HP BSA Essentials

For the Windows®, Linux, and Solaris operating systems

Software Version: 2.0

User Guide

Document Release Date: May 2010

Software Release Date: May 2010

Legal Notices

Warranty

The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.

Restricted Rights Legend

Confidential computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Copyright Notices

Trademark Notices

Intel® and Itanium® are trademarks of Intel Corporation in the U.S. and other countries.

Java™ is a U.S. trademark of Sun Microsystems, Inc.

Microsoft®, Windows®, Windows, XP® are U.S. registered trademarks of Microsoft Corporation.

Oracle™ is a registered trademark of Oracle Corporation and/or its affiliates. UNIX, is a registered trademark of The Open Group.

UNIX® is a registered trademark of The Open Group.

Adobe® and Acrobat® are trademarks of Adobe Systems Incorporated.

This product includes software developed by the Apache Software Foundation (http://www.apache.org/).

PDF Version of BSA Essentials 2.0 Online Help

This document is a PDF version of the BSA Essentials 2.0 online help. This PDF file is provided so you can easily print multiple topics from the help information or read the online help in PDF format.

Note: Some topics do not convert properly to PDF format. You may encounter formatting problems or unreadable text in certain document locations. Those problem topics can be successfully printed from within the online help.

Table of Contents

Welcome to BSA Essentials

Welcome to BSA Essentials 2.01, which provides both high level and detailed historical reporting on your data center's automation processes for BSA Server and Network Automation products. BSA Essentials gives you insight through a rich reporting regarding the cost effectiveness and return on investments for the various automated processed in your data center, and provides a window into the compliance state of your servers, devices, and business applications.

Supported Browsers

BSA Essentials 2.x Web Client is supported running in the following browsers.

Browser	Version
Firefox	2.x, 3.0
Windows Explorer	6.x (supported but not recommended) 7.0 (recommended)

Firefox and JRE for Reporting

If you are launching the BSA Essentials Web client on Firefox, the first time you access the reporting panel and create a new Web Intelligence Document, Firefox may not have the correct version of JRE. If you encounter a problem with this, please following the instructions listed below.

Windows
http://www.java.com/en/download/help/firefox_online_install.xml

Linux
http://www.linux-noob.com/forums/index.php?/topic/1101-how-to-install-the-java-plugin-in-firefox/

Logging In To BSA Essentials Web Client

In order to use the BSA Essentials Web Client, you need to log in to the client using a supported Web browser.

Note: To view the list of supported Web Browsers, click here.

Before logging on, make sure you have the proper user name and password for the authentication system configured to work with BSA Essentials:

- If authenticating with Active Directory (AD) or LDAP, you need to enter your BSA Essentials username and AD or LDAP password.
- If authenticating with SA, you need to enter your SA username and SA password.

To log in to the BSA Essentials Web Client, perform the following steps:

1. Enter the URL of the BSA Essentials core server in a browser. For example:

   `https://<bsae-core-hostname>:8443`

2. In the boxes presented, enter your username and password. For example:
   - **Authentication Source**: Select an external authentication source, if configured
   - **Login Name**: Enter your BSA Essentials (or AD or LDAP or SA) user name
   - **Password**: Enter your BSA Essentials (or AD or LDAP or SA) password
3. Click **Log In**.

Note: Users can log in with username "guest" (no quotes, all lower case) and no password, if the Guest user account has been enabled. For more information on the Guest user and its permissions, see "Default Users and Groups". For information on how to enable a user account, see "Suspending User Accounts".

Logging In to the BSA Essentials Client

To access BIRT reporting and to create security boundaries for data access items in the BSA Essentials Web Client, you need to log in to the BSA Essentials Client. For instructions on how to download and install, see "Installing the SAR Client "

Logging In to the BSA Essentials Client

The BSA Essentials Client Launcher allows you to log in to a BSA Essentialscore server, specifically in order to set Data Access Boundaries on reporting objects.

Before you can log in to the BSA Essentials Client, you need to download the installer from the BSA Essentials core server. For information on how to do this, see Installing the BSA Essentials Client.

Note: The BSA Essentials Client Launcher only allows you to log into aBSA Essentials 2.x core. If you attempt to log into a pre-2.x SAR core, you will get a 404 page not found Java Web Start error message and not be able to log on to the core.

Note: (Windows 2000 only) If you are running the BSA Essentials Client Launcher on Windows 2000, you may see a missing DLL error message when you log on. This error will not affect the log on procedure. To fix this so the error message does not appear, install this Microsoft update.

Log In to the BSA Essentials Client

To launch the BSA Essentials Client, perform the following steps:

1. Start the BSA Client Launcher by selecting **Start → All Programs → HP Business Service Automation → HP BSA Essentials Client**.
2. In the Log In to HP BSA Essentials Client window, enter your BSA Essentials user name, password, and the BSA Essentials server you want to log in to.

   Note: If you are using an external authentication system with BSA Essentials, such as AD, LDAP or SA, you need to append your username with that authentication system when you log in, using the following syntax:

   `username@$authsource_name`

For example, if a user named `joe_user` wanted to log in and was using `SA` as an external authentication source, the username log in would look like this:

```
joe_user@sa
```

3. Enter the BSA Essentials server's IP address or host name in the core server field, such as: https://<bsae-2-0-servername:8443>. (A port number is required. 8443 is the default port used by the BSA Essentials Web Client. If the port number has changed, consult your BSA Essentials administrator.

   If this is the first time you are logging into a specific BSA Essentials server, the launcher will download the latest version of the BSA Essentials Client when you log in. If you would like to differentiate between the SAR server you log in to and the core from which you download the latest version of the BSA Essentials Client, you can change those options by clicking **More** in the log in window and configuring your Client Host Server.

4. Click **Log In**.
5. If you are asked to accept the certificate from the core server, click **Yes**. The BSA Essentials Client now appears. For information on how to create data access permission security boundaries, see "Creating Data Access Security Boundaries".

JRE Versions and Report Authoring

For users who need to create reports in BSA Essentials, it is possible the installed version of JRE installed on your system might conflict with the JRE version required for Web Intelligence Java report panel-based report authoring feature.

Internet Explorer Users

If you are using Internet Explorer (6.x or 7.0) and you are trying to author or modify a report and the reporting panel displays an error message regarding JRE versions or in general fails to successfully load the Web Intelligence Java report panel, perform the following steps:

1. Close the report window without saving, close the Web browser and uninstall the incompatible version of JRE in your system.
2. After you uninstall JRE, launch the BSA Essentials Web Client, log in, return to the reporting features and try to edit the report as before.

Web Intelligence will prompt you to install the required version. Accept the installation and you should be able to author reports without this error once the required JRE is installed.

Firefox Users

If you are using Firefox (2.x or 3.0) and you are trying to author or modify a report and the reporting panel displays an error message regarding JRE versions or in general fails to successfully load the Web Intelligence Java report panel, go to http://java.sun.com/products/archive/j2se/6u3/index.html, select your platform, then download and install the correct version of JRE.

Support

Visit the HP Software Support Online web site at:

www.hp.com/go/hpsoftwaresupport

This web site provides contact information and details about the products, services, and support that HP Software offers.

HP Software online support provides customer self-solve capabilities. It provides a fast and efficient way to access interactive technical support tools needed to manage your business. As a valued support customer, you can benefit by using the support web site to:

- Search for knowledge documents of interest
- Submit and track support cases and enhancement requests
- Download software patches Manage support contracts
- Look up HP support contacts Review information about available services
- Enter into discussions with other software customers
- Research and register for software training

Most of the support areas require that you register as an HP Passport user and sign in. Many also require a support contract. To register for an HP Passport ID, go to:

http://h20229.www2.hp.com/passport-registration.html

To find more information about access levels, go to:

http://h20230.www2.hp.com/new_access_levels.jsp

Documentation Updates

The title page of this document contains the following identifying information:

- Software Version number, which indicates the software version.
- Document Release Date, which changes each time the document is updated.
- Software Release Date, which indicates the release date of this version of the software.

To check for recent updates or to verify that you are using the most recent edition of a document, go to:

http://h20230.www2.hp.com/selfsolve/manuals

This site requires that you register for an HP Passport and sign in. To register for an HP Passport ID, go to:

http://h20229.www2.hp.com/passport-registration.html

Or click the New users - please register link on the HP Passport login page. You will also receive updated or new editions if you subscribe to the appropriate product support service. Contact your HP sales representative for details.

Reports

BSA Essentials Web Intelligence reporting provides the ability to report on data from both Server Automation (SA) and Network Automation (NA) products. Using Cross Item Groups, and by selecting data from the SA and NA reporting universes, you can build Web Intelligence documents to define and display historical and trending information about your data center.

For other sources of data from other BSA product lines such as Storage Essentials, Operations Orchestration, and Client Automation, you can use custom SQL to write reports for those products.

For more information on creating reports, see the following topics:

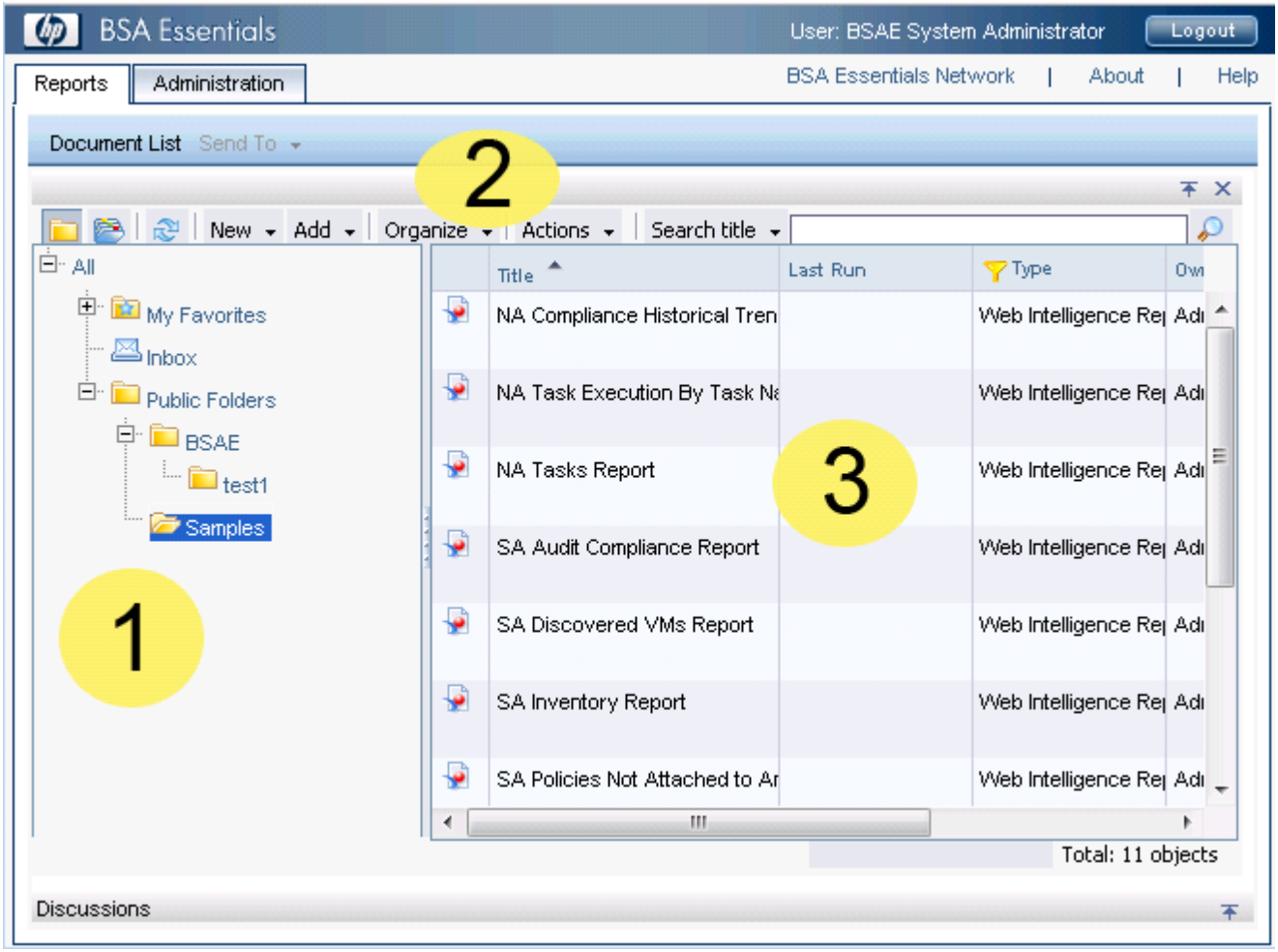
- "Reporting User Interface Document List" (on page 10)
- "Before Creating Reports" (on page 12)
- "About Web Intelligence Documents" (on page 12)
- "Web Intelligence Document Interface" (on page 13)
- "Sample Reports" (on page 14)
- "Creating a Report" (on page 15)
- "About Universes" (on page 24)
- "BSA Essentials Reporting Universes" (on page 24)

For more information on the full set of documentation for the Web Intelligence Java reporting panel, see InfoView Business Object Help.

Reporting User Interface Document List

The BSA Essentials reporting interface utilizes InfoView, a web desktop that gives you access to a broad range of useful business information about your organization. Each report that is created and saved is saved on a per user basis here. Public reports are also listed here for all users.

Details of the Reporting interface features and parts, see the "Reporting User Interface Document List" (on page 11) table below.



Reporting User Interface Document List

Feature	Description
1. Document List Folders	The Documents List folder hierarchy contains folders to store all of your Web Intelligence Documents. You can create favorites and other folders to help organize your documents and reports. You can also operate on a folder or document in the list by right-clicking a folder in order to: • Create a new Web Intelligence Document • View a folder's or document's properties. • Create a new folder.
2. Document List Toolbar	Allows you to perform several important operations, such as: • **New**: Create a New Web Intelligence Document or Folder. • **Add**: Add local documents.
3. Document List Contents	Displays the contents of a Documents List folder.

Before Creating Reports

Creating a report in BSA Essentials requires that the following tasks have already been performed:

- **Configure User Groups and Permissions**: Make sure that users and user groups have been created that possess the proper permissions to create reports. For more information, see "Creating User Groups" and "Creating User Accounts" and "Assigning Permissions to Groups".
- **Create Security Boundaries**: (Optional) Create BSA Essentials security boundaries to limit the types of information you can use to build reports from. For more information, see "Creating Security Boundaries"
- **Create Cross Item Groups**: (Optional) Create Cross Item Groups (CIGs) if you would like to restrict the types of data you build your reports from. For more information, see "Configuring Cross Device, Policy, and Job Groups".

Note: These tasks are typically performed by an administrative user.

For specific JRE requirements related to report authoring, see "JRE Versions and Report Authoring" (on page 8).

About Web Intelligence Documents

BSA Essentials utilizes SAP BusinessObjects Web Intelligence Documents (WID) to allow you to build reports based upon data selected from your universes, save the document, print it, and share it with other users in your organization.

Designing Reports with Web Intelligence Documents

The Web Intelligence document is not just the report result itself, but rather defines, through queries filters and data objects, the exact kinds of data you want to retrieve from the SA or NA databases over a specified period of time (or, a specific snapshot in time). The document also contains all the necessary formatting and configuration details to enable your reports to display the information meaningfully.

Sharing Web Intelligence Documents

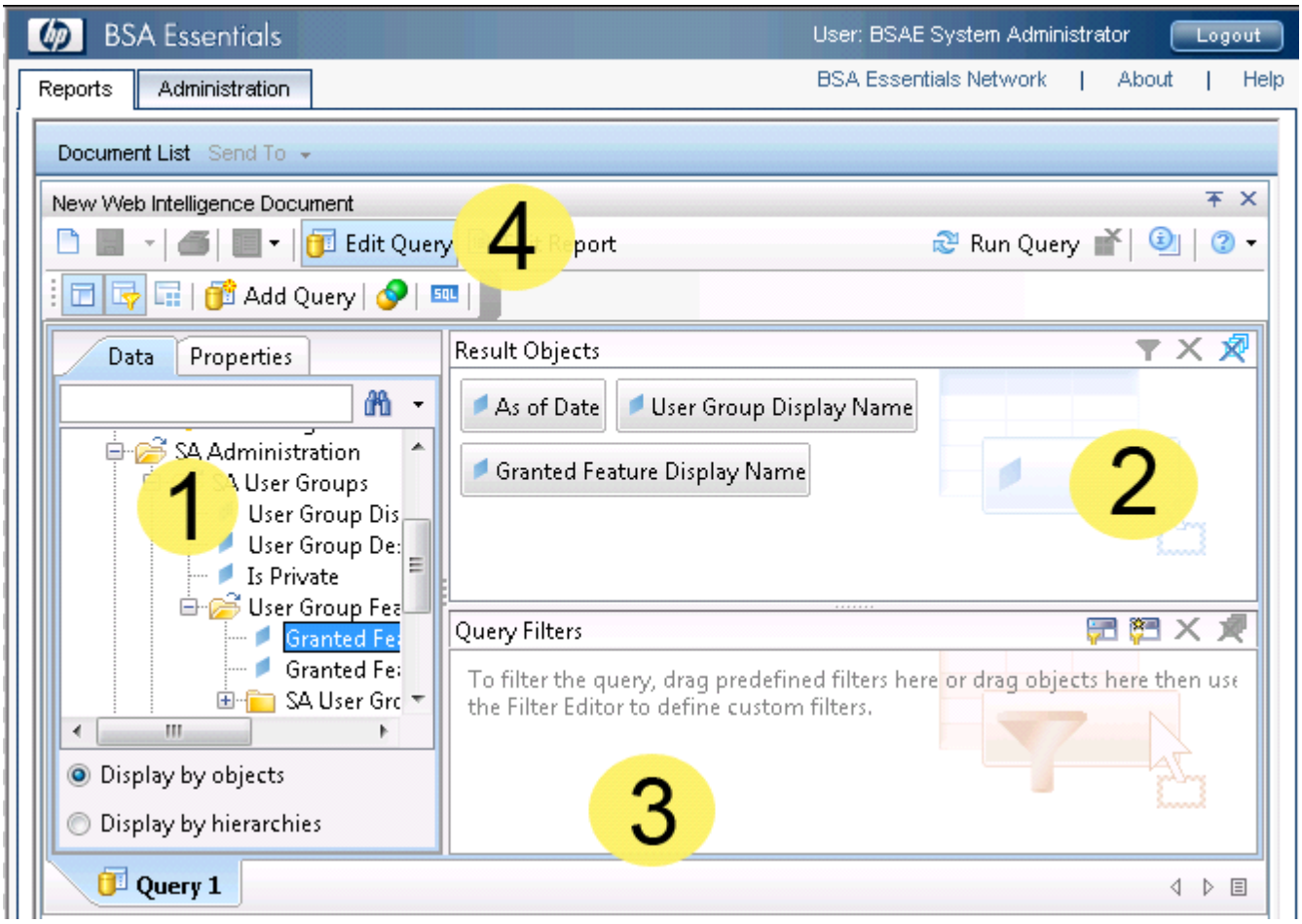
With Web Intelligence Documents, you can share reporting information in the following ways:

- You can save your documents as public documents and send them directly to your colleagues via email. Public Web Intelligence documents are visible in the main InfoView reporting panel, in the document list folder hierarchy.
- You can share Web Intelligence documents with non-InfoView users by saving your reports in Microsoft Excel, Adobe PDF, and Web Intelligence documents. You can send them to your colleagues as email attachments for your colleagues to view and print.

For more information, consult the Web Intelligence online help.

Web Intelligence Document Interface

The Web Intelligence Document is the graphical user interface for creating and building report queries. The main features of the interface are shown in the following diagram and "Web Intelligence Document Interface" (on page 14).



Web Intelligence Document Interface

Feature	Description
1. Universe Browser	This pane lists all of the universe's classes and objects. To build the report query, drag and drop universe objects (or entire classes) to this pane to define the elements of your report. A universe can contain more than one query by clicking Add Query.
2. Results Objects	This panel allows you select objects from the universe browser Data tab and drag them here.
3. Query Filters	This pane is where you can drag and drop query filters to limit the results of the repot by setting run-time options, filtering on users, groups, machine types, and so on. Typically, this pane is used for setting a date ranger filter to set the time frame of the report results.
4. Toolbar	Contains toolbar functions for the Web Intelligence Document, such as: • **Add Query**: Add another query to the document.. This allows you to select objects from another universe. • **Edit Report**: Allows you to edit the visual display of the report results. • **SQL**: Allows you to view and edit the SQL layer of the query. • **Run Query**: Runs the document query and produces report results.

Sample Reports

BSA Essentials provides several sample reports that illustrate the kinds of data and historical information a BSA Essentials reports can display.

Sample reports are located in the Reports tab in the main document list, under Public Folders → Samples.

NA Sample Report

Network Automation (NA) Sample Reports	Description
NA Compliance Historical Trending Report	Displays the trend of network device non-compliance over time. A device is considered non-compliant when the device configuration does not match the configuration defined in the compliance policy attached to the device.
NA Task Execution by Task Name	Displays NA tasks executed over a specific range of time, run on Nan A device group Inventory.
NA Tasks Report	Displays NA task status distribution.

SA Sample Reports

Server Automation Sample Reports	Description
SA Audit Compliance Report	Shows compliance statuses for servers in a device group with audits attached to them , plus a breakdown of each audit's details.
SA Discovered VMs Report	Displays all the virtual machines (VMs) discovered by SA through their respective hypervisors. VMs can include VMware VMs, Solaris local zones, and Microsoft Hyper-V VMs.
SA Inventory Report	Reports on servers under management and their inventory details within SA for a given time range.
SA Policies Not Attached To Any Server	Displays a list of SA policies that are not attached to any servers, but excluding audits. SA policies can include software policies, patch policies (Windows-only), and application configurations.
Servers Without Policies	Shows the managed servers that do not have any policies attached.
SA Trending of Unmanaged And Managed VMs Report	Shows the trend over time of managed and unmanaged virtual machines in SA. Server Automation discovers these VMs and their state through their respective hypervisors.
SA User Permissions Report	Lists feature permissions grouped by user name, including the total number of permissions for each user.
Server & Network Cross Device Group Inventory Report	This report shows the servers and network devices under management and their inventory details within a Cross Device Group that includes devices managed by both Server Automation and Network Automation.

Creating a Report

The basic workflow for creating a report consists of the following tasks. In this example, you learn how to create a Web Intelligence Document and build a basic query to report to display all Server Automation private user group feature permissions.

1. Create a Web Intelligence Document

In order to create a report, you need to first create a Web Intelligence Document from the Reporting panel. The Web Intelligence document allows you to select a universe, build data queries using filters and universe objects, and all other formatting information to create a interesting and meaningful report.

To create a Web Intelligence Document, perform the following steps:

1. Select the Reports tab in the BSA Essentials Web Client. You see the Web Intelligence Java reporting panel.
2. From the **New** menu click **New Web Intelligence Document**.

2. Select a Universe

A BusinessObject universe is the interfacing layer between a client (BSA Essentials Web client) and a database (SA or NA). The BSA Essentials universes hides the typical database structure and makes database objects intelligible and accessible, so you can build meaningful reports.

To select a universe, perform the following steps:

1. After you have created a Web Intelligence Document, in the Web Intelligence Document → New Document Window you see a list of possible universes to choose from; SA General, SA Compliance, and NA General. To continue, select the SA General Universe. (For more information, see "BSA Essentials Reporting Universes" (on page 24))
2. After you select the SA General Universe, the Web Intelligence Document interface appears, showing you all the objects available from the selected universe. (For more information about the Web Intelligence Document user interface, see ""Web Intelligence Document Interface" (on page 13)".)

3. Build the Report Query

Building a report query enables you to specify the types of objects you want to report on from the universe. For example, you might want to create a report that displays all private SA user groups in and their feature permissions.

In this task, you will choose objects from the SA universe.

To build the report query, perform the following steps:

1. From the Universe browser on the left side of the Web Intelligence Document window, select the objects you want to report on.
2. For example, if you wanted to report on all of the SA user groups and their feature permissions, you would select the SA Administration → SA User Groups → User Groups → User Group Display Name object and drag it to the Results Object pane.
3. Select the Is Private object and drag it into the Query Filter pane.
4. Select the Is Private object you just dragged into the Query Filter pane, and using the In List drop-down, select Equals.
5. In the text field, type Yes.
6. Next, from the same folder, expand the User Group Features and drag and drop the Granted Feature Display Name object to the Results Objects pane,
7. Then, expand the SA User Group Features Advanced folder, and select the Granted Feature Name object and drag it into the Results Objects pane.
8. Last, at the root of the SA General Universe, expand the General folder and drag the Single Date Filter and drag this object to the Query Filters pane on the bottom of the window. This query filter object allows you to specify a single date in history that you want to report on.

For more information on universe object descriptions, see "BSA Essentials Reporting Universes" (on page 24).)

4. Run the Report Query

Next, to generate report results you will run the query.

To run the query, perform the following steps:

1. From the upper right of the Web Intelligence Document window, click the **Run Query** on the document toolbar.
2. Since you selected a Single Date filter, you need to specify a date on which you want to base the report. From the Prompts dialog, click the Select a Custom Date button to choose a date.
3. Click **Run Query**. When the query has finished running, the report results display in the Web Intelligence Document window.

5. Save the Web Intelligence Document

Once you have built the query and run the report, you need to save the Web Intelligence Document. You can also save the document to your local computer as Excel, PDF, or CSV.

To save the Web Intelligence Document, perform the following steps:

1. From the Web intelligence Document toolbar, click **Save**. The Save Document dialog box appears.
2. To save the report on the BSA Essentials Server, select either My Favorites so only you can view it (private) or select a Public folder so others on your team can access the report.
3. To save the report results to your local computer, from the Document menu, select Save to my computer as → Excel, PDF, CSV or CSV with Options.

Enabling Actionability in BIRT Reports

The BSA EssentialsClient reports can support actionable items. For example, a server entry in a report can be set as actionable. Right-clicking on that server displays a pop-up menu of actions available for that server.

Setting a Table as Actionable

To set a table as actionable, perform the following steps:

1. Launch BIRT RCP Designer.
>
2. In the Outline pane, expand the report name, and then expand Body.
3. Select the table name.
4. In the Property Editor -table name, click the Properties tab.
5. In the Properties list, select Bookmark.
6. In the text field, enter the following string:

   ```
   id=''actionable''
   ```
7. From the File menu, select Save.

Adding Source and Item IDs to a Custom Report

To add the source and item id to your custom report, perform the following steps:

1. Launch BIRT RCP Designer.
2. Expand Data Set.
3. Double-click the data set that is associated with the report.
4. In the query text field, add an actionable text string. See for the acceptable formats and values.
5. In the left list of the Edit Data Set window, click Output Columns.
6. Click OK.
7. Expand the Data Set.
8. Drag the new column into the table as the first column of the Detail Row of the table.
9. BSA Essentials Actionable Item Formatting

10. The format for BSA Essentials actionable report items is:

    `ci_type:item_id`

    For example:

    `SAS_SERVER:1001`

    where `SAS_SERVER` is the CI Type and 1001 is the item id of the specific item. The item id is a numeric value unique to your BSA Essentials installation. All CI Types have actionability supported for the View action, and other actions may also be supported dependent on the CI Type. For a list of valid CI Types in BSA Essentials, seethe next task, Viewing CI Types.

Viewing CI Types

To see a list of valid CI Types, perform the following steps:

1. In a web browser, enter the following URL:

   `https://omdbserver:8443/catalog/`

   where `omdbserver` is a BSA Essentials server that you have an account you can log in to.
2. Click ListItem Types. The CI Types are shown in the "Type Name" column.

Scheduling Reports

This topic shows you how to schedule a report. Scheduling is a process which allows you to run a report object automatically at specified times. When you schedule an object, you choose the recurrence pattern that you want and specify additional parameters to control exactly when and how often the object will be run.

Scheduling Reports

1. Select a report.
2. Click Actions → Schedule. The "Schedule" dialog box appears, showing the default settings for the object.
3. Enter an appropriate instance title.
4. Click Recurrence and select the recurrence pattern you want. For example, select Weekly.
5. Specify the Run option and parameters that you want. For example, select Weekly and then specify Monday, Wednesday, and Friday.
6. Click Formats and Destinations and set Output Format and Destination Options (email recipients).
7. Set any of the other schedule options and parameters as required.
8. Click Schedule. The system will create a scheduled instance and run it according to the schedule information you specified. You can view the scheduled instance on the "History" page for the object.

Enabling Actionability of OO Flows for BIRT Reports

To enable HP Operations Orchestration (OO) actions on objects for BIRT reports in theBSA Essentials Client, the BSA Essentials Administrator must add an existing OO Flow to BSA Essentials by defining the

for BSA Essentials in the BSA Essentials configuration file `pas_actions.xml`, located in the `/opt/opsware/omdb/deploy/birt.war/` directory.

Note: The tasks shown in this chapter were created using version 7.0 of PAS. Refer to the documentation for your version of PAS or OO to identify Flow variables such as Flow name, Flow ID, and target names of inputs.

To add an OO Flow to BSA Essentials, you need to know the following information:

- the OO Flow Name
- the OO Flow ID
- the BSA Essentials CI Type the OO Flow is associated with
- the Target Name and the Source Name of each input that BSA Essentials should pass to the OO Flow

For example, to configure a OO flow with an input named "host" to run on an SA Server and to pass that server's IP address to OO, you must:

- Identify the appropriate input name of the OO Flow
- Configure the following elements of the BSA Essentials `pas_actions.xml` file:
  - `<ci-type name="SAS_SERVER">`
  - `<source-name>opsware.sa.PrimaryIp</source-name>`
  - `<target-name>host</target-name>`

For more information on working with the BSA Essentials pas_actions.xml file, see "Adding an OO Flow to BSA Essentials" (on page 21) and "Example CI-Type and Flow Elements in pas_actions.xml" (on page 22).

Identify the ci-type name and source-name values using the BSA Essentials Data Catalog. For more information, see Identifying the CI Type and Identifying the Source Name of an OO Flow Input.

To identify the target-name value, find the name of the input for the OO Flow you want to configure to run from BSA Essentials. For example, an OO flow might have a flow variable named "host," with a value of "${host}". Using the example pas_actions.xml tokens, BSA Essentials would pass the value of a SAS_SERVER's IP address as a variable with the name of "host" to the OO server for use in its workflow, as part of the remote flow execution call. For more information, see "Inputs: Providing data to operations" in the OO Author's Guide.

The following tasks show how to gather the required information, and then how to add the OO Flow definition to BSA Essentials:

Identifying the OO Flow Name

This tasks show you how to identify the OO flow name so you can add accountability to your flows inside of BSA Essentials.

Note: You must use the name of the Flow shown in OO as the Flow Name in the file `pas_actions.xml`.

To find the name of a Flow, perform the following steps:

1. Using the OO Central web-based application, log into the OO server where the OO Flow is installed.
2. Select the Flow Library tab.
3. View the folder tree of the Flow Library until you find the name of the OO Flow you want to add to BSA Essentials.
4. Right-click the selected Flow, then select About. The Flow Information window is displayed. The name of the OO Flow is displayed as the top line of text in the window.

Tip: See “Finding an Ops Flow” in the OO Central Users’ Guide for more information.

Identifying OO Flow ID

An example of a Flow ID resembles the `following` text string:

```
13adf024-c87f-46ef-b734-c8d6ad21c8ba
```

To identify the Flow ID of the OO Flow you are working with, perform the following steps:

1. Using the OO Central web-based application, log into the OO server that the OO Flow is on.
2. Select the Flow Library tab.
3. Right-click the selected Flow, then select **About**. The Flow Information window is displayed. The Flow UUID is displayed in the Flow Information window.

Identifying the CI Type

To see a list of valid CI Types in BSA Essentials, perform the following steps:

1. In a web browser, enter the following URL:

   ```
   https://omdbserver:8443/catalog/
   ```

   where omdbserver is a BSA Essentials server that you have an account you can log in to.
2. Click ListItem Types. The CI Types are shown in the "Type Name" column.

Identifying Target Name of an OO Flow Input

Each input for a OO Flow needs to be defined in pas_actions.xml with both a Source Name and a Target Name. The Target Name is the parameter name used by the OO server when a flow is defined.

Examining the design of a flow using the OO Studio can help in understanding a flow’s inputs and the data types expected for a given input.

To view the list of target-names to use as inputs for an OO Flow, perform the following steps:

1. Using the PAS Central web-based application, log into the OO server that the OO Flow is present on.
2. Select the Flow Library tab.
3. Right-click the selected Flow, then select Guided Run.
4. In the Advanced Details pane, choose the appropriate Input name as the text string you will use as the target name.

Note: The above task was created using version 7.0 of PAS. Refer to the documentation for your version of PAS or OO to identify flow variables.

Identifying Source Name for an OO Flow Input

Each input for a OO Flow needs to be defined in pas_actions.xml with both a Source Name and a Target Name. The Source Name is created from the definition of an attribute of a CI Type in the BSA Essentials Data Catalog.

To identify the source name of a OO Flow input, perform the following steps:

1. In a web browser, enter the following URL:

   `https://omdbserver:8443/catalog/`

   where omdbserver is the BSA Essentials server that you have an account you can log in to.
2. Click ShowFullCatalog. The CI Types are shown in alphabetic order.
3. Find the CI Type you are working with.
4. Find the attribute you want to use. Read the attribute's value in the Attribute Namespace column. We will refer to this value as `attribute_namespace`.
5. Find the attribute's value shown in the Attribute Key column. We will refer to this value as `attribute_key`.
6. Assemble the source name by writing the `attribute_namespace`, a period (.), and then the `attribute_key`. For example, the assembled source name would be in the following format: `attribute_namespace.attribute_key`.

Adding an OO Flow to BSA Essentials

Now that you have gathered the required information, you can add the OO Flow to BSA Essentials.

1. On the BSA Essentials Core server, open a terminal window.
2. Copy the following file:

   `/opt/opsware/omdb/deploy/birt.war/pas_actions.xml`

   to

   `/opt/opsware/omdb/deploy/birt.war/pas_actions_backup.xml`

   `pas_actions.xml` is a file included with BSA Essentials that provides example Configuration Item (CI) types and PAS workflows.
3. Using a text editor, open the following file:

   /opt/opsware/omdb/deploy/birt.war/pas_actions.xml

4. Perform one of the following two actions:

   If the CI Type you are adding a flow for does not already exist in the pas_actions.xml file, add a new CI Type element for the CI Type you want to add the PAS Flow to. Go to step 5.

   Or

   If the CI Type you are adding a flow for does already exist in the pas_actions.xml file, modify the existing matching CI Type element of the file to match your desired Flow ID, Flow Name, source name, and target name, and then go to step 10.
5. Copy a Flow element from <flow> to </flow>, and paste the flow element between the last </flow> and the </ci-type> closing tag for the CI Type.
6. In the copied Flow element, edit the value of <flow id="flow_id"> by replacing flow_id with the Flow ID you identified in Identifying the Flow ID.
7. In the copied Flow element, edit the value of <flow-name>flow_name</flow-name> by replacing flow_name with the OO Flow Name you identified in Identifying the Flow Name.
8. In the <input> tag of the copied Flow element, edit the value between the <source-name> and </source-name> tags with the attribute_namespace.attribute_key value you identified in Identifying the Source Name of an OO Flow Input.
9. In the <input> tag of the copied Flow element, edit the value in <target-name> and </target-name> tags with the value you identified in Identifying the Target Name of an OO Flow Input.
10. Delete the example data for the example flows in the pas_actions.xml file.
11. Save your changes to pas_actions.xml, and then exit the text editor.
12. (Optional) Before restarting the BSA Essentials Core, check the validity and structure of the pas_actions.xml file using a tool such as the UNIX utility xmlwf.
13. Restart the BSA Essentials Core. See Starting and Stopping SAR for more information.

Example CI-Type and Flow Elements in pas_actions.xml

The following example text shows one CI-Type element containing two Flow elements. This example text is not a complete pas_actions.xml file.

```
<ci-type name="CI_TYPE">

<!-- SMTP check: flow1_id -->

<flow id="flow1_id">

<flow-name>flow1_name</flow-name>

<inputs>

<input>

<!-- input names should be valid attributes of the CI type -->

<!-- The attribute's value should be passed as an input to the

PAS workflow.-->

<source-name>flow1_source_name1</source-name>

<target-name>flow1_target_name1</target-name>
```

```
</input>
<input>
<source-name>flow1_source_name2</source-name>
<target-name>flow1_target_name2</target-name>
</input>
</inputs>
</flow>
<flow id="flow2_id">
<flow-name>flow2_name</flow-name>
<inputs>
<input>
<source-name>flow2_source_name1</source-name>
<target-name>flow2_target_name1</target-name>
</input>
<input>
<source-name>flow2_source_name2</source-name>
<target-name>flow2_target_name2</target-name>
</input>
</inputs>
</flow>
</ci-type>
```

The <filter> and <multi-select> elements are not supported in earlier versions of BSA Essentials, speci

BSA Essentials Reporting Universes

BSA Essentials leverages SAP BusinessObjects (BO) reporting technology to enable cross-product historical reporting. One essential component of utilizing BO technologies are the reporting "universes," which determine the kinds of objects you can report upon from the different BSA products (SA and NA).

A reporting universe is the interfacing layer between a client and a database. The universe defines the relationship among the various database tables and visualizes how the tables in a database are connected. BSA Essentials uses information filtered through the universes to create an SQL query based on the "objects" you choose in your report designer when you create a Web intelligence document.

Each universe also contains generic report query filters such as date range filters,which help specify a time frame on which to base the report. Each universe contains access to any Cross Item Groups for Jobs, Policies, and Devices that have been created on your BSA Essentials core. For example, you can select a Cross Device Group containing SA servers in order to add them to your report.

For more information on creating Cross Item Groups, see "Configuring Cross Item Groups".

BSA Essentials 2.xprovides three universes from which to create your reports:

- **"SA General Universe" (on page 27)**: Provides data items for all general areas of Server Automation, such as information about servers (hostname, IP, name, OS), SA Library items such as Software Policies, Audits, APXs, software packages, OS installation profiles, SA Job, and more.
- **"SA Compliance Universe" (on page 38)**: Contains everything related to SA compliance policies for your reports, such as Audits, Audit Policies Software Policies, Application Configurations, and Windows Patch Policies, and how each of these relate to servers. For example, the SA Compliance universe allows you to select filters so you can create a report that shows over time, how many of the policies attached to the server are in compliance.
- **"NA General Universe" (on page 52)**: Enables you to created reports based on NA data, such as device types and detailed device attributes and metadata (asset details, configuration details, port details, and so on), device groups, compliance information, tasks, event, users, and diagnostics.

About Universes

A BusinessObject universe is the interfacing layer between a client (BSA Essentials Web client) and a database (SA or NA). The universe defines the relationship among the various tables in the database.

A universe is extremely useful for creating reports because it hides the typical database structure and makes database objects intelligible and accessible, so you can build meaningful reports.

The BSA Essentials universes - SA General, SA Compliance, and NA General - organize reporting objects extracted from the SA and NA database(s) into relevant and understandable categories. When you create a Web Intelligence document to design a report, you select a universe to query the SA or NA database where the data that interests you is stored.

A universe contains three basic elements:

Class

A class is a logical grouping of related objects. Web Intelligence represents a class with a folder  icon

Objects are grouped into folders called classes, each of which can also contain one or more subclasses. Subclasses contain objects that are a further subcategory of the objects in the upper level of the class.

When you create queries on a universe, classes help you to find the objects that represent the information that you want to use in a query.

For example, in the SA General Universe, you might want to create a report that displays all the feature permissions granted to a specific public user group.

The SA General Universe organizes this information in the following class hierarchy:

SA Administration → SA User Groups → User Group Features → SA User Group Features Advanced.

Object

An object is an element in a universe that maps to a specific set of data in your SA or NA database. Each object in a universe is defined with a business term that your organization uses commonly, such as Server, Device, Customer, Compliance Policy, User or Device Group, and so on.

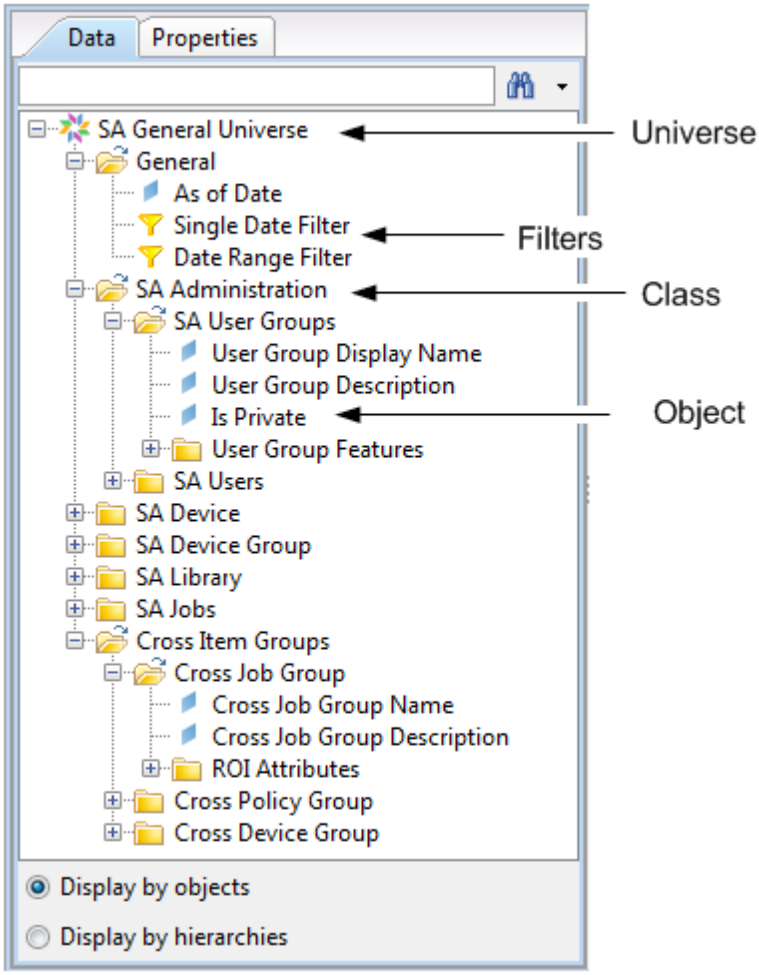
Key types of universe objects used in reporting include:

- **Dimension** Retrieves the data that provides the basis for analysis in a report. Dimension objects typically retrieve character-type data. For example, for an SA server, the SA general universe contains dimensions such as Server Name, Host Name, OS name, server model, and so on.
- **Measure** : Retrieves numeric data that result from calculations on the data in the database. For example, the Cross Job Group "Cross Job Group Total ROI" measure allows the report to indicate the value you are getting from the jobs being run by the BSA software suite.

Query Filter

A query filter is a type of object allows you to restrict the data returned by an object in a query, and is represented with a yellow funnel icon. In the SA universe, for example, such common predefined query filters include Single Date Filter and Date Range Filter, so you can select the time frame for the report.

The SA General Universe hierarchy is shown below.



SA Universes: Compliance vs General

Before you start creating reports based on Server Automation Data, using either the SA General or Compliance Universes, consider the following:

- SA Compliance Universe must be employed to build any BusinessObjects queries and reports that report on SA policy compliance - either current or historical - and policy attachment relationships to SA servers or SA device groups.
- SA General Universe is designed to cater to all other reporting SA reporting use cases - including inventory, virtualization and ROI.

Note: BSA Essentials updates SA Compliance Universe information via a nightly job and thus you may see unexpected latency in SA Compliance Universe information if your reporting frequency is more than the frequency at which the nightly job refreshes the SA Compliance Universe. For information on how to change the nightly job run frequency, refer to the BSA Essentials 2.0 Administrator's Guide.

SA General Universe

The SA general universe defines a typical set of SA objects and their attributes and allows you to report on them. For example, the SA General universe defines servers and all related information about servers, such as name, hostname, OS, primary IP address and so on.

Additionally, the SA general universe contains generic query filters and Cross Item Group objects so you can limit your report results to specific device groups, job groups, and user groups from SA.

The following tables describe the contents of the SA general universe:

General

Object	Description
As of Date	Date associated with a row record, e.g. as of 4/10/2009, device r144 compliant state was Non-Compliant. Include this if you want the date corresponding to each row in the report. In any historical or trending report, you must include As Of Date in the Result Objects for your report or the data will not display properly. (Note: The As of Date universe object can only be used as a Result Object and cannot be used as a filter.)
Single Date Filter	Use the Single Date Filter to specify a single date in history where you want to report on an object from the Device, Device Group, Administration and Library objects. Do not use this filter with the SA Jobs objects.
Date Range Filter	Use the Date Range Filter to specify the historical date range you want to report on for the Device, Device Group, Administration and Library objects. Do not use this filter with the SA Jobs objects. The Date Range Filter is most useful when you want to create trending reports. When using the Date Range Filter, it is recommended that you include the As Of Date element in the Result Objects panel.

SA Administration

Object	Description
SA User Groups	All User Group reporting objects.
User Group Name	The name of the User Group.
User Group Description	The description of the User Group.
Is Private	Is Private refers to the Private User Group, which gets created automatically every time a user is created in HP SA. Use this to dimension to filter out private User Groups from your overall reports. In general, Private User Groups will not be of interest. The possible values are Y and N. Y means it is a Private User Group. N means it is not a Private User Group.
SA User Groups Advanced Attributes	Advanced User Group reporting objects. (These should not be necessary in most reports.)
Is Admin	Is Admin refers to the Super Admin privilege which allows a User Group to manage user permissions. The possible values are N and Y. Y means the User Group has Super Admin privileges and can manage user permissions. N means the User Group does not have Super Admin privileges.

Object	Description
User Group Features	The User Group Features allow you to report on what SA actions members of the user group can take.
Granted Feature Display Name	This is the name of the Granted Feature. Note that these names will not be the same as the names presented in the SA Client.
Granted Feature Category	This identifies where the Granted Features are found in the SA Client. There are several tabs of permissions in the SA UI and this object reports the specific tab this Granted Feature is found on.
SA User Group Features Advanced Attributes	
Granted Feature Name	This is the internal name for the Granted Feature. You should not typically need to use this object.
Granted Feature Is Deprecated	This identifies those Granted Features which are now deprecated. Use this to identify which permissions you may want to remove after an upgrade.
Granted Feature Description	This is the Granted Feature description which describes the feature. This field is not currently implemented in SA.
SA Users	All User reporting objects.
User Status	The status of the User. This dimension has 3 possible values: active, deleted and suspended.
Username	The login name for this user.
Full Name	The full name for this user.
Email Address	The registered email address for this user.

SA Device

Object	Description
Server Name	The name of the server as displayed in the SA User Interface.
Host Name	Server name as reported by the command uname or the computer name.
Serial Number	The serial number of the server as displayed in the SA User Interface.
Reported OS	The operating system for the server, as reported by the SA agent.

Object	Description
OS Name	The attached OS role class. This is a less descriptive name than Reported OS.
Server Model	The model number of the server.
Server Manufacturer	The name of the hardware vendor.
Primary IP Address	The primary IP Address for this server.
Primary Mac Address	The MAC address associated with the primary IP Address for this server.
Server Type	The type of server. This dimension has 3 possible values: physical, virtual machine or hypervisor.
Customer Name	The HP Server Automation Customer the server belongs to.
Facility Name	The HP Server Automation Facility the server belongs to.
Custom Attribute Name	The HP SA Custom Attribute Name. This is most often paired with the Custom Attribute Value.
Custom Attribute Value	The HP SA Custom Attribute Value. BSA Essentials only stores the first 4000 characters of the data.
Last Agent Report	The date the SA Agent last made a report to the SA server.
Agent Version	The version of the agent running on the server.
Attached Application Configuration	All reporting objects related to application configurations which are attached to servers. Objects in this folder must be paired with server or device group entities.
AppConfig Name	The name of the Attached Application Configuration attached to the server, as seen in the SA Client. This element must be paired with a server or device group dimension when used in reports.
AppConfig Description	The description of the Attached Application Configuration. This element must be paired with Application Configuration Name and a server or device group attribute when used in reports.
AppConfig Version	The version of the Attached Application Configuration. This element must be paired with Application Configuration Name and a server or device group attribute when used in reports.
AppConfig Modified By	The user who modified the Attached Application Configuration. This element must be paired with Application Configuration Name and a server or device group attribute when used in reports.
AppConfig Modify Date	The date the Attached Application Configuration was modified. This element must be paired with Application Configuration Name and a server or device group attribute when used in reports.

Object	Description
Attached Patch Policy	All reporting objects related to patch policies which are attached to servers. Objects in this folder must be paired with server or device group elements. To report on server compliance with patch policies, use the SA Compliance Universe.
Patch Policy Name	The Patch Policy name applied to the server. This element must be paired with a server or device group attribute when used in reports. To report on server compliance with this patch policy, use the SA Compliance Universe.
Patch Policy Description	The description of the Patch policy. This element must be paired with a server or device group attribute when used in reports. To report on server compliance with this patch policy, use the SA Compliance Universe.
Attached Software Policy	
Software Policy Name	The Attached Software Policy name applied to the server. This element must be paired with a server or device group dimension when used in reports. To report on server compliance with this software policy, use the SA Compliance Universe.
Software Policy Description	The description of the Attached Software Policy. This element must be paired with Attached Software Policy Name and a server or device group attribute when used in reports. To report on server compliance with this software policy, use the SA Compliance Universe.
Inventory	
Disks	All reporting objects related to the Disks as reported by servers. Elements in this folder must be paired with a server or device group dimension when used in reports.
Model	The device model as reported by the server. This element must be paired with a server or device group attribute when used in reports.
Media	The device media as reported by the server. Typical values are SCSI Disk, CDROM, etc. This element must be paired with a server or device group attribute when used in reports.
Manufacturer	The manufacturer of the disk, such as SEAGATE. This element must be paired with a server or device group attribute when used in reports.
Device	This is the disk "device" as reported by the server. Typical values are volumes, partitions and drives. This element must be paired with a server or device group attribute when used in reports.
Capacity (MB)	The size of the disk, in MB. This element must be paired with a server or device group attribute when used in reports.
Hardware	All reporting objects related to the system hardware as reported by the server. Elements in this folder must be paired with a server or device group dimension when used in reports.
Number of CPUs	The number of CPUs for the server. This element must be paired with a server or device group attribute when used in reports.
Memory: RAM	The RAM for this server. This element must be paired with a server or device group attrib-

Object	Description
(MB)	ute when used in reports.
Memory: SWAP (MB)	The SWAP space for this server. This element must be paired with a server or device group attribute when used in reports.
CPU Model	The model of the CPU. This element must be paired with a server or device group attribute when used in reports.
Network	All reporting objects related to the network interfaces as reported by the server. These will report on all network interfaces on the server. Elements in this folder must be paired with a server or device group dimension when used in reports.
Interface Mac Address	The MAC Address of the specific interface. This element must be paired with a server attribute when used in reports.
Interface IP Address	The IP Address of the specific interface. This element must be paired with a server attribute when used in reports.
Interface	The name of the interface. This element must be paired with a server attribute when used in reports.
Host Name	The hostname as reported by the interface. This element must be paired with a server attribute when used in reports.
Connected Port Name	The port name of the network device this server is attached to. This element only works when Network Automation integration is enabled. This element must be paired with a server attribute when used in reports.
Installed Packages	All reporting objects related to the packages installed on the server. Objects in this folder must be paired with server or device group elements.
Installed Package File Name	The file name of the installed package. This element must be paired with a server or device group attribute when used in reports.
Installed Package Name	The name of the installed package. This element must be paired with a server or device group attribute when used in reports.
Installed Package Version	The file version of the installed package. This element must be paired with a server or device group attribute when used in reports.
Installed Package Type Name	The type of the installed package. Examples include Zip, Windows MSI, etc. This element must be paired with a server or device group attribute when used in reports.
Installed Package Platform Name	The platform for which this package is targeted.
Installed Patches	All reporting objects related to the patches installed on the server. Objects in this folder must be paired with server or device group elements.
Installed Patch Name	The name of the installed patch. This element must be paired with a server or device group attribute when used in reports.

Object	Description
Installed Patch Description	The installed patch description. This element must be paired with a server or device group attribute when used in reports.
Installed Patch Type	The type of the installed patch. Examples include Windows Update Rollup, Windows Hotfix, etc. This element must be paired with a server or device group attribute when used in reports.
Installed Patch Platform Name	The platform for which this patch is targeted.
Virtualization	All reporting objects related to virtualization.
Hypervisor Attributes	All reporting objects related to managed Hypervisors.
Hosting Hypervisor Reported OS	The operating system for the hypervisor, as reported by the SA agent.
Hosting Hypervisor Primary IP	The primary IP Address of hosting hypervisor
Hosting Hypervisor Host Name	Hosting Hypervisor hostname reported by the computer
Hosting Hypervisor Display Name	The name of the Hosting Hypervisor as displayed in the SA User Interface.
Discovered Virtual Machine Attributes	All reporting objects related to virtual machines discovered via their hypervisors.
Virtual Server Description	This is the virtual machine description as discovered through its hypervisor
Virtual Server Name	This is the virtual machine's name as discovered through its Hypervisor. This is typically the user supplied name.
Virtual Server Status	This is the virtual machine's power state as discovered through its Hypervisor. Typical values are Powered On, Suspended, Powered Off.
Virtualization Type	This is the virtualization type, such as VMware VM or Solaris 10 Container, as discovered through its Hypervisor.
Hypervisor Measures	
Guests Not Under Man-	The VMs discovered, but not managed by Server Automation

Object	Description
agement	
Managed Guests	The VMs discovered and managed by Server Automation
Total Guests	The total VMs discovered from the hypervisor
Server Advanced Attributes	
Server Identifier	Use this to filter query results based on the name of a server
Management IP Address	The IP address that HP Server Automation uses to communicate with the Server Agent on the managed server.This object thus is meaningful only when paired with a managed server.

SA Device Group

Object	Description
SA Device Group	All reporting objects related to SA Device Groups
Display Name	The device group name as displayed in the SA Client.
Group Owner	The owner of the device group.
Group Name	The internal device group name.
Device Group Single Date Filter	Use the Single Date Filter to specify a single date in history where you want to report on an object from the Device Group.
Device Group Date Range Filter	Use the Date Range Filter to specify the historical date range you want to report on for the Device Group. The Date Range Filter is most useful when you want to create trending reports. When using the Date Range Filter, it is recommended that you include the As Of Date element in the Result Objects panel.

SA Library

Object	Description
SA Library	All reporting objects related to the SA Library. The Dimensions in this folder are meant to be used with other dimensions in the SA Library folder. You cannot use these dimensions with any dimensions from the SA Device folder.

Object	Description
Application Configuration	All reporting objects related to the Application Configurations stored in the SA Library. The Dimensions in this folder are meant to be used with other dimensions int he SA Library folder. You cannot use these dimensions with the device attributes.
AppConfig Name	The name of the Application Configuration as displayed in the SA Client.
AppConfig Description	The user who modified the Application Configuration.
AppConfig Modified By User	The description of the Application Configuration as displayed in the SA Client.
AppConfig Last Modified Date	The date the Application Configuration was modified.
APXs	All reporting objects related to the Application Extensions stored in the SA Library. The Dimensions in this folder are meant to be used with other dimensions in the SA Library folder. You cannot use these dimensions with the device attributes.
Extension Display Name	The APX display name as seen in the SA client.
Extension Internal Name	This is the non-changeable, globally unique name for the APX.
Extension Type	The APX type, such as Web or Program.
Extension Modified By User	The user who modified the APX.
Extension Modified On Date	The date the APX was modified.
OS Installation Profiles	All reporting objects related to the OS Installation Profiles stored in the SA Library. The Dimensions in this folder are meant to be used with other dimensions in the SA Library folder. You cannot use these dimensions with the device attributes.
OS Installation Profile Name	The name of the OS Installation Profile.
OS Installation Profile Version	The OS Installation Profile version.
OS Installation Profile	The date the OS Installation Profile was modified.

Object	Description
Modified On Date	
Library Packages	All reporting objects related to the Packages stored in the SA Library. The Dimensions in this folder are meant to be used with other dimensions in the SA Library folder. You cannot use these dimensions with the device attributes
Package Name	The name of the package
Package Type	The type of package, e.g. Zip or MSI
Package OS Name	The OS that this package can be installed on. Some packages can be installed on multiple OSs.
Package File Size (Bytes)	The size of the package in MB.
Package Modified On Date	The date the package was modified on.
Patch Policies	All reporting objects related to the Patch Policies stored in the SA Library. The Dimensions in this folder are meant to be used with other dimensions in the SA Library folder. You cannot use these dimensions with the device attributes.
Patch Policy Name	The name of the Patch Policy.
Patch Policy Description	The description of the Patch Policy.
Library Patches	All reporting objects related to the Patches stored in the SA Library. The Dimensions in this folder are meant to be used with other dimensions in the SA Library folder. You cannot use these dimensions with the device attributes.
Patch Name	The name of the patch.
Patch Description	The description of the patch.
Patch Type	The type of patch, such as Windows Service Pack or Hotfix.
Patch Platform	The platform for which this patch is targeted.
SA Folders	All reporting objects related to the Folders in the SA Library. The Dimensions in this folder are meant to be used with other dimensions in the SA Library folder. You cannot use these dimensions with the device attributes.
Folder Name	The folder name.
Folder Modified By User	The user who modified the SA Folder.
Modified On Date	The date the SA Folder was modified.

Object	Description
Folder Created On Date	The date the SA Folder was created.
Folder Created By User	The user who created the SA Folder.
Software Policies	All reporting objects related to the Software Policies stored in the SA Library. The Dimensions in this folder are meant to be used with other dimensions in the SA Library folder. You cannot use these dimensions with the device attributes.
Software Policy Name	The software policy name.
Software Policy Description	The software policy description.
Software Policy Modified On Date	The date the software policy was modified on.
Software Policy Modified By User	The user who modified the software policy

SA Jobs

Object	Description
SA Jobs	All reporting objects related to jobs run on servers. Elements in this folder must be paired with a server or device group dimension when used in reports. Note that elements in this folder CANNOT be used with the Single Date Filter or Date Range Filters
Job ID	The internal SA job identification number. This element must be paired with a server or device group attribute when used in reports. This element CANNOT be used with the Single Date Filter or the Date Range Filter.
Job Server Result Name	The job results for the given server. This element must be paired with a server or device group attribute when used in reports. This element CANNOT be used with the Single Date Filter or the Date Range Filter.
Job Server Status	The job status. Typical examples include Scheduled, Succeeded, Failed, etc. This element must be paired with a server or device group attribute when used in reports. This element CANNOT be used with the Single Date Filter or the Date Range Filter.
Job Description	The job description. This element must be paired with a server or device group attribute when used in reports. This element CANNOT be used with the Single Date Filter or the Date Range Filter.
Job Run Date	The date the job ran. This element must be paired with a server or device group attribute when used in reports. This element CANNOT be used with the Single Date Filter or the Date Range Filter.

Object	Description
Job Run by User	The user who ran this job. This element must be paired with a server or device group attribute when used in reports. This element CANNOT be used with the Single Date Filter or the Date Range Filter.
Job Run Date On	Filter to a specific date the jobs ran. This element must be paired with a server or device group attribute when used in reports. This element CANNOT be used with the Single Date Filter or the Date Range Filter.
Job Schedule Date On	Filter to a specific date the job was scheduled to run. This element must be paired with a server or device group attribute when used in reports. This element CANNOT be used with the Single Date Filter or the Date Range Filter.
Job Run Date Between	Filter to a specific date range in which the jobs ran. This element must be paired with a server or device group attribute when used in reports. This element CANNOT be used with the Single Date Filter or the Date Range Filter.
Job Schedule Date Between	Filter to a specific date range when the jobs were scheduled to run. This element must be paired with a server or device group attribute when used in reports. This element CANNOT be used with the Single Date Filter or the Date Range Filter.

Cross Item Groups

Object	Description
Cross Item Groups	Cross Item Groups are groups that contain Server Automation and Network Automation data. Use these objects as filters or as report output when you want to create cross-BSA reports. These objects are configured in the Administration tab of BSA Essentials.
Cross Job Group	Cross Job Groups contain jobs and/or tasks from Server Automation and Network Automation. Use these objects as filters or as report output when you want to create cross-BSA reports. These objects are configured in the Administration tab of BSA Essentials.
Cross Job Group Name	The name of the Cross Job Group. This object is configured in the Administration tab of BSA Essentials.
Cross Job Group Description	The description of the Cross Job Group. This object is configured in the Administration tab of BSA Essentials.
ROI Attributes	
Cross Job Group ROI Label	The Return on Investment (ROI) label assigned to this Job Group; for example: hours, dollars or euros. This object is configured in the Administration tab of BSA Essentials.
Cross Job Group ROI Value	The Return on Investment (ROI) value assigned to this Job Group. This object is configured in the Administration tab of BSA Essentials.
Sum of Cross Job Group ROI	Numerical sum of ROI values for all tasks in one Cross Job Group instance. This object is configured in the Administration tab of BSA Essentials.

Object	Description
Value	
Cross Policy Group	Cross Policy Groups contain policies from Server Automation and Network Automation. Use these objects as filters or as report output when you want to create cross-BSA reports. These objects are configured in the Administration tab of BSA Essentials.
Cross Policy Group Name	The name of the Cross Policy Group. This object is configured in the Administration tab of BSA Essentials.
Cross Policy Group Description	The description of the Cross Policy Group. This object is configured in the Administration tab of BSA Essentials.
Cross Device Group	Cross device groups contain devices and device groups from Server Automation and Network Automation. Use these objects as filters or as report output when you want to create cross-BSA reports. These objects are configured in the Administration tab of BSA Essentials.
Cross Device Group Name	The name of the Cross Device Group. This object is configured in the Administration tab of BSA Essentials.
Cross Device Group Description	The description of the Cross Device Group. This object is configured in the Administration tab of BSA Essentials.

SA Compliance Universe

The SA compliance universe defines a typical set of SA objects related to compliance and policies, allowing you to report on the various compliance levels for devices in your data center.

For example, you can report the compliance state of your servers of server groups over time, breaking down each policy by type, including SA audits, software policies, patch policies (Windows and Unix), and software policies. You can break down your server's compliance states to a more granular level by display such information as total number of policies for a server of groups of servers, exact number of non-compliant policies, and so on.

Additionally, the SA compliance universe contains generic query filters and Cross Group objects so you can limit your compliance report results to specific device groups, job groups, and user groups from SA.

The following tables describe the contents of the SA Compliance universe:

General

Object	Description
As of Date	Date associated with a row record; for example, such as of 4/10/2009, device r144 compliant state was Non-Compliant. Include this if you want the date corresponding to each row in the report. In any historical or trending report, you must include As Of Date in the Result Objects for

Object	Description
	your report or the data will not display properly. (Note: The As of Date object can only be used as a Result Object and cannot be used as a filter.)
Single Date Filter	Use the Single Date Filter to specify a single date in history where you want to report on an object from the Device, Device Group, Administration and Library objects. Do not use this filter with the SA Jobs objects.
Date Range Filter	Use the Date Range Filter to specify the historical date range you want to report on for the Device, Device Group, Administration and Library objects. Do not use this filter with the SA Jobs objects. The Date Range Filter is most useful when you want to create trending reports. When using the Date Range Filter, it is recommended that you include the As Of Date element in the Result Objects panel.

Cross Item Groups

Object	Description
Cross Item Groups	Cross Item Groups are groups that contain Server Automation and Network Automation data. Use these objects as filters or as report output when you want to create cross-BSA reports. These objects are configured in the Administration tab of BSA Essentials.
Cross Job Group	Cross Job Groups contain jobs and/or tasks from Server Automation and Network Automation. Use these objects as filters or as report output when you want to create cross-BSA reports. These objects are configured in the Administration tab of BSA Essentials.
Cross Job Group Name	The name of the Cross Job Group. This object is configured in the Administration tab of BSA Essentials.
Cross Job Group Description	The description of the Cross Job Group. This object is configured in the Administration tab of BSA Essentials.
ROI Attributes	
Cross Job Group ROI Label	The Return on Investment (ROI) label assigned to this Job Group, e.g. hours, dollars or euros. This object is configured in the Administration tab of BSA Essentials.
Cross Job Group ROI Value	The Return on Investment (ROI) value assigned to this Job Group. This object is configured in the Administration tab of BSA Essentials.
Sum of Cross Job Group ROI Value	Numerical sum of ROI values for all tasks in one Cross Job Group instance. This object is configured in the Administration tab of BSA Essentials.
Cross Policy Group	Cross Policy Groups contain policies from Server Automation and Network Automation. Use these objects as filters or as report output when you want to create cross-BSA reports. These objects are configured in the Administration tab of BSA Essentials.

Object	Description
Cross Policy Group Name	The name of the Cross Policy Group. This object is configured in the Administration tab of BSA Essentials.
Cross Policy Group Description	The description of the Cross Policy Group. This object is configured in the Administration tab of BSA Essentials.
Cross Device Group	Cross device groups contain devices and device groups from Server Automation and Network Automation. Use these objects as filters or as report output when you want to create cross-BSA reports. These objects are configured in the Administration tab of BSA Essentials.
Cross Device Group Name	The name of the Cross Device Group. This object is configured in the Administration tab of BSA Essentials.
Cross Device Group Description	The description of the Cross Device Group. This object is configured in the Administration tab of BSA Essentials.

SA Device

Object	Description
Server Name	The name of the server as displayed in the SA User Interface.
Host Name	Server name as reported by the command uname or the computer name.
Primary IP Address	The primary IP Address for this server.
Reported OS	The operating system for the server, as reported by the SA agent.
Server Model	The model number of the server.
Server Manufacturer	The name of the hardware vendor.
Server Type	The type of server. This dimension has 3 possible values: physical, virtual machine or hypervisor.
Customer Name	The HP Server Automation Customer the server belongs to.
Facility Name	The HP Server Automation Facility the server belongs to.
Custom Attribute Name	The HP SA Custom Attribute Name. This is most often paired with the Custom Attribute Value.

Object	Description
Custom Attribute Value	The HP SA Custom Attribute Value. BSA Essentials only stores the first 4000 characters of the data.
Server Compliance for Policies	This dimension object indicates the rolled up compliance state for this server across all policies This object may be used as a Condition in a query to filter by compliance state. The precedence logic for determining the rollup state is the following: Scan Failed → Scan Needed → Non Compliant → Partial Compliant → Compliant. This object is meaningful only when paired with a server.
Server Measures	Folder containing the policy roll up measures for server compliance
Compliance State	Compliance State for a server and policy combination. The compliance state rollup value that this object reports is keyed to the dimensions that it is paired with. Specifically: • Can be paired with a policy and a server to report the compliance state just for that combination. • Can be used with just a server to report the rolled up compliance state across all policies attached to that server • Can be used with just a policy name to report the rolled up compliance state across all servers that this policy applies to • Can be used with a device group name to report the rolled up compliance state for all member servers across all policies. Compliance state is initially rolled up to each server (across all policies), and then across all devices that are members of the device group • Can be used with a device group and a policy to report the same as above but just for a single specific policy This object is a calculated value and so cannot be used as a Condition in a query. The precedence logic for determining the rollup state is the following: Scan Failed → Scan Needed → Non Compliant → Partial Compliant → Compliant.
Number of Compliant Policies	The number of policies that are compliant for the given server. This is an aggregate roll up across all types of policies if unfiltered. If you apply the policy type filter, it can be constrained to a specific type of policy. This is meaningful only when paired with a server.
Number of Non-Compliant Policies	The number of policies that are not compliant for the given server. This is an aggregate roll up across all policies if unfiltered. If you apply the policy type filter, it can be constrained to a specific type of policy or to a group of policies. This is meaningful only when paired with a server.
Number of Scan-Needed Policies	The number of policies where a scan is needed for the given server. This is an aggregate roll up across all policies if unfiltered. If you apply the policy type filter, it can be constrained to a specific type of policy or to a group of policies. This is meaningful only when paired with a server.
Number of Scan-Failed Policies	The number of policies for which scan had failed for the given server. This is an aggregate roll up across all policies if unfiltered. If you apply the policy type filter, it can be constrained to a specific type of policy or to a group of policies. This object is meaningful only when paired with a server.

Object	Description
Total Number of Policies	The total number of policies for the given server. This is an aggregate roll up across all policies if unfiltered. If you apply the policy type filter, it can be constrained to a specific type of policy or to a group of policies. This object is meaningful only when paired with a server.
Compliant Ratio	The number of compliant policies over the total number of policies attached to a server, e.g. 4/12. This is an aggregate roll up across all policies if unfiltered. If you apply the policy type filter, it can be constrained to a specific type of policy or to a group of policies. This object is meaningful only when paired with a server.
Non-Compliant Ratio	The number of non-compliant policies over the total number of policies attached to a server, e.g. 4/12. This is an aggregate roll up across all policies if unfiltered. If you apply the policy type filter, it can be constrained to a specific type of policy or to a group of policies. This object is meaningful only when paired with a server.
Server Advanced Attributes	Folder containing objects related to advanced server attributes, mostly related to virtualization
Server Identifier	This object indicates the unique machine identifier that SA generates when the agent is installed on a server. This object is meaningful only when paired with a managed server.
Management IP Address	The IP address that HP Server Automation uses to communicate with the Server Agent on the managed server.This object thus is meaningful only when paired with a managed server.
Server Name Filter	Use this to filter query results based on the name of a server.
Customer Filter	Use this to filter query results based on the name of a Customer.
Facility Filter	Use this to filter query results based on the name of a Facility

Virtualization

Object	Description
Virtualization	All reporting objects related to virtualization.
Hypervisor Attributes	All reporting objects related to managed Hypervisors.
Hosting Hypervisor Display Name	The name of the Hosting Hypervisor as displayed in the SA User Interface.
Hosting Hypervisor Reported OS	The operating system for the hypervisor, as reported by the SA agent.
Hosting Hypervisor Primary IP	The primary IP Address of hosting hypervisor
Hosting Hypervisor Host Name	Hosting Hypervisor hostname reported by the computer

Object	Description
Discovered VM Attributes	All reporting objects related to virtual machines discovered via their hypervisors.
Discovered VM Name	This is the virtual machine's name as discovered through its Hypervisor. This is typically the user supplied name.
Discovered VM Description	This is the virtual machine description as discovered through its hypervisor
Discovered VM Status	This is the virtual machine's power state as discovered through its Hypervisor. Typical values are Powered On, Suspended, Powered Off.
Discovered VM Type	This is the virtualization type, such as VMware VM or Solaris 10 Container, as discovered through its Hypervisor.

Device Group

Object	Description
Device Group	All reporting objects related to SA Device Groups
Device Group Name	The device group name as displayed in the SA Client.
Device Group Owner	The owner of the device group.
Device Group Root Parent	The parent device group, in the cases where a device group contains children device groups.
Device Group Path	Absolute pathame of the device group.
Device Group Measures	Folder containing the device group compliance policy rollup measures
Total Servers In Device Group	Total number of servers in the device group that have any type of policies attached to them. Note that this object does not count those servers in the device group that do not have attached policies. This object is meaningful only when paired with a device group.
Total Servers in State	The number of servers that are in the selected state within the device group. State for a server is calculated based on the policies attached to it. Even though a server can be in different states with respect to different policies, this object indicates the aggregate state roll up across all policies attached to each server. This object is meaningful only when paired with a device group. This object automatically adds an embedded filter condition to the query. The embedded condition prompts for the specific state value keyed to the Total Servers In State object.

Object	Description
Total Compliance Policies	Total number of compliance policies that are compliant and apply to servers within the device group. This is an aggregate roll up across all types of policies if unfiltered. You may optionally constrain the results by applying a specific policy type filter, or selecting a subset of policies as filters. This object is meaningful only when paired with a device group.
Total Policies	Total number of policies that apply to servers within the device group. This is an aggregate roll up across all types of policies if unfiltered. You may optionally constrain the results by applying a specific policy type filter. This object is meaningful only when paired with a device group.
Device Group Filter	

Policy

Object	Description
Policy	Folder containing a number of policy-related objects in Server Automation
Common Policy Attributes	Folder that contains objects common to all types of policies in Server Automation, e.g. across Audit, AppConfig etc.
Policy Name	Name of the policy. This is a generic policy name object that can report the policy name for any policy type –app config, patch, software or audit.
Policy Description	Description of the policy. This is a generic policy description object that can report the policy description for any policy type – app config, windows patch, software or audit. This object is meaningful only when paired with a policy.
Policy Type	Type of the policy. This specifies the policy type - app config, windows patch, software or audit. This object is meaningful only when paired with a policy.
Policy Server Last Scan Date	Last scan date for a server+policy combination. The value indicated by this object is meaningful only when paired with a specific server and a policy.
Policy Compliance for Servers	This dimension object indicates the rolled up compliance state for this policy across all servers This may be used as a Condition in a query. The precedence logic for determining the rollup state is the following: Scan Failed → Scan Needed → Non Compliant → Partial Compliant → Compliant. This object is meaningful only when paired with a policy.
Policy Server Last Scan Date Range	User this filter to filter all records that have Policy Server Most Recent Scan Date values between the two user date inputs (inclusive of the two end dates).
Common Policy Measures	Folder that contains roll up measures common to all types of policies in Server Automation.
Number of Compliant Servers	The number of servers that passed the compliance scan for the policy. This is an aggregate roll up across all servers that have the attached compliance policy if unfiltered. If you apply a server attribute or a device group filter, this object can be constrained to the corresponding subset of servers. This object is meaningful only when paired with a pol-

Object	Description
	icy.
Number of Partially Compliant Servers	The number of servers that are Partially Compliant to the policy. This is an aggregate roll up across all servers that have the attached compliance policy if unfiltered. If you apply a server attribute or a device group filter, this object can be constrained to the corresponding subset of servers. This object is meaningful only when paired with a policy.
Number of Non-Compliant Servers	The number of servers that are "Non Compliant" to the policy. This is an aggregate roll up across all servers that have the attached compliance policy if unfiltered. If you apply a server attribute or a device group filter, this object can be constrained to the corresponding subset of servers. This object is meaningful only when paired with a policy.
Number of Scan-Needed Servers	The number of servers that are "Scan Needed" for the policy. This is an aggregate roll up across all servers that have the attached compliance policy if unfiltered. If you apply a server attribute or a device group filter, this object can be constrained to the corresponding subset of servers. This object is meaningful only when paired with a policy.
Number of Scan-Failed Servers	The number of servers that are "Scan Failed" for the policy. This is an aggregate roll up across all servers that have the attached compliance policy if unfiltered. If you apply the server or device group filter, it can be constrained to a specific server or a device group. This object is meaningful only when paired with a policy.
Number of Servers	The number of servers that are associated with the policy. This is an aggregate roll up across all servers that have the attached compliance policy if unfiltered. If you apply a server attribute or a device group filter, this object can be constrained to the corresponding subset of servers. This object is meaningful only when paired with a policy.
Compliant Server Ratio	The number of compliant servers over the total number of servers for the given policy; for example, 4/12. This object is meaningful only when paired with a policy. This is an aggregate roll up across all devices if unfiltered. If you apply the server or device group filter, it can be constrained to a specific server or a device group.
Compliance State	
Server Audit/Audit Policy Compliance	Folder that contains roll up measures and attributes specific to Audits and Audit Policies in Server Automation
Audit	Folder that contains attributes specific to Audits in Server Automation.
Audit Name	Name of an Audit in Server Automation.
Audit Description	Description of the Audit in Server Automation.
Audit Compliance State	Compliance state of the Audit. This indicates the status of the audit with respect to the server, and is meaningful only when paired with a server and an audit.
Audit Server Last Scan Time	Last scan date for a server+audit combination. The date has a meaningful value only when paired with a server and audit.

Object	Description
Audit Server Last Scan Date Range	Date range for a server+audit combination. The date range has a meaningful value only when paired with a server and audit.
Audit Rules	
Audit Rule Name	Name of an audit rule. This is meaningful only when paired with an audit. Description of the Audit Rule in Server Automation. This is meaningful only when paired with an audit and a rule.
Audit Rule Type	Type of the Audit Rule. This is meaningful only when paired with an audit and a rule.
Audit Rule Expected Value	Expected value from the Audit Rule. This is the expected return value or standard output associated with the audit rule. The expected value is tested against the actual audit value. This object is meaningful only when paired with an audit and a rule
Audit Rule Actual Value	Actual value from the audit rule run. This is the observed return value or standard output observed when the audit rule was run. This is meaningful only when paired with a server, an audit and a rule.
Audit Rule Operator	Operator used in audit rule evaluation. This is meaningful only when paired with an audit and a rule.
Audit Rule Compliance State	Compliance state of the audit rule. The state is meaningful only when paired with an audit, a rule and a server or device group that is a target of this audit rule.
Audit Exceptions	Folder that contains objects specific to Audit Exceptions for rules in Audits that were attached to and scanned for a server. Audit exception is specific to an audit, rule and a server.
Audit Exception Reason	Reason for an Audit Exception. This is meaningful only when paired with an audit exception.
Audit Exception Expiration Date	Expiration Date for an Audit Exception. This is meaningful only when paired with an audit exception.
Audit Exception Created By	Creator of an Audit Exception. This shows the SA user who created the exception for the selected audit. This is meaningful only when paired with an audit exception.
Audit Exception Ticket Date	Ticket ID for the Audit Exception. This is the ticket associated with an Audit Exception entry. This is meaningful only when paired with an audit exception.
Audit Rule Exception Exist Filter	Use this to filter query results based on the existence of an audit exception
Audit Exception Expiration Date Filter	Use this to filter query results based on the expiration date of an audit exception. Note that all Exceptions that never expire will be filtered out.

Object	Description
Audit Exception Expiring in N Days	Use this to filter query results based on the an audit exception expiring in N Days from today. Note that all Exceptions that never expire will be filtered out.
Jobs Info for Audit Scan	Folder that contains objects related to SA Audit job runs.
Audit Job Status	Status of Audit job completion. This indicates the audit job completion status as applicable to a specific server, so is meaningful only when paired with a server and an audit.
Audit Schedule Date	Audit Schedule Date. This object indicates the date the job was scheduled to run on. This is meaningful only when paired with a server and an audit.
Audit Job Run Date	Date on which the job was run. This object indicates the date the audit job actually ran on. This is meaningful only when paired with a server and an audit.
Audit Job Run By	User who scheduled the audit job. This is meaningful only when paired with a server and an audit.
Audit Job Run Date Range Filter	User this filter to filter all records that have Audit Job Run Date values Between the two user date inputs (inclusive of the two end dates).
Audit Job Run Date Filter	User this filter to filter all records that have Audit Job Run Date Equal To user input
Server Audit Measures	Folder that contains objects related to rollup measures related to SA Audits
Total Audit Non-Compliant Rules	Number of non-compliant audit rules. This object indicates the aggregate number of audit rules that are not in the "Compliant" state for the given server across all audits. This is meaningful only when paired with a server. If you apply the audit or audit policy filter or reported together with audit or audit policy dimensions, the measure can be constrained to a specific audit or audit policy attached to that server.
Total Audit Compliant Rules	Number of compliant audit rules. This object indicates the aggregate number of audit rules that are in the "Compliant" state for the given server across all audits. This is meaningful only when paired with a server. If you apply the audit or audit policy filter or reported together with audit or audit policy dimensions, the measure can be constrained to a specific audit or audit policy attached to that server.
Number of Audit Rules	Total number of audit rules. This object indicates the aggregate number of audit rules that apply to the given server across all audits. This is meaningful only when paired with a server. If you apply the audit or audit policy filter or reported together with audit or audit policy dimensions, the measure can be constrained to a specific audit or audit policy attached to that server.

Object	Description
Compliant Audit Rules Ratio	The ratio of compliant audit rules over the total number of audit rules that apply to the server. This object indicates the aggregate ratio of compliant audit rules that apply to the given server across all audits. This is meaningful only when paired with a server. If you apply the audit or audit policy filter or reported together with audit or audit policy dimensions, the measure can be constrained to a specific audit or audit policy attached to that server.
Non-Compliant Audit Rules Ratio	The ratio of non-compliant audit rules over the total number of audit rules that apply to the server. This object indicates the aggregate ratio of non-compliant audit rules that apply to the given server across all audits. This is meaningful only when paired with a server. If you apply the audit or audit policy filter or reported together with audit or audit policy dimensions, the measure can be constrained to a specific audit or audit policy attached to that server.
Server Patch Compliance (Windows Only)	Folder that contains patch compliance policy items in patch policies attached to a server with a successful last scan
Patch Policy Patches	Folder that contains objects related to patches in patch policies specific to Windows servers in Server Automation.
Patch name	This object indicates the name of the Patch in the patch policy. This object is meaningful only when paired with a patch policy.
Patch Type	This object indicates the type of the patch in the Patch Policy, e.g. hot fix, service pack. This object is meaningful only when paired with a patch policy and a patch in that patch policy
Patch Description	This object indicates the complete description of the patch in the patch policy. This object is meaningful only when paired with a patch policy and a patch in that patch policy.
Patch Size in KB	This object indicates the patch size in KB for the patch in the Patch Policy. This object is meaningful only when paired with a patch policy and a patch in that patch policy.
Patch Compliance State	This object indicates the compliance state for the patch associated with the patch policy attached to a server. This object is meaningful only when paired with a patch policy, a patch in that patch policy and a server.
Patch Bulletin	This object indicates the Microsoft patch bulletin number associated with a patch in the patch policy. This object is meaningful only when paired with a patch policy and a patch in that patch policy.
Patch Severity	This object indicates the Microsoft-recommended severity of the Windows patch associated with the patch in the patch policy. This object is meaningful only when paired with a patch policy and a patch in that patch policy.
Patch Exceptions	Folder that contains objects related to exceptions for patches in Patch Policies for Windows servers in Server Automation.
Patch Exception Reason	This object indicates the reason for a granted exception to a patch in a patch policy. This object is meaningful only when paired with a patch, patch policy and an attached server.

Object	Description
Patch Exception Rule	This object indicates the rule to be applied on a granted exception to a Patch Policy. This object is meaningful only when paired with a patch policy and an attached server.
Patch Exception Created Dated	This object indicates the date on which a granted exception to a patch was created. This object is meaningful only when paired with a patch in a patch policy attached to a server.
Patch Exception Exist Filter	Use this to filter query results based on the existence of an Patch exception
Server Patch Policy Measures	Folder containing the patch policy compliance measures
Number of Compliant Patches	This object indicates the aggregate number of compliant patches from all patch policies that apply to this server. This object is meaningful only when paired with a server. This object may be optionally filtered on a patch policy to return the compliant patch count just in that patch policy.
Number of Non-Compliant Patches	This object indicates the aggregate number of non-compliant patches from all patch policies that apply to this server. This object is meaningful only when paired with a server. This object may be optionally filtered on a patch policy to return the non-compliant patch count just in that patch policy.
Number of patches	This object indicates the aggregate number of patches from all patch policies that apply to this server. This object is meaningful only when paired with a server. This object may be optionally filtered on a patch policy to return the patch count just in that patch policy.
Number of Exceptions	This object indicates the aggregate number of exceptions on all patch policies that apply to this server. This object is meaningful only when paired with a server.
Compliance Patch Ratio	This object indicates the aggregate ratio of compliant patches over all the patches in the patch policy attached to this server. This object is meaningful only when paired with a patch policy and a server.
Non-Compliant Patch Ratio	This object indicates the aggregate ratio of non-compliant patches over all the patches in the patch policy attached to this server. This object is meaningful only when paired with a patch policy and a server.
Server App Configuration Compliance	Folder that contains all objects related to Application Configuration policies in Server Automation
App Config Policy	Folder that contains Application Configuration Policy related-objects, when the policies are attached to one or more servers and have been scanned once against attached servers
App Config Policy Item	This object identifies a specific App Config policy item related to this Policy. This object is meaningful only when paired with an App Config policy.
App Config Policy Item Compliance	This object indicates the compliant state of the specific App Config policy item related to this policy attached to a server. This object is meaningful only when paired with an App Config policy, a policy item, and a server.

Object	Description
App Config Compliance Jobs	Folder containing objects related to App Config compliance job runs.
App Config Job Status	This object indicates the job status of an App Config compliance job run. This object is meaningful only when paired with an App Config policy and a server.
App Config Job Type	This object indicates the job type of an App Config compliance job run. This object is meaningful only when paired with an App Config policy and a server.
App Config Job Schedule Date	This object indicates the date an App Config compliance job is scheduled to run on. This object is meaningful only when paired with an App Config policy and a server.
App Config Job Run Date	This object indicates the job type of an App Config compliance job run. This object is meaningful only when paired with an App Config policy and a server.
App Config Job Run By	User who scheduled the app config job. This is meaningful only when paired with a server and an app config.
App Config Job Run Date Range	User this filter to filter all records that have App Config Job Run Date values between the two user date inputs (inclusive of the two end dates)
App Config Job Run Date Filter	User this filter to filter all records that have App Config Job Run Date Equal To user input
Server App Config Policy Measures	Folder containing all the rollup measures related to App Config Policies from a server-centric perspective when the policies are attached to one or more servers and have had a successful last scan
Number of Config Files	This object indicates the aggregate number of config files checked for the application defined in the app config policy. If the application has multiple available instances, this object represents the aggregate number of config files across all such instances. This object may be filtered on or reported together with a subset of App Config policies. This object is meaningful only when paired with a server.
Number of Compliant Config Files	Number of Compliant Config Files. This object indicates the number of compliant config files among the total number of config files checked for the application defined in the app config policy. If the application has multiple available instances, this object is based on the aggregate number of config files across all such instances. This object may be filtered on or reported together with a subset of App Config policies. This object is meaningful only when paired with a server.
Compliant Config File Ratio	This object indicates the ratio of compliant config files over the total number of config files checked for the application defined in the app config policy. If the application has multiple available instances, this ratio is computed based on the aggregate number of config files across all such instances. This object may be filtered on or reported together with a subset of App Config policies. This object is meaningful only when paired with a server and an App Config policy.
Non-Compliant Config File Ratio	This object indicates the number of non-compliant config files among the total number of config files checked for the application defined in the app config policy. If the appli-

Object	Description
	cation has multiple available instances, this object is based on the aggregate number of config files across all such instances. This object may be filtered on or reported together with a subset of App Config policies. This object is meaningful only when paired with a server.

SA Compliance Universe Policy Considerations

The following is a list of considerations when building reports on SA Policies from the SA Compliance Universe:

- All policies in SA can be reported on at the top-level always, independent of the attached and/or compliance status of a policy with respect to a server or a device group.
- For software policies, the contained item level information can be reported if the policy is directly or indirectly attached to a server and was scanned once, independent of the compliance status of the policy.
- For AppConfig and Patch policies, the contained item level information within a policy can be reported only if the following is true:
  - Policy must be attached (patch policies may also be indirectly attached) to a server
  - Last scan of the policy for a server has to be successful. If the Scan was successful at some point and then subsequently failed, the Universe still cannot report on the policy details.
- Audits and Audit policies in general can report the rule level detail always, with a couple of additional considerations
  - Audits have to be attached to a server and have had a scan
  - Known caveat: "Unknown error" audit status in some cases may prevent the rule level information from being reported on

Policy Rule Counts in Report Results

The reported rule count for Policy objects and Audits in SA Compliance Universe may be 0 any time:

- Software policy - if the policy was never scanned against the attached target(s)

  OR
- Patch policy & AppConfig Policy - the policy object has not successfully scanned against their attached target(s) in the last scan on the reporting day - in other words, Compliance State = Scan Failed for the last scan of the policy

  OR
- Audits and/or Audit Policy: refer to the previous section on when rule-level detail is available

  OR
- The policy or audit object truly has 0 rules

This applies to the following types of SA Compliance Universe objects

- SA Software Policy
- SA Patch Policy

- SA AppConfig Policy
- SA Audit Policy
- SA Audit (which has audit rules as direct members)

NA General Universe

The NA general universe defines a typical set of NA objects and their attributes and allows you to report on them. For example, the NA General universe defines network devices and all significant related information about them such as asset, port, and configuration details; related device groups, advanced attributes, compliance and diagnostic information; task user, and job information, so on.

Additionally, the NA compliance universe contains generic query filters and Cross Item Group objects so you can limit your compliance report results to specific device groups, job groups, and user groups from NA.

The following tables describe the contents of the NA Compliance universe:

General

Object	Description
As of Date	The As Of Date displays the date the specific record was captured in the BSA Essentials database. You include this dimension if you want to display the date corresponding to each output row in the report. In any historical or trending report, including the associated date for each record is especially useful. (Note: The As of Date object can only be used as a Result Object and cannot be used as a filter.)
Single Date Filter	Use the Single Date Filter to specify a single date in history where you want to report on. Do not use this filter with the NA Jobs objects.
Date Range Filter	Use the Date Range Filter to specify the historical date range you want to report on. Do not use this filter with the NA Jobs objects. The Date Range Filter is most useful when you want to create trending reports. When using the Date Range Filter, it is recommended that you include the As Of Date element in the Result Objects panel.

NA Devices

Object	Description
NA Devices	Folder containing report objects related to NA devices.
Asset Details	Folder containing the asset information objects related to managed devices.
Host Name	This object indicates the Host Name of the device as configured on the device.
Primary IP	This object indicates the primary IP address that uniquely identifies the selected device. This object thus is meaningful only when paired with a device.
Device Vendor	This object indicates the vendor who manufactured the device. This object thus is meaningful only when paired with a device.
Device Model	This object indicates the manufacturer's model number for the device. This object thus is meaningful only when paired with a device.

Object	Description
Device Name	Name of a device as displayed in NA.
Driver Name	This object indicates the NA driver assigned to the device and thus is meaningful only when paired with a device.
Access Methods	This object indicates the means of accessing a managed device. This object thus is meaningful only when paired with a device.
Serial Number	This object indicates the manufacturer's serial number for the device. This object thus is meaningful only when paired with a device.
Asset Tag	This object indicates the company's asset tag number for the device. This object thus is meaningful only when paired with a device.
Device Software Version	This object indicates the version of operating system software running on the device. This object thus is meaningful only when paired with a device.
Device Descriptions	This object indicates the user defined description of the device. This object thus is meaningful only when paired with a device.
Device Comments	Descriptive comments associated with the NA device.
System Memory (MB)	This object indicates the total amount of RAM (MB) on the device. This object thus is meaningful only when paired with a device.
Port Details	Folder containing the objects related to port-specific attributes.
Port Name	The unique device interface port name as defined by the device vendor such as Ethernet0 or Serial1. This object thus is meaningful only when paired with a port.
Port IP	This object indicates the IP address of a port. When paired with a device, this object reports the Port IP address as configured on the device.
Port Type	The network interface type of the port such as Ethernet, FastEthernet etc. This object thus is meaningful only when paired with a port.
Port Status	This object indicates the configured port status of a network device interfaces. This object thus is meaningful only when paired with a port.
Running Port State	This object indicates the line state of port (for example, if there is a link on the port). This object thus is meaningful only when paired with a port.
Free Ports	This object indicates the total number of ports NOT configured up for a device. This object thus is meaningful only when paired with a device.
Percentage Free Ports	This object indicates the percentage of ports NOT configured up for a device. This object thus is meaningful only when paired with a device.
Total Ports	This object indicates the total number of ports on the device. This object thus is meaningful only when paired with a device.
Ports in Use	This object indicates the total number of ports configured up for a device. This object thus is meaningful only when paired with a device.
Percentage of Ports in Use	This object indicates the percentage of ports configured up for a device. This object thus is meaningful only when paired with a device.

Object	Description
Port Description	This object indicates the port description as configured on the device. This object is meaningful only when paired with a port.
MAC Address	This object indicates the MAC address found in MAC table of a device. When paired with a device, this shows the MAC addresses associated with that device.
Configured Duplex	This object indicates Duplex configured within the interface configuration (for example, full, half, auto). This object is meaningful only when paired with a port.
Configured Speed	This object indicates the speed in Mbps configured within the interface configuration (for example, 10, 100, 1000, 10000). This object is meaningful only when paired with a port.
Negotiated Duplex	This object indicates Duplex negotiated by device and remote device via auto-configuration of duplex within interface configuration. This object is meaningful only when paired with a port.
Negotiated Speed	This object indicates the speed negotiated by device and remote device via auto-configuration of speed within interface configuration. This object is meaningful only when paired with a port.
VLAN Name	When paired with a device, this object reports the VLAN name as configured on the device. When paired with a port, this object indicates the VLAN name for the VLAN that this port is a part of.
VLAN Description	This object reports the VLAN description as configured on the device. This object is meaningful only when paired with a device. When paired with a port, this object indicates the VLAN description for the VLAN that this port is a part of.
Configuration Details	This Folder includes all configuration-related objects for managed devices.
Configuration Text	This is the current configuration for each device. This field is typically used to search for devices that contain or do not contain a certain commands.
Configuration Template Name	This object indicates the name of a configuration template. A configuration template may optionally be paired with configuration template fields such as vendor or driver to report on the fields of a template.
ACL ID	The ACL ID is an number based on the device ACL list, while the ACL Handle is a descriptive name or value assigned by the user. By default, the ACL ID and ACL Handle are the same until the user defines the ACL Handle. This object thus is meaningful only when paired with a device.
ACL Handle	This object indicates the descriptive name or value assigned by the user. By default, the ACL ID and ACL Handle are the same until the user defines the ACL Handle. This object thus is meaningful only when paired with a device.
ACL Type	This object indicates the Access Control List Type defined by the device vendor. This object thus makes sense only when paired with a device or a driver.
ACL Application	This object indicates the configuration text associated with how a specific ACL is being applied. ACLs are commonly applied to interfaces and other features in NA. This object can thus be paired with a number of NA Universe objects that an ACL

Object	Description
	Application may relate to in a Network Automation deployment.
Service Type	This object indicates the type of service provided by a Device which typically indicates its purpose. An example is "VoIP". Note that this field is not automatically populated for each device. This object thus is meaningful only when paired with a device.
Custom Service Type	This object reports on the Custom Service Type which is a free form text field that can contain information about a Device. New Custom Service Types for the NA deployment may be defined by the Admin interface.
Partition	This object indicates the partition name that the device, interface, command scripts, policies, etc is associated with. This object can thus be paired with a number of NA Universe objects that a Partition may relate to in a Network Automation deployment.
Device Group	Allows you to filter the report results by the Device Group.
Partition	Allows you to filter the report results by the Partition.
Module Details	Folder containing the report objects related to Module attributes.
Module Slot	This object indicates the slot number of the module for the real or virtual location as identified by the device vendor. This object is thus meaningful only when paired with a module.
Module Description	This object indicates the description of the module as identified by the device vendor. This object is thus meaningful only when paired with a module.
Module Model	This object indicates the model name of the module as identified by the device vendor. This object is thus meaningful only when paired with a module.
Module Serial	The object indicates the module's serial number. This object is meaningful when paired with a device.
Module Memory	This object indicates the total amount of RAM (MB) on the module. This object is thus meaningful only when paired with a module.
Module Firmware Version	This object indicates the version number of the firmware loaded on the module. This object is thus meaningful only when paired with a module.
Module Hardware Revision	This object indicates the module's hardware revision designation by the manufacturer. This object is thus meaningful only when paired with a module.
Module Comments	This object reports the free form text that can contain any user-input data about each module. This object is thus meaningful only when paired with a module.
Operational Details	Folder containing objects related to the operational aspects of the managed devices.
Device Management Status	This object indicates the current management status of the device such as active, inactive or pre-production. This object thus is meaningful when paired with a device.
Password Rule	This object indicates the password rule name for the device which was set as the preferred password rule to try first. This object thus is meaningful when paired with a device.

Object	Description
Compliance State	This measure object aggregates the compliance state for this device always across all the policies attached the device. Policy level compliance is rolled up across all the rules defined for the policy. The aggregate value of the object evaluates to "Y" or "N". This object is meaningful only when paired with a device.
Different Start-up/Running	This object reports "Y"when the startup configuration of a device does not match its running configuration, or reports "N" if the two do match. This object thus is meaningful when paired with a device.
Changed Time	This object indicates the date and time the device's configuration was last changed. This object thus is meaningful when paired with a device.
Changed By	This object indicates the login name of the person who changed the configuration of a device. This object thus is meaningful when paired with a device.
Different Startup Running Config	Allows you to filter the report results by whether or not there is a difference between the device's startup and running configuration.
Device Status	Allows you to filter by the Device Status. Device Status can be inactive, active or pre-production
Device Group	Folder containing the objects related to NA Device Group attributes
Parent Group Item ID	This object indicates the NA Item ID of the parent device group of the selected device or device group. This is meaningful only when paired with a device or device group.
Device Group Name	This object indicates the name of the parent device group of the selected device or device group. This is meaningful only when paired with a device or device group.
Description	This object indicates the description of the parent device group of the selected device or device group. This is meaningful only when paired with a device or device group.
NA Device Group Device Compliance	
Advanced Attrib-utes	Folder containing NA device group attributes
NA Device ID	This object indicates the unique ID within NA for the managed device. This object thus is meaningful when paired with a device.

NA Compliance

Object	Description
NA Compliance	Folder containing all compliance related objects for NA.
Device Compliance Summary	This measure object aggregates the compliance state for this device always across all the policies attached the device. Policy level compliance is rolled up across all the rules defined for the policy. The aggregate value of the object evaluates to "Y" or "N"
Policy	Folder containing objects related to NA configuration policies

Object	Description
Policy Name	This object indicates the name of a policy.
Policy Description	This object indicates the description of a policy and thus is meaningful only when paired with a policy.
Policy Tag	This object indicates the tag name a policy is grouped under. This object is meaningful only when paired with a policy.
Policy Modified Date	Date on which the policy was last modified.
Policy Is Active	Status of the policy. This object indicates the current status of a policy - either active or inactive. This object is meaningful only when paired with a policy. (Currently reports Y or N, should report "Active" or "Inactive")
CVE	Common Vulnerabilities and Exposures name for a vulnerability. This object reports the CVE out of a list of standardized names for vulnerabilities and other information on security exposures. This field is automatically populated when the policy is from the HP Security and Compliance.
Disclosure Date	Disclosure date for a vulnerability. This object indicates the first date when a vulnerability was first flagged. This field is automatically populated when the policy is from the HP Security and Compliance Service. This object is meaningful only when paired with a policy.
Solution	Solution text for a policy. This object indicates the first 4000 characters of the detailed solution text, if any, for a policy. This field is automatically populated when the policy is from the HP Security and Compliance Service. This object is meaningful only when paired with a policy.
Vendor Advisory URL	Vendor Advisory for the vulnerability. This object indicates the Vendor Advisory external reference URL for advisory information on a vulnerability. This field is automatically populated when the policy is from the HP Security and Compliance Service. This object is meaningful only when paired with a policy.
Vendor Solution URL	Vendor Solution for the vulnerability. This object indicates the Vendor Solution external reference URL where more information from the device vendor on possible solutions to the vulnerability may be found. This field is automatically populated when the policy is from the HP Security and Compliance Service. This object is meaningful only when paired with a policy.
Partition	Name of the partition. This object indicates the name of the partition that a policy belongs to. Consequently, this object is meaningful only when paired with a policy.
Rule	Folder containing objects related to NA configuration policies.
Rule Name	Name of the rule. This object indicates the name of the rule in the policy, and thus is meaningful only when paired with a policy.
Rule Importance	Importance of this rule. This object indicates the importance level of a rule as one of Informational, Low, Medium, High or Critical. This object is meaningful only when paired with a policy and a rule.
Rule Type	Type of a rule. This object indicates if a rule is a configuration, or a diagnostic or a software rule. This object is meaningful only when paired with a policy and a rule.

Object	Description
Rule Description	Description of a rule. This object indicates the description of a rule in a policy and thus is meaningful only when paired with a policy and a rule.
Rule Compliance State	Compliance state for a rule. This object indicates the state of compliance of a device with respect to a specific rule in a policy. This object is meaningful only when paired with a device, a policy and a rule.
Software Levels	Folder containing the objects related to software levels.
Software Level Name	Name of the software level. This object indicates the name of the software level.
Software Level Disclosure Date	Disclosure date for vulnerability for this software level. This object indicates the disclosure date for the security vulnerability information attached to this software level if this software level is of "Security Risk" compliance level. This object is meaningful only when paired with a software level.
Software Level Active	Status of this software level. This object indicates the current active or inactive status of this software level. This object is meaningful only when paired with a software level. (This object should report "Active" or "Inactive" in stead of the current "Y" or "N".)
Software Level Configuration Pattern	Configuration pattern for this software level. This object indicates the configuration pattern used to match against the current device configuration to determine if this software level compliance applies to a given device. This object is meaningful only when paired with a software level.
Software Level Driver Name	Device Driver name used with this level. This object indicates the device driver name used to access the device as part of the matching criteria for this software level. This object is meaningful only when paired with a software level.
Software Level Software Version	Version of software this level is matched against. This object indicates the version of the software running on the device as part of the matching criteria for this software level. This object is meaningful only when paired with a software level.
Software Level Compliance Level Name	Compliance rating of the software level. This object indicates the compliance rating attached to this software level, such as "Security Risk", "Gold" etc. This object is meaningful only when paired with a software level.
Policy Exceptions	Folder containing the objects related to policy exceptions.
Policy Excluded Device	Device excluded from this policy. This object indicates the device that is exempted from this policy applicability. This object is meaningful only when paired with a policy.
Rule Exceptions	Folder containing the objects related to rule exceptions
Rule Exception Expiration Date	Device excluded from this rule. This object indicates the device that is exempted from this rule applicability. This object is meaningful only when paired with a policy and a rule.
Rules	Expiration Date for an exception. This object indicates the expiration for a specific excep-

Object	Description
Excluded Device	tion granted to a device from this rule applicability. This object is meaningful only when paired with a policy, a rule and a device that is exempted from the rule.

NA Diagnostics

Object	Description
NA Diagnostics	Folder containing objects related to device diagnostic information
Diagnostic Create Date	This object indicates the date a diagnostic was created on. This object is meaningful when paired with a diagnostic.
Diagnostic Modified Date	This object indicates the date and time the diagnostic was last modified. This object thus is meaningful when paired with a diagnostic.
Diagnostic Text	This object indicates the logged text of the diagnostic event. This object thus is meaningful when paired with a device.
Diagnostic Type	This object indicates the type of the Diagnostic, such as Basic IP, Memory Troubleshooting, NA OSPF Neighbors etc.

NA Tasks

Object	Description
NA Task	Folder containing the objects related to NA task attributes
Task Name	This object reports the task name. This object thus is meaningful when paired with a task.
Scheduled By	This object indicates the login name of the person who scheduled the task (or the last user to modify the task). This object thus is meaningful when paired with a task.
Schedule Date	This object indicates the date and time when NA is scheduled to run the task. This object thus is meaningful when paired with a task.
Task Status	This object indicates the status of the task such as Paused, Pending etc. This object thus is meaningful when paired with a task.
Task Comments	This object indicates the comments entered by the user for the task. This object thus is meaningful when paired with a task
Task Result	This object indicates the result of the task that was run. This object thus is meaningful when paired with a task.
Approval Date	This object indicates the date the task was created. This object thus is meaningful when paired with a task.
Approval Status Name	This object indicates the approval status for the task such as Waiting Approval,Not Approved etc. This object thus is meaningful when paired with a task.
Task Run Date	The date on which the task was run.
Tasks By Run Date	When this filter is added, a date filter from the general class used in the query is applied to the tasks' run dates.

Object	Description
Tasks By Schedule Date	When this filter is added, a date filter from the general class used in the query is applied to the tasks' schedule dates.
Task Schedule Date Between	This filter prompts the user for a date range, which is used to filter tasks by their schedule dates.
Task Schedule Date	This filter will prompt the user for a single date which will be used to filter tasks by their schedule date.
Task Run Date Between	This filter will prompt the user for a date range which will be used to filter tasks by their run dates.
Task Run Date	This filter will prompt the user for a single date, which will be used to filter tasks by their run dates.

NA Events

Object	Description
NA Events	Folder containing the objects related to events in NA.
Event Date	This object indicates the date the event occurred on. This object thus is meaningful when paired with an event.
Event Summary	This object shows the first 4000 characters of the description of the event. This object thus is meaningful when paired with an event.
Event Added By	This object indicates the login name of the person who created the event. This object thus is meaningful when paired with an event.
Event Description	This object shows the first 4000 characters of the description of the event. This object thus is meaningful when paired with an event.

NA Users

Object	Description
NA Users	Folder containing the objects related to NA Users.
User Security	Folder containing the objects related user security attributes.
AAA User Name	This object indicates the AAA username that NA uses to log into devices and NA for this user. This object is thus meaningful when paired with an NA user.
Permission	This object indicates the Permission that the user have due to the user group memberships and roles granted to the user. This object is thus meaningful when paired with an NA user.
User Group	This object indicates the NA User Group that this user belongs to. This object is thus meaningful when paired with an NA user.
User Information	Folder containing objects related to user account attributes.

Object	Description
First Name	This object indicates the First Name associated with the user account. This object is thus meaningful when paired with an NA user.
Last Name	This object indicates the Last Name associated with the user account. This object is thus meaningful when paired with an NA user.
User Name	This object indicates the user name of an NA user account.
Email Address	This object indicates the email address associated with the user account. This object is thus meaningful when paired with an NA user.
User Comments	This object indicates the comments attached to the user account. This object is thus meaningful when paired with an NA user.

Cross Item Groups

Object	Description
Cross Item Groups	Cross Item Groups are groups that contain Server Automation and Network Automation data. Use these objects as filters or as report output when you want to create cross-BSA reports. These objects are configured in the Administration tab of BSA Essentials.
Cross Job Group	Cross Job Groups contain jobs and/or tasks from Server Automation and Network Automation. Use these objects as filters or as report output when you want to create cross-BSA reports. These objects are configured in the Administration tab of BSA Essentials.
Cross Job Group Name	The name of the Cross Job Group. This object is configured in the Administration tab of BSA Essentials.
Cross Job Group Description	The description of the Cross Job Group. This object is configured in the Administration tab of BSA Essentials.
ROI Attributes	
Cross Job Group ROI Label	The Return on Investment (ROI) label assigned to this Job Group; for example: hours, dollars or euros. This object is configured in the Administration tab of BSA Essentials.
Cross Job Group ROI Value	The Return on Investment (ROI) value assigned to this Job Group. This object is configured in the Administration tab of BSA Essentials.
Sum of Cross Job Group ROI Value	Numerical sum of ROI values for all tasks in one Cross Job Group instance. This object is configured in the Administration tab of BSA Essentials.
Cross Policy Group	Cross Policy Groups contain policies from Server Automation and Network Automation. Use these objects as filters or as report output when you want to create cross-BSA reports. These objects are configured in the Administration tab of BSA Essentials.

Object	Description
Cross Policy Group Name	The name of the Cross Policy Group. This object is configured in the Administration tab of BSA Essentials.
Cross Policy Group Description	The description of the Cross Policy Group. This object is configured in the Administration tab of BSA Essentials.
Cross Device Group	Cross device groups contain devices and device groups from Server Automation and Network Automation. Use these objects as filters or as report output when you want to create cross-BSA reports. These objects are configured in the Administration tab of BSA Essentials.
Cross Device Group Name	The name of the Cross Device Group. This object is configured in the Administration tab of BSA Essentials.
Cross Device Group Description	The description of the Cross Device Group. This object is configured in the Administration tab of BSA Essentials.

Appendix A: Index