOFTWARE\Wow6432Node\BigFix\Enterprise Server\BESReports\Paths`.

This registry key has a string value named `wsdl` that contains the path name for the WSDL file.

The request includes a tag labeled `relevanceExpr`, which contains the relevance expression number of BigFix computers. This is one of the operations defined in the WSDL file.

Some of the available methods include:

```
GetRelevanceResult( String relevanceExpression, String username, String
 password )
StoreSharedVariable( dashID, variableName, variableValue, [success/failure
callback], [database id] )
DeleteSharedVariable( dashID, variableName, [success/failure callback],
[database id] )
```

Note: Only Web Report administrators are allowed to use the `StoreSharedVariable` and `DeleteSharedVariable` methods.

To submit queries from SOA clients specify the following BigFix http path:

```
http://web_report_server/soap
```

where *web_report_server* is the hostname or IP address of the Web Report server.

PERL

PERL code using the SOAP::Lite module.

It takes three arguments, Web Reports username, password, and relevance expression, and prints the results of the call.

```
use SOAP::Lite;
#arguments: [hostname] [username] [password] [relevance expression]
#hostname only, e.g. 'example.com' rather than
 'http://example.com/webreports'
my $host = $ARGV[0];
my $username = SOAP::Data->name('username' => $ARGV[1] );
my $password = SOAP::Data->name('password' => $ARGV[2] );
my $expr = SOAP::Data->name('relevanceExpr' => $ARGV[3] );
my $service = SOAP::Lite -> uri( 'http://' . $host . '/webreports?wsdl' )
-> proxy('http://' . $host );
```

```
my $result = $service -> GetRelevanceResult( $expr, $username, $password );
if( $result->fault ) {
print "faultcode: " . $result->faultcode . "\n";
print "faultstring: " . $result->faultstring . "\n";
}
else {
  foreach my $answer
 ( $result->valueof( "//GetRelevanceResultResponse/a" ) ) {
    print $answer . "\n";
  }
}
```

Raw SOAP Request and Response Format

How the SOAP request and response look like.

A SOAP request looks like this:

```
<?xml version="1.0" encoding="UTF-8"?>
<env:Envelope xmlns:env="http://schemas.xmlsoap.org/soap/envelope/" >
 <env:Body>
  <GetRelevanceResult xmlns="http://[webreportshostname]:[webreportsport]
     /webreports?wsdl">
   <relevanceExpr>names of bes computers</relevanceExpr>
   <username>user</username>
   <password>password</password>
  </GetRelevanceResult>
 </env:Body>
</env:Envelope>
```

A SOAP response looks like this:

```
<?xml version="1.0" encoding="UTF-8"?>
<env:Envelope xmlns:env="http://schemas.xmlsoap.org/soap/envelope/">
 <env:Body>
```

```
  <GetRelevanceResultResponse
 "xmlns=http://[webreportshostname]:[webreportsport]
      /webreports?wsdl">
   <a>Computer 1</a>
   <a>Computer 2</a>
   <a>Computer 3</a>
  </GetRelevanceResultResponse>
 </env:Body>
</env:Envelope>
```

Sample relevance expressions are available at Resources. You can also consult your BigFix representative for more information.

Session Inspectors

Console and Web Reports both depend on an in-memory session cache to provide an efficient view of your database.

Due to their distinct environments, these two programs have some significant differences:

BigFix Console	BigFix Web Reports
Does not maintain Fixlet History inspectors.	Maintains Fixlet History inspectors, however, to reduce the memory footprint, version 8.0 runs slower.
Current inspectors are designed to work in the BigFix Console only.	**Current** inspectors do not work.
Inspectors dealing with globally visible Fixlet messages are consistent across applications.	Locally visible Fixlet messages return nothing.
Works with only one BigFix server.	Works across multiple BigFix servers.

JavaScript **Relevance** calls are instantaneous.	JavaScript **Relevance** calls generate an HTTP request, which incurs a round-trip penalty to the server.
Links to Fixlet filters, computer groups, computers, Fixlet messages, tasks, and analyses work.	Links to Fixlet filters and computer groups *do not* work. However, links to computers, Fixlet messages, tasks, and analyses *do* work.

Displaying Web Reports from Content Sites

Web Reports accepts a report format that can display reports from content sites, allowing new reports to be added, edited, or removed by Fixlet actions or tasks.

There are three basic report types: **External**, **Template,** and **Custom**. The report file must be a valid XML file with an extension of **.beswrpt or .webreport**.

The **Name** tag corresponds to the same-named columns in Report listings.

The contents and the existence of the **URLParameters** and **Data** tags depend on the **Type** tag. The Type tag can be one of three case-sensitive strings: TemplateReport, CustomReport, or ExternalReport.

The .beswrpt file can also contain multiple reports in a single XML file:

```
<BESWebReports>
  <BESWebReport>
    .
    .
    .
  </BESWebReport>
  <BESWebReport>
    .
    .
    .
  </BESWebReport>
 </BESWebReports>
```

External Reports

An External Report contains a URL pointing to another page, service, or reporting engine.

The report file is a simple wrapper containing the full URL of the destination. When you import an External Report, it is shown in the Web Reports list like any other report. When you click an External Report, it loads the target page into the browser.

Template Reports

A Template Report is similar to an External Report, except that the base of the URL is assumed to be the Web Reports server.

These reports are essentially the same as the native Web Reports. The information in this section is included for completeness; in general you only need to use Custom or External reports.

The Data tag does not exist for this report. Instead, it passes all its information in the **URLParameters** tag.

For example, you might create this Issue Assessment report:

```
 <BESWebReport>
  <Name>Example Issue Assessment Report</Name>
  <Description>
   An example report. Runs the Issue Assessment report with specific
 Fixlets,
BES Support/129 and BES Support/173.
  </Description>
  <Type>TemplateReport</Type>
  <Category>Issue Assessment</Category>
  <Source>HCL</Source>
  <URLParameters>
   FixletParam=BES Support%2f129&amp;FixletParam=BES
Support%2f173&amp;page=VAReport
  </URLParameters>
 </BESWebReport>
```

In XML as in HTML, you need to escape the URL Parameter.

Disabling local operators on Web Reports

Starting from BigFix Version 10.0.8, you can decide to disable the local operators from logging into Web Reports, to use LDAP operators instead.

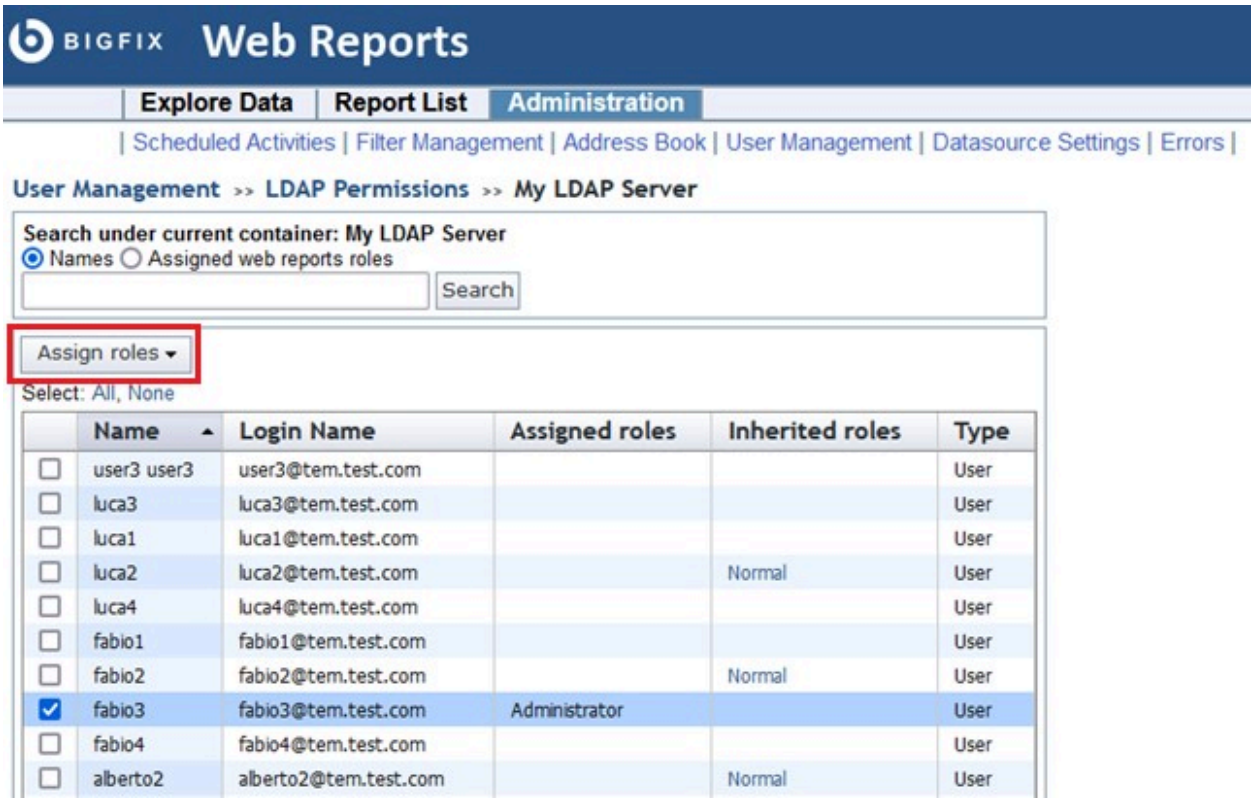
For details about how to disable the local operators, see the **securitysettings** described in BESAdmin Windows Command Line and BESAdmin Linux Command Line.

When logging into the Web Reports using a local operator, the login will be disabled if at least one of the connected BigFix servers (DataSources) has the local operators disabled. In this case, when a local operator attempts to log into the Web Reports, the following error message is displayed:

When logging into the Web Reports using an LDAP user and local operators are disabled, several links and buttons in Web Reports will be greyed out or hidden in order to avoid accounting operations on both local operators or LDAP users.

In the User Management page, the **Create user** link and the **Assign roles** button will be hidden and the **Delete** button will be greyed out for the local operators. The local operators in the list will be showed as normal text.

In My LDAP Server page, the **Assign roles** button will be greyed out when an LDAP user is selected. It will be still possible to associate LDAP groups to Web Reports roles.



In the Global User Options page, the **Password Complexity Rules** and **Password Complexity Desciption** sections will be hidden.

Appendix B. Glossary

This glossary provides terms and definitions for the Modern Client Management for BigFix software and products.

The following cross-references are used in this glossary:

- *See* refers you from a non-preferred term to the preferred term or from an abbreviation to the spelled-out form.
- *See also* refers you to a related or contrasting term.

A *(on page 126)* B *(on page 127)* C *(on page 128)* D *(on page 130)* E *(on page 132)* F *(on page 132)* G *(on page 132)* L *(on page 132)* M *(on page 133)* N *(on page 134)* O *(on page 134)* P *(on page 135)* R *(on page 135)* S *(on page 135)* T *(on page 138)* U *(on page 138)* V *(on page 138)* W *(on page 139)*

A

action

1. See Fixlet *(on page 132)*.
2. A set of Action Script commands that perform an operation or administrative task, such as installing a patch or rebooting a device.

Action Script

Language used to perform an action on an endpoint.

agent

See BigFix agent *(on page 127)*.

ambiguous software

Software that has an executable file that looks like another executable file, or that exists in more than one place in a catalog (Microsoft Word as a standalone product or bundled with Microsoft Office).

audit patch

A patch used to detect conditions that cannot be remediated and require the attention of an administrator. Audit patches contain no actions and cannot be deployed.

automatic computer group

A computer group for which membership is determined at run time by comparing the properties of a given device against the criteria set for group membership. The set of devices in an automatic group is dynamic, meaning that the group can and does change. See also computer group *(on page 128)*.

B

baseline

A collection of actions that are deployed together. A baseline is typically used to simplify a deployment or to control the order in which a set of actions are applied. See also deployment group *(on page 130)*.

BigFix agent

The BigFix code on an endpoint that enables management and monitoring by BigFix.

BigFix client

See BigFix agent *(on page 127)*.

BigFix console

The primary BigFix administrative interface. The console provides a full set of capabilities to BigFix administrators.

BYOD

Bring Your Own Device (BYOD) refers to employees using personal devices to connect to their organizational networks and access work-related systems and potentially sensitive or confidential data.

C

client

A software program or computer that requests services from a server. See also server *(on page 136)*.

client time

The local time on a BigFix client device.

Cloud

A set of compute and storage instances or services that are running in containers or on virtual machines.

Common Vulnerabilities and Exposures Identification Number (CVE ID)

A number that identifies a specific entry in the National Vulnerability Database. A vendor's patch document often includes the CVE ID, when it is available. See also National Vulnerability Database *(on page 134)*.

Common Vulnerabilities and Exposures system (CVE)

A reference of officially known network vulnerabilities, which is part of the National Vulnerabilities Database (NVD), maintained by the US National Institute of Standards and Technology (NIST).

component

An individual action within a deployment that has more than one action. See also deployment group *(on page 130)*.

computer group

A group of related computers. An administrator can create computer groups to organize systems into meaningful categories, and to facilitate deployment of content to multiple computers. See also automatic computer group *(on page 127)* and manual computer group *(on page 133)*.

console

See BigFix console *(on page 127)*.

content

Digitally-signed files that contain data, rules, queries, criteria, and other instructions, packaged for deployment across a network. BigFix agents use the detection criteria (Relevance statements) and action instructions (Action Script statements) in content to detect vulnerabilities and enforce network policies.

content relevance

A determination of whether a patch or piece of software is eligible for deployment to one or more devices. See also device relevance *(on page 131)*.

Coordinated Universal Time (UTC)

The international standard of time that is kept by atomic clocks around the world.

corrupt patch

A patch that flags an operator when corrections made by an earlier patch have been changed or compromised. This situation can occur when an earlier service pack or application overwrites later files, which results in patched files that are not current. The corrupt patch flags the situation and can be used to re-apply the later patch.

custom content

BigFix code that is created by a customer for use on their own network, for example, a custom patch or baseline.

CVE

See Common Vulnerabilities and Exposures system *(on page 128)*.

CVE ID

See Common Vulnerabilities and Exposures Identification Number *(on page 128)*.

D

data stream

A string of information that serves as a source of package data.

default action

The action designated to run when a Fixlet is deployed. When no default action is defined, the operator is prompted to choose between several actions or to make an informed decision about a single action.

definitive package

A string of data that serves as the primary method for identifying the presence of software on a computer.

deploy

To dispatch content to one or more endpoints for execution to accomplish an operation or task, for example, to install software or update a patch.

deployment

Information about content that is dispatched to one or more endpoints, a specific instance of dispatched content.

deployment group

The collection of actions created when an operator selects more than one action for a deployment, or a baseline is deployed. See also baseline *(on page 127)*, component *(on page 128)*, deployment window *(on page 131)*, and multiple action group *(on page 134)*.

deployment state

The eligibility of a deployment to run on endpoints. The state includes parameters that the operator sets, such as 'Start at 1AM, end at 3AM.'

deployment status

Cumulative results of all targeted devices, expressed as a percentage of deployment success.

deployment type

An indication of whether a deployment involved one action or multiple actions.

deployment window

The period during which a deployment's actions are eligible to run. For example, if a Fixlet has a deployment window of 3 days and an eligible device that has been offline reports in to BigFix within the 3-day window, it gets the Fixlet. If the device comes back online after the 3-day window expires, it does not get the Fixlet. See also deployment group *(on page 130)*.

device

An endpoint, for example, a laptop, desktop, server, or virtual machine that BigFix manages; an endpoint running the BigFix Agent.

device holder

The person using a BigFix-managed computer.

device property

Information about a device collected by BigFix, including details about its hardware, operating system, network status, settings, and BigFix client. Custom properties can also be assigned to a device.

device relevance

A determination of whether a piece of BigFix content applies to applies to a device, for example, where a patch should be applied, software installed, or a baseline run. See also content relevance *(on page 129)*.

device result

The state of a deployment, including the result, on a particular endpoint.

Disaster Server Architecture (DSA)

An architecture that links multiple servers to provide full redundancy in case of failure.

DSA

See Disaster Server Architecture *(on page 131)*.

dynamically targeted

Pertaining to using a computer group to target a deployment.

E

endpoint

A networked device running the BigFix agent.

F

filter

To reduce a list of items to those that share specific attributes.

Fixlet

A piece of BigFix content that contains Relevance and Action Script statements bundled together to perform an operation or task. Fixlets are the basic building blocks of BigFix content. A Fixlet provides instructions to the BigFix agent to perform a network management or reporting action.

Full Disk Encryption

To reduce a list of items to those that share specific attributes.

G

group deployment

A type of deployment in which multiple actions were deployed to one or more devices.

L

locked

An endpoint state that prevents most of the BigFix actions from running until the device is unlocked.

M

MAG

See multiple action group *(on page 134)*.

management rights

The limitation of console operators to a specified group of computers. Only a site administrator or a master operator can assign management rights.

manual computer group

A computer group for which membership is determined through selection by an operator. The set of devices in a manual group is static, meaning they do not change. See also computer group *(on page 128)*.

master operator

A console operator with administrative rights. A master operator can do everything that a site administrator can do, except creating operators.

masthead

A collection of files that contain the parameters of the BigFix process, including URLs to Fixlet content. The BigFix agent brings content into the enterprise based on subscribed mastheads.

MCM and BigFix Mobile

Refers to the offering by Bigfix that is common for both Modern Client Management to manage laptops (Windows and macOS) and BigFix Mobile to manage mobile devices (Android, iOS, and iPadOS).

mirror server

A BigFix server required if the enterprise does not allow direct web access but instead uses a proxy server that requires password-level authentication.

Multicloud

The utilization of distinct sets of cloud services, typically from multiple vendors, where specific applications are confined to a single cloud instance.

multiple action group (MAG)

A BigFix object that is created when multiple actions are deployed together, as in a baseline. A MAG contains multiple Fixlets or tasks. See also deployment group *(on page 130)*.

N

National Vulnerability Database (NVD)

A catalog of officially known information security vulnerabilities and exposures, which is maintained by the National Institute of Standards and Technology (NIST). See also Common Vulnerabilities and Exposures Identification Number *(on page 128)*.

NVD

See National Vulnerability Database *(on page 134)*.

O

offer

A deployment option that allows a device holder to accept or decline a BigFix action and to exercise some control over when it runs. For example, a device holder can decide whether to install a software application, and whether to run the installation at night or during the day.

open-ended deployment

A deployment with no end or expiration date; one that runs continuously, checking whether the computers on a network comply.

operator

A person who uses the BigFix WebUI, or portions of the BigFix console.

P

patch

A piece of code added to vendor software to fix a problem, as an immediate solution that is provided to users between two releases.

patch category

A description of a patch's type and general area of operation, for example, a bug fix or a service pack.

patch severity

The level of risk imposed by a network threat or vulnerability and, by extension, the importance of applying its patch.

R

relay

A client that is running special server software. Relays spare the server and the network by minimizing direct server-client downloads and by compressing upstream data.

Relevance

BigFix query language that is used to determine the applicability of a piece of content to a specified endpoint. Relevance asks yes or no questions and evaluates the results. The result of a Relevance query determines whether an action can or should be applied. Relevance is paired with Action Script in Fixlets.

S

SCAP

See Security Content Automation Protocol *(on page 136)*.

SCAP check

A specific configuration check within a Security Content Automation Protocol (SCAP) checklist. Checks are written in XCCDF and are required to include SCAP enumerations and mappings per the SCAP template.

SCAP checklist

A configuration checklist that is written in a machine-readable language (XCCDF). Security Content Automation Protocol (SCAP) checklists have been submitted to and accepted by the NIST National Checklist Program. They also conform to a SCAP template to ensure compatibility with SCAP products and services.

SCAP content

A repository that consists of security checklist data represented in automated XML formats, vulnerability and product name related enumerations, and mappings between the enumerations.

SCAP enumeration

A list of all known security related software flaws (CVEs), known software configuration issues (CCEs), and standard vendor and product names (CPEs).

SCAP mapping

The interrelationship of enumerations that provides standards-based impact measurements for software flaws and configuration issues.

Security Content Automation Protocol (SCAP)

A set of standards that is used to automate, measure, and manage vulnerability and compliance by the National Institute of Standards and Technology (NIST).

server

A software program or a computer that provides services to other software programs or other computers. See also client *(on page 128)*.

signing password

A password that is used by a console operator to sign an action for deployment.

single deployment

A type of deployment where a single action was deployed to one or more devices.

site

A collection of BigFix content. A site organizes similar content together.

site administrator

The person who is in charge of installing BigFix and authorizing and creating new console operators.

software package

A collection of Fixlets that install a software product on a device. Software packages are uploaded to BigFix by an operator for distribution. A BigFix software package includes the installation files, Fixlets to install the files, and information about the package (metadata).

SQL Server

A full-scale database engine from Microsoft that can be acquired and installed into the BigFix system to satisfy more than the basic reporting and data storage needs.

standard deployment

A deployment of BigFix that applies to workgroups and to enterprises with a single administrative domain. It is intended for a setting in which all Client computers have direct access to a single internal server.

statistically targeted

Pertaining to the method used to target a deployment to a device or piece of content. Statically targeted devices are selected manually by an operator.

superseded patch

A type of patch that notifies an operator when an earlier version of a patch has been replaced by a later version. This occurs when a later patch updates the same files as an earlier one. Superseded patches flag vulnerabilities that can be remediated by a later patch. A superseded patch cannot be deployed.

system power state

A definition of the overall power consumption of a system. BigFix Power Management tracks four main power states Active, Idle, Standby or Hibernation, and Power Off.

T

target

To match content with devices in a deployment, either by selecting the content for deployment, or selecting the devices to receive content.

targeting

The method used to specify the endpoints in a deployment.

task

A type of Fixlet designed for re-use, for example, to perform an ongoing maintenance task.

U

UTC

See Coordinated Universal Time *(on page 129)*.

V

virtual private network (VPN)

An extension of a company intranet over the existing framework of either a public or private network. A VPN ensures that the data that is sent between the two endpoints of its connection remains secure.

VPN

See virtual private network *(on page 138)*.

vulnerability

A security exposure in an operating system, system software, or application software component.

W

Wake-from-Standby

A mode that allows an application to turn a computer on from standby mode during predefined times, without the need for Wake on LAN.

Wake on LAN

A technology that enables a user to remotely turn on systems for off-hours maintenance. A result of the Intel-IBM Advanced Manageability Alliance and part of the Wired for Management Baseline Specification, users of this technology can remotely turn on a server and control it across the network, thus saving time on automated software installations, upgrades, disk backups, and virus scans.

WAN

See wide area network *(on page 139)*.

wide area network (WAN)

A network that provides communication services among devices in a geographic area larger than that served by a local area network (LAN) or a metropolitan area network (MAN).

Appendix C. 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.