HP BSA Essentials

For the Windows®, Linux, and Solaris operating systems

Software Version: 2.0

Administration Guide

Document Release Date: May 2010

Software Release Date: May 2010

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.

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/).

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" (on page 18). For information on how to enable a user account, see "Activating or Suspending User Accounts" (on page 20).

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 BSA Essentials Client " (on page 22)

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 "Setting Data Access Security Boundaries" (on page 21).

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.

Managing Users and User Groups

In BSA Essentials, group permissions control all user actions and access to viewing data in reports.

In order to user BSA Essentials features - such as create and view reports, to create Cross Item Groups, and so on - you need to creating users and then add them to groups. Once users have been added to groups, you can assign the appropriate permissions to the group so all its members can perform the actions allowed by the group's data access and application privileges.

Managing user and user groups consists of the following tasks:

- "First Time User and Group Setup" (on page 10)
- "Working with User Accounts" (on page 14) (Creating, Modifying, Deleting)
- "Creating User Groups" (on page 16) (Creating, Modifying, Deleting)
- "Assigning Permissions to Groups" (on page 20) (Application and Data Access Permissions)

First Time User and Group Setup

When you first install BSA Essentials, an admin user is created who has the credentials to log in to the application and set up user and group accounts. Before people can start using the product, the admin user must create user groups, add users to the groups, and then apply permissions to the groups.

If your BSA Essentials was setup using an external authentication system, then those users and groups will appear in the Administration tab of the client when you first log in.

Setting up users and groups in BSA Essentials requires performing (or understanding) the following topics:

- "Logging In To BSA Essentials Web Client" (on page 6) to BSA Essentials Web Client
- "The Admin User" (on page 12)
- "Default Users and Groups" (on page 18)
- "Permission Types" (on page 13)
- "Working with User Accounts" (on page 14)
- "Creating User Groups" (on page 16)
- "Assigning Permissions to Groups" (on page 20)

Importing Users From Server Automation

If you are using Server Automation (SA) as your user authentication system for BSA Essentials2.0, you can perform the following task in order to import all of your pre-existing users and user groups into BSA Essentials.

Importing users from SA requires performing the following tasks:

Adding the SA Authentication Source

1. Log in to the BSA Essentialscore server.
2. Change your user to become the BSA Essentials super user on the server. For example:

   ```
   su - omdb
   ```

3. Change directories to the following location:

   ```
   cd /opt/opsware/omdb/bin
   ```

4. Execute the following command:

   ```
   ./loginconfig.sh add
   ```

5. Select HP-SA.
6. When you are prompted for the "Auth Source Name", enter the FQDN for the SA server hosting the SA "twist" component.

Setting the 'User Importing Enabled' Property

1. Log in to the BSA Essentialscore server.
2. Change your user to become the BSA Essentials super user on the server. For example:

   ```
   su - omdb
   ```

3. Using a text editor, open the following file so you can edit it. For example:

   ```
   vi /etc/opt/opsware/omdb/omdb.properties
   ```

4. Set the following parameter to "`true`":

   ```
   com.opsware.cmdb.security.importusers.enabled=true
   ```

5. Save the file.
6. Change to the root user:

   ```
   su - root
   ```

7. Then restart the Restart the BSA Essentials core server:

   ```
   /etc/init.d/opsware-omdb restart
   ```

Note: SA user import into BSA Essentials is an ongoing process, supported by standard SA data mining.

Enabling LDAP Authentication

If you would like to configure BSA Essentials to use an external authentication system such as LDAP, you can do so by performing the following task. Note that after you perform this task to enable LDAP authentication, you still will need to create user and group account for your LDAP users. For more information, see "Working with User Accounts" (on page 14).

Configuring to Use an LDAP Authentication System:

1. Log in to the BSA Essentials core server.
2. Change your user to become the BSA Essentials super user on the server. For example:

   ```
   su - omdb
   ```

3. Change directories to the following location:

   ```
   cd /opt/opsware/omdb/bin
   ```

4. Execute the following command:

   ```
   ./loginconfig.sh add
   ```

5. Use a local administrative account to connect to the BSA Essentials core server.
6. Select LDAP from the list of choices.
7. The interview will ask you to enter values for the following parameters:
   - Host: The IP address or host name of LDAPserver
   - Enable SSL [yes]:
   - Port: The port used to connect to LDAP server
8. If the answer to Enable SSL is Yes, the following parameters need to be configured:
   - Full file name of server CA certificate: LDAP server certificate
   - Enable use client certificate [no]:
9. If the answer is yes, the following parameters need to be configured:
   - Full file name of client certificate: LDAP client certificate
10. After you have finished entering the values, exit the shell.

The Admin User

The admin user in BSA Essentials is created during installation and enables you to setup and manage users and groups and their permissions, as well as set up reporting data delivered with the product. The admin password is also set during install time, so to access this password consult your BSA Essentials administrator.

The BSA Essentials admin user is pre-configured to be able to perform all the necessary steps to allow your team to use the product, including:

- Access to all application and data permissions, and the ability to grant permissions to User Groups.
  - For more information, see "Permission Types" (on page 13) and "Assigning Permissions to Groups" (on page 20)
- Ability to create and delete users (except the admin user itself) and user groups
  - For more information, see "Working with User Accounts" (on page 14) and "Creating User Groups" (on page 16)
- Ability to create security boundaries in the BSA Essentials Client
  - For more information, see "Setting Data Access Security Boundaries" (on page 21)

Permission Types

InBSA Essentials, group permissions regulate the actions that users in group are able to perform, as well as control the types of data that a user can view in a report:

- An *application permission* allows members of a group perform specific actions, such as run reports, schedule reports, or manage report folders, and so on.
- A *data access permission* allows members of a group view specific kinds of data from the different automation applications. For example, you can allow a group to view Network Automation and Server Automation Device Groups, virtual servers, and so on.

For more information on setting security boundaries on data types, see "Creating Security Boundaries" (on page 24).

The following two tables list all of the application and data access permissions that you can add associate with a group.

Application Permissions

Application Permission Name	Actions
BSA Essentials Reporting Application	Create Web Intelligence Documents and running report queries using the InfoView Java reporting panel.
BIRT Reporting Enterprise Report Scheduling Management	Manage all BIRT report scheduling in the SAR Client. For more information, see "Logging In to the BSA Essentials Client" (on page 23).)
BIRT Reporting Personal Report Scheduling Management	Manage your own user's BIRT report scheduling in the SAR Client. For more information, see "Logging In to the BSA Essentials Client" (on page 23).)
Report Folder Access Control Management	Set permissions on report folders in the Document List in the Reporting panel.

Data Access Permissions

Data Access Permission Category	Data Types
ASAS (Storage Visibility and Automation)	Agent, Database, Disk Drive, Fibre Alias, Fibre Fabric, Fibre Zone, Fibre Zone Set, File System, Port, Port Controller, Replication Group, Service, Storage Device, Storage Extent, Storage Pool
Item Groups	Access to all Cross Item Group Data (Devices, Policies, and Jobs)
NAS (Network Automation)	Approval Rule, Configuration Policy, Configuration Rule, Core, Custom Script, Device, Device File System, Device Group, Device View, Event, Event Rule, Role, Satellite, Satellite Realm, Site, Software Image, Software Policy, Task, Task Types, Template, User, UserGroup,
PAS (Oper-	Flow Runs, Flows, Run Steps

Data Access Permission Category	Data Types
ations Orchestration)	
SAS (Server Automation)	Application Configuration, Application Installation, Audit, Audit Exclusion (exception), Audit Policy. Audit Result, Authentication Source, Business Applications, Customer, Facility, Feature, Folder, Job, Job Type, OPE (APX), Operating System, Patch Exception, Patch Policy, SMO, Security Boundary, Security Boundary EORV Value, Security Boundary Field Value, Server, Server Group, Snapshot, Software Package, Software Policy, User, User Group, Virtual Server

Folder Permissions

In the Document List of the reporting panel, each folder structure is governed by permissions that are controlled by the BusinessObjects Enterprise Central Management Console (CMC). For information on how to use the CMC, consult the BusinessObjects Enterprise.

A few rules to consider when working with folders in the Document List:

- Users may view all report results that are stored in folders that they have Read access to regardless of whether they have data permissions for the report results.
- A user's configured Data permissions are applied at the time that a report is run (not viewed).
- Users with the necessary permissions to modify permissions of report folders should pay close attention to the group permissions that they assign access to.
- Newly-created report folders by default inherit the permissions of the parent folder.

Working with User Accounts

Create user accounts for all people you want to be able to view, edit, create and run reports, create cross item groups, and so on.

Each newly-created user is placed automatically into the "Everyone" group, which by default has the "BSA Essentials Reporting Application" permission but no data permissions.

In order to receive permissions beyond the default reporting permissions, such as data access permissions and so on, you will need to add new users to groups and then assign permissions to those groups. "Creating User Groups" (on page 16)

"Creating User Groups" (on page 16)or instructions on how to create a user group, see "Creating User Groups" (on page 16) For more information on permission types, see "Permission Types" (on page 13)

Creating a user account consists of the following tasks:

Creating a User Account

To create a user account, perform the following steps:

1. From inside the BSA Essentials Web Client, select the Administration tab.
2. From the left side, under the Security folder, select Users.

3. On the right side of the page, select the new user button.
4. In the New User dialog, enter the following user information:
   - **First Name**: Must be at least two characters long.
   - **Last Name**: Must be at least two characters long.
   - **Full Name**: Enter user's full name.
   - **Authentication Source**: If your BSA Essentials core has more than one authentication source configured, then you can choose from this list. If you choose LDAP as your authentication source, your user will be asked for a Distinguished Name (DN) instead of a password. The format of the DN needed will depend on the LDAP or Active Directory server configuration. For more information on configuring an LDAP authentication source for BSA Essentials, see "Enabling LDAP Authentication" (on page 11).
   - **Email**: This is a required field.
   - **Username**: Username must be at least four characters long and contain no special characters.
   - **Password**: Password can contain regular and special characters.
5. Click **Save**.

Changing Login Password

To change a user's login password, perform the following steps:

1. From the BSA Essentials Administration tab, select Security → Users.
2. Select a user.
3. Below the user, select the Login tab.
4. Enter the new user password twice.
5. Click Save (far right of lower pane) to save your changes.

Modifying Group Membership

To modify a user's group membership, perform the following steps:

1. From the BSA Essentials Administration tab, select Security → Users.
2. Select a user.
3. Below the user, select the Group Membership tab.
4. To assign the user to a group, click the Add icon.
5. In the Add Group dialog, select the check box next to the group name you want to add the user to and click **Add**. (Do this for every group you want to add the user to.
6. Click **OK**. The user's profile Group Membership displays all the group the user is a member of.
7. To remove the user from a group, select the check box next to the user's name and then click the remove icon.
8. Click the Save button (far right of lower pane) to save your changes.

Editing User Preferences

To edit a user's preferences, such as time zone and data format, perform the following steps:

1. From the BSA Essentials Administration tab, select Security → Users.
2. Select a user.
3. Below the user, select the Preferences tab.
4. From the Time Zone selector, choose a time zone appropriate to your location.
5. From the Long Date Format selector, select a date format for when the user interface displays the full date
6. From the Short Date Format selector, select a date format for when the user interface displays a shortened date.
7. Click the Save button (far right of lower pane) to save your changes.

Creating User Groups

In BSA Essentials, all user permissions are applied to user groups. When you add permissions to a group, and then add users to the group, all users that belong to the group receive all the permissions associated with the group. With group (or often called "role-based authentication") you can create groups of users that you want to be able to perform specific actions and access specific data.

Creating user groups consists of the following tasks:

Creating a User Group

To create a user group, perform the following steps:

1. From inside the BSA Essentials Web Client, select the Administration tab.
2. From the left side, under the Security folder, select Groups.
3. On the right side of the page, select the New Group button.
4. In the New Group dialog, enter a Name and Description (optional) for the group, and then click **Save**.

Adding Users to a Group

To add users to a group, perform the following steps:

1. From inside the BSA Essentials Web Client, select the Administration tab.
2. From the left side, under the Security folder, select Groups.
3. On the right side of the page, select the group you want to add members to and click the Add Users button.
4. In the add User dialog, select a user or multiple users and then click **Add**. (To select multiple users, you can select hold SHIFT or CTRL while you select).
5. When you are finished adding users, click **OK**.
6. Click **Save** (far right of lower pane) to save your changes.

Adding Application Permissions to a Group

For more information on application permissions, see "Permission Types" (on page 13)

To add application Permissions to a group, perform the following tasks:

1. From the BSA Essentials Administration tab, select Security → Groups.
2. Select a group you want to add application permissions to.
3. Below the group, select the Application Permissions tab.
4. Click the Add Application Permission ✚ button.
5. In the Add Application Permission dialog, select a feature name by click the checkbox next to the name. You can use CTRL + select or SHIFT + select to select more than one permission to add to the group.
6. To add the selected application permissions, click **Add**.
7. Click **Save** 💾 (far right of lower pane) to save your changes.

Adding Data Access Permissions to a Group

Fore more information on data access permissions, see "Permission Types" (on page 13)

1. From the BSA Essentials Administration tab, select Security → Groups.
2. Select a group you want to add application permissions to.
3. Below the group, select the Data Access Permissions tab.
4. Click the Add Data Access Permission ✚ button.
5. In the Add Data Permission dialog, you select All Data Permissions to add access to all data for the group.
6. To add specific data access permissions, from the Item Type drop-down list, select a data item type.
7. If the data type has any security boundaries associated with it, then you will be able to select from one of the item listed under the main data type. For more information on creating data item security boundaries, see "Setting Data Access Security Boundaries" (on page 21)
8. To add the selected application permissions, click **Add**.
9. Click **Save** 💾 (far right of lower pane) to save your changes.

Adding Users To Groups

After you create a group, you need to add users to the group.

For more information on assigning permissions to groups, see "Assigning Permissions to Groups" (on page 20)

Adding Users to a Group

To add users to a group, perform the following steps:

1. From inside the BSA Essentials Web Client, select the Administration tab.
2. From the left side, under the Security folder, select Groups.
3. On the right side of the page, select the group you want to add members to and click the Add Users ✚ button.
4. In the add User dialog, select a user or multiple users and then click **Add**. (To select multiple users, you can select hold SHIFT or CTRL while you select).

5. When you are finished adding users, click **OK**.
6. Click **Save** (far right of lower pane) to save your changes.

Default Users and Groups

When you install BSA Essentials Web Client and log in for the first time, some default users and user groups are already created. These user groups and users help you get started using the product and setting up user accounts so your team can start using the product.

Default Users

By default, two users are created during installation (these user account names are all lower case, and are case-sensitive):

- **admin**: The admin user is the first user that is created during installation, is given automatic group membership to the default user groups, and has the ability to create users and groups and grant all permissions. This user is also granted extra permissions that no other user has that enables this user to configure BSA Essentials, such as setting security boundaries for data items from the BSA Essentials Client. The admin account cannot be deleted.
- **guest**: A basic user who is created during installation, but with its account disabled. This account can be used for generic users who may not be typical BSA Essentials users but who may need access to reports. This account needs to be activated to be functional and cannot be deleted.

Default User	Description
"admin"	The first-time user created upon installing the product, which enables you to set up all other user accounts, user groups, permissions, cross item groups, and so on.
Group Membership	Everyone, System-Administrators
Hidden permissions	Access to the Admin console Access to the BSA Essentials Client and ability to set security boundaries on data items

Default User	Description
"guest"	This account allows any user to log in to the BSA Essentials Web Client. This account is disabled by default. For information on how to activate a user account, see "Activating or Suspending User Accounts" (on page 20).
Group membership	Guest

Default Groups

By default, there are three user groups created during install that the admin user can use to setup the kinds of users that can access the BSA Essentials features:

- **Everyone**: Default group designed for permissions you want all users to have.
- **Guest**: Default group designed for guest users who might need to access Reports. By default, this account is disabled.
- **System-Administrators**: Default group designed for BSA Essentials super users.

Default User Group	Description
"Everyone"	
Application Permissions	BSA Essentials Reporting Application
Data Access Permissions	None
Hidden Permissions	Access to the BSA Essentials Client, but no ability to set security boundaries on data items
Default Member	admin

Default User Group	Description
"Guest"	
Application Permissions	BSA Essentials Reporting Application
Data Access Permissions	None
Default Member	guest

Default User Group	Description
"System-Administrators"	
Application Permissions	BSA Essentials Reporting Application BIRT Reporting Enterprise Report Scheduling Management BIRT Reporting Personal Report Scheduling Management Report Folder Access Control Management
Data Access Permissions	All
Hidden Permissions	Access to the BSA Essentials Client and ability to set security boundaries on data items
Default Member	admin

Activating or Suspending User Accounts

If you need to block access for a user account, you can suspend the account.When a user account is suspended, that user will not be able to log in to the BSA Essentials Web client.

If you want the user to have access, you can activate the user account, and then the user will be able to log in to BSA Essentials.

To suspend or activate a user account, perform the following steps:

1. From inside the BSA Essentials Web client, select the Administration tab.
2. From the left side, under the Security folder, select Users.
3. From the Users list, select the user account you want to suspend.
4. Click **Suspend** at the top of the user list.
5. When the user account is suspended, the user icon has a red X through it ✗.
6. To reactivate the account,select the user and click **Activate**.

Assigning Permissions to Groups

In order for your BSA Essentials users to be able to perform actions (create and run reports, view the right data in reports, and so on), they need to belong to a group or groups that have permissions associated with it. All user actions and access to data in reports and the Dashboard are controlled by group permissions.

There are two kinds of permissions you can apply to groups to allow your users to access BSA Essentials features:

- An *application permission* allows members of a group perform specific actions, such as run reports, schedule reports, or manage report folders, and so on.
- A *data access permission* allows members of a group view specific kinds of data from the different automation applications. For example, you can allow a group to view Network Automation and Server Automation Device Groups, virtual servers, and so on.

For more information on permissions, see "Permission Types" (on page 13).

For more information on creating data item security boundaries, see "Setting Data Access Security Boundaries" (on page 21)

Assigning Application Permissions to a User Group

To assign application permissions to a group, perform the following steps:

1. From the BSA Essentials Administration tab, select Security → Groups.
2. Select a group you want to add application permissions to.
3. Below the group, select the Application Permissions tab.
4. Click the Add Application Permission ✚ button.

5. In the Add Application Permission dialog, select a feature name by click the checkbox next to the name. You can use CTRL + select or SHIFT + select to select more than one permission to add to the group.
6. To add the selected application permissions, click **Add**.
7. Click **Save** 💾 (far right of lower pane) to save your changes.

Assigning Data Access Permissions to a User Group

To assign data access permissions to a group, perform the following steps:

1. From the BSA Essentials Administration tab, select Security → Groups.
2. Select a group you want to add application permissions to.
3. Below the group, select the Data Access Permissions tab.
4. Click the Add Data Access Permission ➕ button.
5. In the Add Data Permission dialog, you select All Data Permissions to add access to all data for the group.
6. To add specific data access permissions, from the Item Type drop-down list, select a data item type.
7. If the data type has any security boundaries associated with it, then you will be able to select from one of the item listed under the main data type. For more information on creating data item security boundaries, see "Setting Data Access Security Boundaries" (on page 21)
8. To add the selected application permissions, click **Add**.
9. Click **Save** 💾 (far right of lower pane) to save your changes.

Setting Data Access Security Boundaries

Data Access permissions in BSA Essentials allow you to control the types of data your users will be able to see and use inside of reports. Creating *security boundaries* around data items allows you to control the exact type of data item and the exact kinds of attributes related to the item.

Note: In this release, security boundaries are created in the BSA Essentials Client.

For example, if your implementation of BSA Essentials is configured to work with Server Automation (SA) , you very likely want your users to be able to report on SA servers.

Granting data access permissions to SA servers and NA devices is probably too general and would yield too much information in reports. You might want a specific BSA Essentials user group to be able to report on and display a specific set of servers and of those servers, only be able to see specific server attributes. To achieve this, you would create security boundaries for the Server data item.

For example, using theBSA Essentials Client you might only want users in a group to be able to report on SA virtual servers from a specific Customer and Facility, only list server information regarding hostname, open ports, and only those servers that yield more than five failed checks when they are scanned during a compliance audit.

Once you create the security item in the BSA Essentials Client, you can see the security boundary when you create a data access permission in the BSA Essentials Web Client.

In order to create security boundaries, you need to perform the following tasks:

- "Installing the BSA Essentials Client " (on page 22)
- "Logging In to the BSA Essentials Client" (on page 23)

- "Creating Security Boundaries" (on page 24)

Installing the BSA Essentials Client

In order to access the BSA Essentials Client you need to download and install the BSA Essentials Client Launcher. You can find the link to download the BSA Essentials Client Launcher on the BSA Essentials Web Client home page, just beneath the login fields.

Installing the BSA Essentials Client requires performing the following tasks:

Learn About the BSA Essentials Client and BSA Client Launcher

The BSA Client Launcher is a self-contained Java application that allows you to access the BSA Essentials Client from any BSA Essentials core. You can use the Launcher to log in to and download the latest version BSA Essentials Client. If the BSA Essentials Client has been upgraded on a specific BSA Essentials server, you can choose the server you would like to use for downloading the BSA Essentials Client.

The BSA Essentials Client Launcher also allows you to configure advanced settings, such as debug settings, locale settings, and access to the Java Web Start that runs the Launcher and BSA Essentials Client.

The BSA Essentials Client is a Java application that installs and runs with its own Java Runtime Environment (JRE). TheBSA Essentials Client will not interfere with any other versions of JRE you may have installed on your system. The JRE will not be used (and is not usable) by any other Java application on the target computer, and it will not set itself as the default JRE on the target computer.

Understand BSA Essentials Client System Requirements

The BSA Essentials Clientis supported on the following operating systems:

- Windows 2003
- Windows 2000
- Windows XP
- Windows Vista

The minimum systems requirements to run the BSA Essentials Client are as follows:

- Minimum 1 GB of DRAM
- Minimum 100 MB of disk space

If using theBSA Essentials Client to connect to a core over a residential DSL connection, a minimum 384 Kbps DSL connection is recommended.

You need to be logged in as a user that has sufficient permissions to install software on the computer. (You do not need to be an administrator user to install the launcher.)

To run the SAR Client, you must download and install the BSA Essentials Client Launcher (accessible from the BSA Essentials Web Client). In order to install the BSA Essentials Client Launcher, you must be a Windows user that is able to install applications on your system.

Install the BSA Client Launcher

In order to run the BSA Essentials Client, you need to download and install the BSA Client Launcher, which is a Java application that allows you to access the BSA Essentials Client from any BSA Essentialsserver. When you install the BSA Client launcher, it installs all the necessary Java applications (Java Web Start and JRE) you need to run the BSA Essentials Client.

If you plan to have multiple users install the BSA Client Launcher on the same computer, we recommend that each user choose a unique path to install the application. For example, if one user has already installed the BSA Client Launcher in the default location, C:\Program Files\HP BSA\Launcher, then if another user logs in to the same computer and attempts to install to that same default location, they will see an error and not be able to install. If this occurs, choose a new location.

To install the BSA Essentials Client Launcher, perform the following steps:

1. Open a Web browser, and enter the URL to the BSA EssentialsWeb Client server. For example: <`https://<bsae-servername:8443`>.
2. On the BSA EssentialsWeb Client home page, under the log in fields, click the Download BSA Launcher link.
3. Download the HP BSA Launcher installation file and double-click to start the launcher installation.
4. In the Welcome window, click **Next**.
5. In the License Agreement window, select the “I accept the agreement” option, and then click **Next** to proceed with the installation.
6. In the Select Destination Directory window, accept the default installation directory, or click **Browse** to select a custom location. Click Next.
7. In the “Select clients to install” window, select HP Service Automation Reporter Client.
8. In the Select Start Menu Folder window, accept the default name and click Next.
9. In the Select Additional Tasks window, accept the default options or choose your own, and then click Next to install the SAR Client Launcher.
10. When the installation has completed, click Finish to exit.

Uninstall the BSA Client Launcher - Optional

You can uninstall the BSA Client Launcher using the Windows Add or Remove Programs utility located in the control panel on your system.

To uninstall the BSA Client Launcher, perform the following steps:

1. From the Start menu, select Control Panel.
2. Double-click the Add or Remove Programs application.
3. In the Currently Installed Programs table, select the HP BSA Launcher application.
4. Click **Remove**.
5. Close the Add or Remove Programs application.

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 "Setting Data Access Security Boundaries" (on page 21).

Creating Security Boundaries

From inside the BSA Essentials Client, you can create security boundaries around data items, which allows you to restrict the kinds of data item attributes that users in BSA Essentials can report on.

When you create security boundaries around data items from inside theBSA Essentials Client, those security boundaries become available when you create *data access* permissions in the BSA Essentials Web Client and apply those permissions to user groups.

For example, you might only want users in a group to be able to report on SA virtual servers from a specific Customer and Facility, only list server information regarding hostname, open ports, and only those servers that yield more than five failed checks when they are scanned during a compliance audit.

You could create security boundaries for each of these restrictions using the BSA Essentials Client, and then using the BSA Essentials Web Client, you can apply those security boundaries to a group through data access permissions.

Configuration Items and Their Attributes

The following terms are important to know when setting BSA Essentials security boundaries on data items:

- **Configuration Item**: An object which can be viewed and managed with BSA Essentials. For example SA Server, NA Device, SA Patch Policy, and so on.
- **Attribute**: A single property of a configuration item, the value of which describes the behavior of the item. Configuration items can have one or more attributes. For example, some of the attributes for the configuration item SA Server includes hostname, life cycle, agent status, and management IP.

A custom attribute is displayed only with the data Item it is defined with. For example, a custom attribute of a Facility is not displayed when viewing a Server that is a member of that facility.

Create Security Boundaries for Data Access Permissions

To create security boundaries in the BSA Essentials Client, perform the following steps:

1. "Logging In to the BSA Essentials Client" (on page 23).
2. From the **View** menu, select **Opsware Administration** → **Security Boundaries**.
3. From the Define Security Boundary around Configuration Item drop-down list, select a data item. For example, SAS Server (SA server).
4. In the Match the following criteria section, from the drop-down lists, select an Attribute (for example, Hypervisor), an operator (equals, contains, does not contain, and so on), and parameters for the security boundary.
5. Depending upon the operator selected, you might have to enter a value, text, or select from a list of values. In the text field, type the appropriate value.
6. (Optional) Click + to define a second criteria. (You can create as many rules as you want.)
7. Click Preview Security Boundary to view the current items defined within the security boundary.
8. Click **Save** to save the security boundary. Once the security boundary is saved, it becomes available as a data access permission item in the BSA Essentials Web Client. For information on how to assign data access permissions on groups in the BSA Essentials Web Client, see "Assigning Permissions to Groups" (on page 20).

Configuring Cross Device, Policy, and Job Groups

Cross Device, Policy, and Job Groups allow you to make cross-product groupings of various devices, policies, and jobs from each of the BSA products deployed in your data center — Server Automation (SA), Network Automation (NA) and Operations Orchestration (OO) — so that you can control the information provided to you in BSA Essentials reports.

For example, you might be responsible for a high profile business application in your data center. You want to be able to report on all the servers and devices that comprise the application; to make sure that these devices meet the specific compliance criteria defined by your organization; and to see how well these devices are delivering the return on investment you expect from the application those devices support..

You can achieve this result by creating a Cross Device Group for all of the devices (servers, network devices, and storage devices) that make up the application, create a Cross Policy Group that contains audits and software policy checks on the servers and devices, and create a Cross Job Group that provides job results for each compliance audit.

There are three kinds of groups types in BSA Essentials:

- **"Creating Cross Device Groups" (on page 26)**: Allow you to group together devices of the BSA product suite deployed in your data center and use in reports. For example, you can use a Cross Device Group to such as servers and device groups from SA and, network devices and device groups from NA.
- **"Creating Cross Policy Groups" (on page 27)**: Allow you to group together important policies from the BSA product suite deployed in your data center and use them in your reports.
- **"Creating Cross Job Groups" (on page 27)**: Allow you to group together important job types from the BSA product suite deployed in your data center and use them in your reports.

Creating Cross Device Groups

Cross Device Groups allow you to group together devices and device groups from both Server Automation (SA) and Network Automation (NA). Once you group together devices and device groups, these groups can be used in reports.

For more information on using Cross Device Groups in reports, see

Create a Cross Device Group

To create a Cross Device Group, perform the following steps:

1. From inside the BSA Essentials Web Client, select the Administration tab.
2. From the left side, under the Configuration folder, select Cross Device Groups.
3. In the right side of the window, click the New Device Group icon.
4. In the New Cross Device Group dialog, enter a name and description for the group, and then click **Save**.
5. To add items to the group, select the new group from the list.
6. Below the group , select the General and Devices and Device Groups tab.
7. Click **Add**✚ to add devices or device groups to the group.

8. In the Add Device/ Groups dialog, select the type of device from the Item Type drop-down list. For example, NAS Device, SAS Server Group, and so on.
9. Once the list has been populated with items, to select an item to add to the group, select the check box next to the name of the item,
10. Click **Add**. Repeat as many times as needed for all the item types you want to add to the device group.
11. When you have finished selecting items to the group, click **OK**.
12. Click **Save** (far right of lower pane) to save your changes.

Creating Cross Policy Groups

Cross Policy Groups allow you to group together policies from Network Automation (NA) and Server Automation (SA). Specifically, you can combine NA Configuration Policies, SA Application Configurations, Audits, Patch Policies, and Software Policies into individual groups.

Once you create a Cross Policy Group, it can be used in reports. For more information on creating reports, see "Creating a Report".

Create a Cross Policy Group

To create a Cross Policy Group, perform the following steps:

1. From inside the BSA Essentials Web Client, select the Administration tab.
2. From the left side, under the Configuration folder, select Cross Policy Groups.
3. In the right side of the window, click the New Policy Group icon.
4. In the New Cross Policy Group dialog, enter a name and description for the group, and then click **Save**.
5. To add items to the group, select the new group from the list.
6. Below the group, select the Policies tab.
7. Click **Add** to add polices to the group.
8. In the Add Policy dialog, select a policy type from Item Type drop-down list. For example, NAS Configuration Policy, SAS Application Configuration, SAS Audit, and so on.
9. Once the list has been populated with items, to select an item to add to the group, select the check box next to the name of the item,
10. Click **Add**. Repeat as many times as needed for all the item types you want to add to the policy group.
11. When you have finished selecting items to the group, click **OK**.

Creating Cross Job Groups

Cross Job Groups allow you to group together important job types from the BSA product suite deployed in your data center and use them in your reports.

For example, you can create groups and add such diverse job types as NA Tasks like Backup Device Software, Check Policy Compliance, Data Pruning; and such SA jobs as Audit Server, Remediate Software Policy, Agent Communications Test, Install Software, and so on.

Additionally, you have the ability to set an ROI (return on investment) unit for all Cross Job Groups, which allows you to indicate the value you are getting from the jobs being run by the BSA software suite. For example, you could set the ROI unit to dollars, and when you create and configure a Cross Job Group, you can specify a value amount for the group which will be labeled in dollars. For information on setting the Cross Job Group ROI unit, see "Setting Cross Job Groups ROI Unit" (on page 28)

Note: ROI unit applies globally across all job groups, but each group can be set with a unique ROI value

For more information on creating reports, see "Creating a Report".

Create a Job Group

To create a Cross Job Group, perform the following steps:

1. From inside the BSA Essentials Web Client, select the Administration tab.
2. From the left side, under the Configurations folder, select Cross Job Groups.
3. In the right side of the window, click the New Job Group icon.
4. In the New Cross Job Group dialog, enter a name and description for the group, and then click **Save**.
5. Select the new group from the list, and below the group, select the General tab.
6. In the ROI Multiplier field, enter a value for the label. For example, if your global ROI unit was set to dollars, you could enter 500 for this group to indicate how much money is saved when the jobs in this group run successfully.
7. Next, to add job types to the group, select the Jobs tab and then click **Add**.
8. In the Add Job dialog, select a job type filter, such as NAS Job Types or SAS job Types.
9. Once the list has been populated with job items, to select an item to add to the group, select the check box next to the name of the item and then click **Add**. Repeat as many times as needed for all the item types you want to add to the job group.
10. When you have finished selecting items to the group, click **OK**.
11. Click **Save** (far right of lower pane) to save your changes.

Setting Cross Job Groups ROI Unit

Before you create and configure Cross Job Groups, you want to set an ROI (return on investment) unit for all job groups. The Cross Job Group ROI unit allows you to indicate the value you are getting from the jobs being run by the BSA software suite.

For example, you could set the ROI unit to dollars, and when you create and configure a Cross Job Group, you can specify a value amount for the group which will be labeled in dollars. Or, you might want to represent the savings created running specific jobs in time, as in how many hours were saved when a group of related jobs run successfully.

Note: ROI unit applies globally across all job groups, but each group can be set with a unique ROI value.

Set Cross Job Groups ROI Unit

To set the Cross Job Group ROI unit, perform the following steps:

1. From inside the BSA Essentials Web Client, select the Administration tab.
2. From the left side, under the Configurations folder, select Cross Job Groups.
3. At the top of the Job Groups list, click **Set ROI Unit**.

4. In the Specify Return on Investment Unit dialog, enter the label for units to be expressed for all Cross Job Groups. For example, you can set "dollars" or "hours" or any unit label you wish.
5. Click OK. The ROI unit label has been set for all Cross Job Groups. For information on how to create a Cross Job Group and set the ROI unit value for a group, see "Creating Cross Job Groups" (on page 27)

Core Administration

This section contains important tasks you can perform for making sure your BSA Essentials core is working well, and contains the following topics:

- "Importing Users From Server Automation" (on page 10)
- "Enabling LDAP Authentication" (on page 11)
- "Configuring BSA Essentials Ports" (on page 30)
- "Enabling Actionability in BSA Essentials Reports"
- "Core Administration Scripts" (on page 31)
- "Enabling Actionability of OO Flows in BSA Essentials"

Configuring BSA Essentials Ports

After you have installed BSA Essentials you might need to change some of the port numbers being used by the BSA Essentials core or database. This section shows you how to change port numbers for both product components.

Changing BSA Essentials Default Ports:

BSA Essentials configuration is retained in `omdb.properties`, and also in the response file created or modified during an installation or upgrade of BSA Essentials. The installer will use these values to setup the configuration rather than requiring the user to modify the scattered files throughout BSA Essentials.

To change the BSA Essentials default ports, perform the following steps:

1. Log in to the BSA Essentials server.
2. sing a text editor, open the BSA Essentials response file from the most recent installation or upgrade on the server. The default location and name of the BSA Essentials response file is:

   ```
   /usr/tmp/oiresponse.omdb
   ```

3. Edit the oiresponse.omdb file to the custom port preferred for the port number, and then save the file.
4. Type the following command:

   ```
   upgrade_opsware -r response_file
   ```

   to set the port parameters from the edited response file.

Changing BSA Essentials Database Port

By default BSA Essentials uses port 1521 to connect BSA Essentials Core services to the BSA Essentials database. Because the BSA Essentials database port is not set during the installation the port number is not part of the BSA Essentials response file, and you cannot change the BSA Essentials database port using the steps in Changing SAR Default Ports.

To change the database port number used by BSA Essentials, perform the following steps:

1. Log in to the BSA Essentials Core server.

2. To shut down the BSA Essentials Core, enter the following command:

   ```
   /etc/init.d/opsware-omdb stop
   ```

3. For each of the files in the following list, open the file using a text editor, change the database port from the default value of 1521 to the required value, and save the file.

   ```
   /etc/opt/opsware/omdb.properties
   ```

   ```
   /opt/opsware/omdb/bin/dmconfig.
   ```

   ```
   /opt/opsware/omdb/deploy/cmdb-admin-ds.xml
   ```

   ```
   /opt/opsware/omdb/deploy/cmdb-ds.xml
   ```

   ```
   /opt/opsware/omdb/deploy/omdb-reporter-ds.xml
   ```

4. To start the BSA Essentials Core, enter the following command:

   ```
   /etc/init.d/opsware-omdb start
   ```

Core Administration Scripts

The following section lists a collection of useful BSA Essentials scripts and tasks that help you with your core administration:

- "Starting and Stopping the Core" (on page 31)
- "Dataminer Watchdog Script" (on page 32)
- "Changing the BSA Essentials Admin Password" (on page 32)
- "BSA Essentials Core Diagnostic Script" (on page 33)
- "SA Compliance Universe Nightly Job Scripts" (on page 34)
- "Oracle User Connectivity Diagnostic Script" (on page 35)
- "Unlocking Oracle User Accounts" (on page 35)
- "Database Pruning Scripts" (on page 35)

Starting and Stopping the Core

The `opsware-omdb` script enables you to start, stop, or restart your BSA Essentials core. You can also use this script to check the current status of your core, the core version number, and more. You must log in as root to run this script.

The script is installed to the following directory:

```
/etc/init.d/opsware-omdb
```

Syntax

```
opsware-omdb <option>
```

Note: If you are restarting a core in a dual server configuration (one server runs the BSA Essentials and the other runs Oracle), make sure that your Oracle database server and all its processes are running before restarting the BSA Essentials core server.

Options

The `opsware-omdb` script has the following command line options:

- `start` - Starts the BSA Essentials core.
- `stop` - Stops the BSA Essentials core.
- `startsync` - Starts the core and the prompt is not returned until the core is fully started.
- `restart` - Restarts the BSA Essentials core.
- `list` - Lists the services that are run by the opsware-omdb script (core and rsync)
- `status` - Gives the current status of BSA Essentials services of running or not running. Also the PID of the process is displayed if the service is running.
- `version` - Displays installation build version numbers for the installed components and the Meta schema and data versions of the BSA Essentials database.
- `help` - Lists full set of command options and syntax.

Dataminer Watchdog Script

The `dmwatch.sh` script allow you to perform different administrative tasks for your BSA Essentials Data Miner, such as restarting your data miner if it quits unexpectedly.

Syntax

```
./dmwatch.sh --<option>
```

This script is located on the BSA Essentials core at `/opt/opsware/omdb/contrib`. This script is intended to work with any supported BSA Essentialsdata miner.

Options

- `dm_home` - Lists the home directory of the dataminer.
- `auto` - Starts or restarts restart the dataminer and rsync if any problems are detected .
- `on_db` - Adds extra transaction information to the output (only use if your BSA Essentials uses the SA database) .
- `append` - Appends information to `dmwatch_laststatus` instead of replacing the information

Changing the BSA Essentials Admin Password

The following script allows you to reset the password for the BSA Essentials administrator.

```
reset_admin_password.sh
```

Syntax

```
./reset_admin_password.sh
```

After you execute the script, follow the steps provided in the output.

Example

1. Log in to the BSA Essentials core server.
2. Change directories to the following path:

   ```
   /opt/opsware/omdb/contrib
   ```

3. Execute the following command:

   ```
   ./reset_admin_password.sh
   ```

4. Edit the file `/etc/opt/opsware/omdb/.properties` and set the following parameter:

   ```
   com.opsware.cmdb.security.allow_internal_user_modification_enabled=true
   ```

5. Restart the BSA Essentialscore by executing the following command:

   ```
   /etc/init.d/opsware-omdb restart
   ```

   Wait for the BSA Essentials system to start completely.

6. Edit the following file `/etc/opt/opsware/omdb/.properties` and set the set the following property:

   ```
   com.opsware.cmdb.security.allow_internal_user_modification_enabled=false
   ```

   Login to BSA Essentials AdminConsole as admin/ and change password for admin to the desired one

Tip: To use a SID other than the default "cmdb", define ORACLE_SID before running this script. For example:

```
export ORACLE_SID=mycmdbsid; ./unlock_oracle_accounts.sh
```

BSA Essentials Core Diagnostic Script

The following script provides useful diagnostic information about your BSA Essentials core, such as environment and runtime information, and more:

```
scene_snap.py
```

This script also provides the following troubleshooting about your BSA Essentialscore: logs, file listings, BSA Essentials environment properties, JBoss Configuration, install info, running processes, platform, memory, CPU, storage, file handles, hostname, interfaces, network statistics (netstat output), database version, Oracle free space and memory structures, load info, data sources, ETL information, and other useful BSA Essentials parameters.

This script is located on the BSA Essentials core at `/opt/opsware/omdb/contrib`.

Syntax

```
./scene_snap.py
```

SA Compliance Universe Nightly Job Scripts

The following scripts allow you to understand, troubleshoot, and modify the regularly scheduled SA compliance fact table calculation used in the SA Compliance Universe.

- `bsae_run_nightly_job.sh` - allows you to view current SA Compliance data in your reports that have not yet been picked up by the latest table calculations.
- `bsae_set_max_fact_days.sh` - allows you to change how many days worth of calculated SA compliance data that the BSA Essentials database can store. (Default is 30 days.)

These scripts are located on the BSA Essentials core at `/opt/opsware/omdb/contrib` directory.

Note: Make sure that you do ***not*** use the script named `bsae_setup_nightly_compliance_job.sh`.

Running Nighty Fact Table Calculation Job

BSA Essentials stores calculated SA compliance data for 30 days. By the default, the calculation job is run at midnight daily. However, if you have made some compliance data changes in SA and you want these changes to be reflected in the compliance reports that are built from the SA compliance universe, then you need to invoke the calculation job in order to see the changes before the following day when the job is run at midnight.

The `bsae_run_nightly_job.sh` script will do the calculation for SA compliance data for a specific number of days depending on the input. For example:

```
/opt/opsware/omdb/contrib/bsae_run_nightly_job.sh
```

Setting Maximum Number of Days Compliance Data is Stored

Also by default, BSA Essentials the job only stores up to 30 days calculated compliance data, which means that SA compliance reports that use data from the SA Compliance Universe can only display 30 days of history. So if you want to report more on data for more than 30 days, then you can run `bsae_set_max_fact_days.sh` to set the number of days that BSA Essentials will store for calculated compliance data.

For example, if you want to set the maximum number days of stored data (60 days), and you already have more than 60 days worth of SA data mined into BSA Essentials, then you can run the `bsae_set_max_fact_days.sh` first to increase the number to 60, by performing the following steps:

1. Change directories to the following location:

   ```
   /opt/opsware/omdb/contrib
   ```

2. Then execute the following script:

   ```
   ./bsae_set_max_fact_days.sh 60
   ```

3. Then you need to run the calculation from the past 30 days to past 60 days, since by default, you will have the history for past 30 days:

   ```
   ./ bsae_run_nightly_job.sh 30 60
   ```

4. Or you could alternately run this command:

   ```
   ./ bsae_run_nightly_job.sh 60
   ```

   The script will calculate for past the past 60 days.

Oracle User Connectivity Diagnostic Script

The following script helps you validates that your BSA Essentials users can log in and have the appropriate permissions, as defined in their user profile:

```
test_datasource_accounts.sh
```

This script is located on the BSA Essentials core at `/opt/opsware/omdb/contrib`. directory.

Syntax

```
./test_datasource_accounts.sh
```

Unlocking Oracle User Accounts

This script allows you to unlock the user accounts if the event ever occurs.

```
unlock_oracle_accounts.sh
```

For example, by default a user with an Oracle account will be locked out after 10 unsuccessful login attempts. This script allows you to reset the account so the user can log in to BSA Essentials.

This script is located on the BSA Essentials core at `/opt/opsware/omdb/contrib`.

Syntax

```
./unlock_oracle_accounts.sh
```

Tip: To use a SID other than the default "cmdb", define ORACLE_SID
before running this script. For example:

```
  export ORACLE_SID=mycmdbsid; ./unlock_oracle_accounts.sh
```

Database Pruning Scripts

The following two scripts allow you to purge your BSA Essentials database of old or unneeded data and table, which can help your core can run more efficiently.

- `delete_datatables.sql`
- `purge_sar_data.sh`

These two scripts are located on your BSA Essentials core in the following directory:

```
/opt/opsware/omdb/contrib
```

Use these two scripts to do the following tasks:

- Purge all data from `cmdb_data` and related `cmdb_meta` data tables for a given data source

  Or,

- Purge all data from `cmdb_data` and related `cmdb_meta` data tables for a given data source if the data is longer than X number of days in the database.

Note: You can only purge data from the database on a per-data source basis. In other words, if you are running an SA data miner and an NA data miner, you need to run the scripts for each data source. For more information about stopping and starting data miners, see the BSA Essentials Installation Guide.

Note: These scripts are only supported in a single server deployment where both the BSA Essentials core services and database components are installed on the same server.

Purging All Data from YourBSA Essentials Database

1. Log in to the BSA Essentialscore server as root.
2. Copy the two scripts `delete_datatables.sql` and `purge_sar_data.sh` from:

   ```
   /opt/opsware/omdb/contrib
   ```

   to

   ```
   /opt/opsware/omdb/bin
   ```

3. Set the following permissions for the two scripts:

   ```
   chmod o+rx delete_datatables.sql
   ```

   ```
   chmod u+rx purge_sar_data.sh
   ```

4. Stop the dataminer of the data source type you want to purge from the database. (For information on how to stop a data miner, see the Installation Guide.
5. Run the purge script (as root, the only user that has the permission to run the script) by executing the following command:

   ```
   /opt/opsware/omdb/bin/purge_sar_data.sh
   ```

6. Answer the questions of the script interview:

   Specify a data source from (SAS, ASAS, NAS, PAS, CA, SE) that you want the data to be purged.

   [Type the name of one of the listed data sources that you want to purge data from.]

7. What is the maximum days that you want to keep the data in the database?

   [Type 0 to purge all data.]

8. What is the desired ORACLE_SID?

[Enter the default cmdb, unless you are using a different SID]

9. Are you sure that you want to purge all SAR data?

   [Type y to purge all data of the selected data source from the database.]

10. After the data is purged, answer the following interview question:

    Do you want to remove all data files in collect received directory? (y/n)

    [Type y to remove all data files in collect received directory, otherwise type n.]

11. When the interview is finished, start the BSA Essentialscore server by executing the following command:

    ```
    /etc/init.d/opsware-omdb start
    ```

12. Delete the following two data miner files, `DMSettingsCache.properties` and all `*.ser` files, located in the directory in where the data miner was un-tarred .
13. Restart the dataminer

Purging All Data from Your BSA Essentials Database After X Days

1. Log in to the BSA Essentialscore server as root.
2. Copy the two scripts `delete_datatables.sql` and `purge_sar_data.sh` from:

   ```
   /opt/opsware/omdb/contrib
   ```

   to

   ```
   /opt/opsware/omdb/bin
   ```

3. Set the following permissions for the two scripts:

   ```
   chmod o+rx delete_datatables.sql
   ```

   ```
   chmod u+rx purge_sar_data.sh
   ```

4. Run the purge script (as root, the only user that has the permission to run the script) by executing the following command:

   ```
   /opt/opsware/omdb/bin/purge_sar_data.sh
   ```

5. Answer the questions of the script interview:

   Specify a data source from (SAS, ASAS, NAS, PAS, CA, SE) that you want the data to be purged:

   [Choose a data source by entering the name from the list.]

6. What is the maximum days that you want to keep the data in the database?

[Select any numerical value except zero. (Zero means purge all data.) This indicates the number of days the data will be stored in the database.]

7. What is the desired ORACLE_SID?

   [Type the name of the Oracle SID (default is cmdb).]

8. Are you sure that you want to purge all SAR data?

   [Enter y for yes, n for no.]

9. When the script finished, start the BSA Essentials core server by executing the following script and command option:

   ```
   /etc/init.d/opsware-omdb start
   ```

Notes

1. In the case of purging data longer than x days, these scripts only purge historical and historical_full tables in cmdb_data. Those historical and historical_full tables have common columns "begin_date" and "end_date". The row will be purged if end_date < sysdate - x days for a given data source. In addition, data from cmdb_meta.item_loads, cmdb_meta.table_loads and cmdb_meta.data_loads are purged accordingly if cmdb_meta.data_loads.begin_date < sysdate - x days.
2. The purge script does not delete "updatable" data (for example, all past PAS/OO runs and runsteps will be kept, since that data is updatable).
3. Under no conditions will the scripts delete data files from collect/failures. If it is desired to remove these files, it must be done manually.

Central Management Console (CMC) Admin Tasks

The BusinessObjects Enterprise Central Management Console (CMC) is a web-based tool that enables you to perform basic administrative task for the reporting panel in the BSA Essentials Web Client, including setting or changing the mail server, scheduling reports, and configuring report publication and publishing.

This section contains the following tasks:

- "Starting and Stopping the Tomcat Server" (on page 38)
- ""Configuring the Reporting Mail Server" (on page 39)
- "Setting the Default Path for Saved Files on the Core" (on page 40)

For more information on these topics and using the CMC console for administration, see the BusinessObjects Enterprise Administrator's Guide.

Starting and Stopping the Tomcat Server

Before you can access the CMC Console, you need to start the Tomcat server where you installed the BSA Essentials core services.

Once you start the Tomcat server you can then log in to the CMC console and perform your administrative tasks. As soon as you finished with your CMC tasks, you need to log back in to the BSA Essentials core server and stop the Tomcat server.

Starting and Stopping the BSA Essentials Tomcat Server

1. Log in to the BSA Essentials core server.
2. Change your user to become the BSA Essentials super user on the server:

   ```
   su - omdb
   ```

3. Execute the following command to start the BSA Essentials Tomcat server:

   ```
   /etc/inii.d/bsae-tomcat start
   ```

   You can now access the CMC console and perform your administrative tasks. Once you are finished using the CMC console, you need to stop the Tomcat server.

4. Execute the following command to stop the BSA Essentials Tomcat server:

   ```
   /etc/inii.d/bsae-tomcat start
   ```

5. Exit the shell.

Configuring the Reporting Mail Server

This task shows you how to configure a mail server for the BSA Essentials reporting feature.

Configuring a Reporting Mail Server

1. Log in to the BSA Essentials core server.
2. Change your user to become the BSA Essentials super user on the server:

   ```
   su - omdb
   ```

3. Execute the following command to start the BSA Essentials Tomcat server:

   ```
   /etc/inii.d/bsae-tomcat start
   ```

   You can now access the CMC and perform your administrative tasks. Once you are finished using the CMC, you need to stop the Tomcat server.

4. Start the CMC by appending to the servername with the following syntax:

   http://<BSA_Essentials_server>:8080/CmcApp

5. Log in as administrator (the password is the same as the admin user for the BSA Essentials Web Client).
6. From the Organize column, select Servers.
7. Select bsae.AdaptiveJobServer.
8. From the Manage menu, select **Properties**.
9. From the left column list, select Destination.
10. In the Destination drop-down list, select Email.
11. Click **Add**.

12. Enter the Domain Name, Host and Port information.
13. Select Authentication method and authentication information if required by your system.
14. Click **Save** & Close the CMC.
15. Return to the BSA Essentialscore server and log in.
16. Change your user to become the BSA Essentials super user on the server:

    ```
    su - omdb
    ```

17. Execute the following command to start the BSA Essentials Tomcat server:

    ```
    /etc/inii.d/bsae-tomcat stop
    ```

Setting the Default Path for Saved Files on the Core

If you would like to set a default file path on the BSA Essentialscore server or saving reports, you can use the CMC to configure this path on your core.

Setting Default Path for Save Files on the Core

1. Log in to the BSA Essentials core server.
2. Change your user to become the BSA Essentials super user on the server:

    ```
    su - omdb
    ```

3. Execute the following command to start the BSA Essentials Tomcat server:

    ```
    /etc/inii.d/bsae-tomcat start
    ```

    You can now access the CMC and perform your administrative tasks. Once you are finished using the CMC, you need to stop the Tomcat server.

4. Start the CMC by appending to the servername with the following syntax:

    http://<BSA_Essentials_server>:8080/CmcApp

5. Log in as administrator (the password is the same as the admin user for the BSA Essentials Web Client).
6. From the Organize column, select Servers.
7. Select bsae.AdaptiveJobServer.
8. From the **Manage** menu, select **Properties**.
9. In the Destination drop-down list, select File System.
10. Click **Add**.
11. Enter the path name on the core server in the Directory field.
12. For a username and password, it is recommended to leave these fields blank, in which case the CMC will use theBSA Essentials Admin user.
13. Click **Save** & Close the CMC.
14. Return to the BSA Essentials core server and log in.

15. Change your user to become the BSA Essentials super user on the server:

    ```
    su - omdb
    ```

16. Execute the following command to start the BSA Essentials Tomcat server:

    ```
    /etc/inii.d/bsae-tomcat stop
    ```

BSA Essentials Core Monitoring

The following tables provide tools you can use to monitor your BSA Essentials core.

BSA Essentials Core Monitoring Details

What can I monitor	Where is it located?	How do I monitor this?	Why?
Database Disk-space	Database file system	Using system tools such as `df`, `mail` and `cron` is one way to monitor database disk space. See the "Monitoring database disk space" (on page 44) script sample for more information, **Note**: Consult with your Oracle DBA before monitoring.	Running out of available database disk-space can cause data load failures, reporting and administration problems, and overall problems with your database.
Database Listener	Database server	Using system tools such as `ps`, `mail`, and `cron` is one way to monitor database listener. See the "Monitoring database listener" (on page 45) script sample for more information. **Note**: Consult with your Oracle DBA before monitoring.	When the database listener is stopped, database-dependent components (reporting, loader, security, and so on) will stop functioning as expected.
Oracle RDBMS Processes	Database server	`ps -ef | grep ora_pmon` (Include other Oracle processes, if desired.) **Note**: Consult with your Oracle DBA before monitoring.	When Oracle is stopped, database-dependent components (reporting, loader, security, and so on) will stop functioning as expected.
Oracle RDBMS Ports	Database server	`netstat -patn | grep 1521` (Or other configured port.) If Oracle is remote from your BSA Essentialscore, then a firewall hole must be allowed for the core to connect. **Note**: Consult with your network administrator for more information.	When Oracle cannot be connected to because port 1521 is blocked, then database-dependant components (reporting, loader, security, and so on) will stop functioning as expected.
BSA Essentials Core disk-space	BSA Essentials Core file system	Using system tools like `df`, `mail`, and `cron` is one way to monitor BSA Essentials core disk space. See the "BSA Essentials Core Monitoring" (on page 41) script example . **Note**: Consult with your storage administrator for more information.	Running out of available disk space at `/var/opt/opsware/omdb` will prevent data and model files from loading. Running out of available disk space at `/var/log/opsware/omdb` will prevent logging.
BSA Essentials Core memory	BSA Essentials Core server	`grep OutOfMemory /var/log/opsware/omdb/server.log`	If the BSA Essentials core application server has an out of memory exception, then it is likely that some other error has happened due to the memory loss.

What can I monitor	Where is it located?	How do I monitor this?	Why?
BSA Essentials Core ports	BSA Essentials Core server	`netstat -patn | grep 8443` (or other configured port) A firewall hole must be allowed for externally available core ports. **Note**: Consult with your network administrator for more information.	When connections to BSA Essentials Core are prevented because port 8443 is blocked, Web reporting is not possible.
Business Objects Processes	BSA Essentials Core server	One method to determine if BusinessObjects processes are running is to check the total number of processes that are running (greater than 10). For example: `ps -aef | grep bo/bobje | wc -l` **Note**: Consult with your Business objects Administrator before monitoring.	If BusinessObjects is not running, then Web reporting is not possible and certain security management functions will not be possible.
Model Deployer	BSA Essentials Core server	Using system tools such `ls`, `wc`, `mail`, and `cron` is one way to monitor failed model deployment. See the "BSA Essentials Core Monitoring" (on page 41) script example for more information.	When the datamodel and ETL fails to deploy, the consequences can vary from unexpected reporting results to data load failures.
Data Loader	BSA Essentials Core server	Using system tools such as `ls`, `wc`, `mail`, and `cron` is one way to monitor failed data loads. See the "Monitoring data loader failures" (on page 46) script example for more information.	When data fails to load, the integrity of report results is reduced. When failed data files are found, the problem can be diagnosed and fixed.
Rsync (core)	BSA Essentials Core server	Check for the rsync process running from `/opt/opsware/omdb/bin` `ps -ef | grep /opt/opsware/omdb/bin/rsync`	When the core-side rsync process is stopped, then each dataminer will accumulate data files (potential disk space issues) and the loader will not be able to load data.
Dataminer Disk-space	Dataminer filesystem	Using system tools like `df`, `mail`, and `cron` is one way to monitor Dataminer disk space. See the "Monitoring dataminer mount point disk space" (on page 47) script example for more information. **Note**: Consult with your storage administrator before monitoring.	Running out of available disk space will cause the data miner to not collect the data from the source system and not add new log entries.
Dataminer Memory	Dataminer system	`grep OutOfMemory dataminer.log`	If the dataminer has an out of memory exception, then it is likely that some other error has occurred related to the memory failure.

What can I monitor	Where is it located?	How do I monitor this?	Why?
Dataminer Process	Dataminer system	`dmwatch.sh` script can be located on the core server at `/opt/opsware/omdb/contrib/dmwatch`. See the "dmwatch script readme" (on page 48) file for more information, or see "Dataminer Watchdog Script" (on page 32) for more information on syntax and usage.	It is very important to have the dataminer always running in order to collect data. if not, then there is potential that the source system will remove the data before it can be mined.
Rsync (Dataminer)	Dataminer system	`dmwatch` script, located on the BSA Essentials core server at `/opt/opsware/omdb/contrib/dmwatch.sh`. See the "dmwatch script readme" (on page 48) file for more information.	When the dataminer-side rsync process is stopped, that dataminer will accumulate data files (potential disk space issues) and the loader will not be able to load that Dataminer's data.
Compliance Checks Rollup Job	BSA Essentials Core server	Use the following SQL query to determine if any errors when running the compliance calculation package for the current day `select description, exception, source, source_id, create_date, category from cmdb_meta.application_events where source like 'compliance_fact_pkg%' and create_date >= sysdate -1 and create_date < sysdate+1`	Failed compliance rollup calculations will cause report result integrity problems and is a sign that ETL data is either missing or incorrect.
Loader Backlog	Core file system	Using system tools like `ls`,`wc`, `mail` and `cron` is one way to monitor excessive loader backlogs. See "Monitoring loader backlog" (on page 47) for more information. **Note**: Consult with your storage administrator before monitoring.	If the number of unloaded data files in the loader collect directory exceeds a certain threshold, then this might be a sign of a loader or environment problem.

Core Monitoring Examples

Note: The example code shown in this section is only meant to illustrate the monitoring concept being discussed in each case. These examples may have to be modified to suit your monitoring needs. Also, the example code snippets have not been formally validated by HP.

<table>
<tr><th>Example Name</th><th>Example Description</th></tr>
<tr><td>Monitoring database disk space</td><td>#!/bin/ksh for i in `df -k|grep /u0|awk '{ print $4 }'`
do
    # Convert the file size to a numeric value
    filesize=`expr i`
If any filesystem has less than 100k, issue an alert</td></tr>
</table>

<table>
<tr><th>Example Name</th><th>Example Description</th></tr>
<tr><td></td><td>

```
    if [ $filesize -lt 100 ]
    then
       mailx -s "Oracle filesystem $i has less than 100k free."
oracle_dba@my.company.com
   fi
done
```

</td></tr>
<tr><td>Monitoring database listener</td><td>

```
#!/bin/bash

listener=LISTENER # the name of your oracle listener for example:
LISTENER
mailto=oracle_dba@my.company.com    # change it to your preferred
E-Mail address
ORACLE_HOME=cmdb                    # set your oracle_home var-
iable

if ! ps -ef |grep -w $listener |grep -v
   then su - oracle -c "$ORACLE_HOME/bin/lsnrctl start $listener"

   echo "Look out! $listener stopped at `date`. Trying to start
the $listener ... `
   if ps -ef |grep $listener |grep -v grep |grep -v mail
   then
       echo $listener was started successfully.
   else
       echo Error starting $listener!
   fi` " | mailx -s "There is no $listener process!" $mailto
fi
```

</td></tr>
</table>

<table>
<tr><th>Example Name</th><th>Example Description</th></tr>
<tr><td>Monitoring loader, model-deployer, logfile mount point disk space</td><td>

```
#!/bin/ksh

filesize=`df -k /var/opt/opsware/omdb | awk '{ print $4 }' | tail
-n1`

# Convert the file size to a numeric value
filesize=`expr $filesize`

# If any filesystem has less than 100k, issue an alert
if [ $filesize -lt 102400 ]
then
    mailx -s "/var/opt/opsware filesystem has less than 100k
free." oracle_dba@my.company.com
fi

filesize=`df -k /var/log/opsware/omdb | awk '{ print $4 }' | tail
-n1`

# Convert the file size to a numeric value
filesize=`expr $filesize` # If any filesystem has less than 100k,
issue an alert
if [ $filesize -lt 102400 ]
then
     mailx -s "/var/log/opsware/omdb filesystem has less than
100k free." bsae_admin@my.company.com
fi
```

</td></tr>
<tr><td>Monitoring model and ETL deployment failures</td><td>

```
#!/bin/bash

mailto=bsae@my.company.com # change it to your preferred E-Mail
adress
failed_etldir=/var/opt/opsware/omdb/deploy/failure/etl
failed_modeldir=/var/opt/opsware/omdb/deploy/failure/datamodel

failed_etldir_filecount=`ls ${failed_etldir} | wc -l`
if [ $failed_etldir_filecount -gt 0 ]; then
     mailx -s "$failed_etldir has $failed_etldir_filecount files.
This usually indicates failed etl deployment files." ${mailto}
fi

failed_modeldir_filecount=`ls ${failed_modeldir} | wc -l`
if [ $failed_etldir_filecount -gt 0 ]; then
     mailx -s "$failed_modeldir has $failed_modeldir_filecount
files. This usually indicates failed model deployment files."
${mailto}
fi
```

</td></tr>
<tr><td>Monitoring data loader failures</td><td>

```
#!/bin/bash

mailto=bsae_admin@my.company.com # change it to your preferred E-
Mail adress
failed_loaderdir=/var/opt/opsware/omdb/collect/failures

failed_loaderdir_filecount=`ls ${failed_loaderdir} | wc -l`
if [ $failed_loaderdir_filecount -gt 0 ]; then
     mailx -s "$failed_loaderdir has $failed_loaderdir_filecount
files. This usually indicates failed data load files." ${mailto}
fi
```

</td></tr>
</table>

<table>
<tr><th>Example Name</th><th>Example Description</th></tr>
<tr><td>Monitoring loader backlog</td><td><pre>
#!/bin/bash

mailto=bsae_admin@my.company.com   # change it to your preferred E-Mail address
collect_dir=/var/opt/opsware/omdb/collect
threshold=10000   # change to preferred threshold

collect_filecount=`ls ${collect_dir} | wc -l`

 if [${collect_filecount} -gt ${threshold}];

     then mailx -s "A BSAE Loader File Backlog has exceeded ${threshold}. Check the loader and environment for any problems." ${mailto}

fi
</pre></td></tr>
<tr><td>Monitoring dataminer mount point disk space</td><td><pre>
#!/bin/ksh

filesize=`df -k /opt/opsware/dataminer/collect | awk '{ print $4 }' | tail -n1`

# Convert the file size to a numeric value
filesize=`expr $filesize`

# If any filesystem has less than 100k, issue an alert
if [$filesize -lt 102400]
then
     mailx -s "/opt/opsware/dataminer filesystem has less than 100k free." bsae_admin@my.company.com
fi
</pre></td></tr>
</table>

Example Name	Example Description
dmwatch script readme	The dmwatch.sh script can be used to automate the start/restart of the dataminer process when (1) the dataminer process has stopped or (2) the dataminer's child rsyncd process hasn't copied the DATS file to BSAE with 24 hours. or (3) the dataminer log has oracle error ORA-01861 The general setup is to use crond to run it once a day with the --auto flag and it will start/restart dataminer when needed. Some information is also logged into the file dmwatch_laststatus that can be used for debugging. [Setup Instructions] 1. scp dmwatch.zip to SA dataminer directory 2. ssh to system running SA dataminer (as root) 3. cd to SA dataminer directory 4. unzip dmwatch.zip (a single file dmwatch.sh should be extracted) 5. view usage .. type-> ./dmwatch.sh --help OMDB Dataminer Watchdog Script "dmwatch.sh" Supported parameters: --dm_home dataminer home directory --auto start/restart the dataminer/rsyncd if any problems are detected --on_db adds extra transaction information to the output (only use if on truth database system) --restart_on_log_fail restarts the dataminer if log file has error ORA-01861 in last 1000 lines --append appends info to dmwatch_laststatus instead of replacing --help show script usage 6. add as daily cron job e.g. crontab -e then insert the following line -> 0 0 * * * /opt/opsware/dataminer/dmwatch.sh --dm_home /opt/opsware/dataminer --auto --restart_on_log_fail --append save and quit -- or add to /etc/cron.daily -- *note* change dataminer location directory if it doesn't match yours 7. done You can also run the dmwatch.sh at anytime to view some transaction related information (and health). e.g.

Example Name	Example Description
	[root@sas dataminer]# ./dmwatch.sh ** dataminer_type: SAS dataminer_status: running (process id 19426) utc_date: Tue Nov 3 21:10:38 UTC 2009 last_processed_tranid: 7390710001 action_needed: none ** or use the --auto flag to tell it to fix dataminer if needed e.g. [root@sas dataminer]# ./dmwatch.sh --auto ** dataminer_type: SAS dataminer_status: stopped utc_date: Tue Nov 3 21:11:19 UTC 2009 last_processed_tranid: 7390710001 action_needed: start dataminer *** warning: The dataminer is not running ** starting dataminer Starting OMDB DataMiner (data source type: SAS) Dataminer is running on 64bit architecture Started (PID: 21867) ** ** dataminer_type: SAS dataminer_status: running (process id 21867) utc_date: Tue Nov 3 21:11:25 UTC 2009 last_processed_tranid: 7390710001 action_needed: none ** *note about the --on_db arg* Because you setup involves the Oracle RDBMS on a separate system than the dataminer, you can not *at this time* use the --on_db flag to gather the transaction information.

Example Name	Example Description

Appendix A: Index