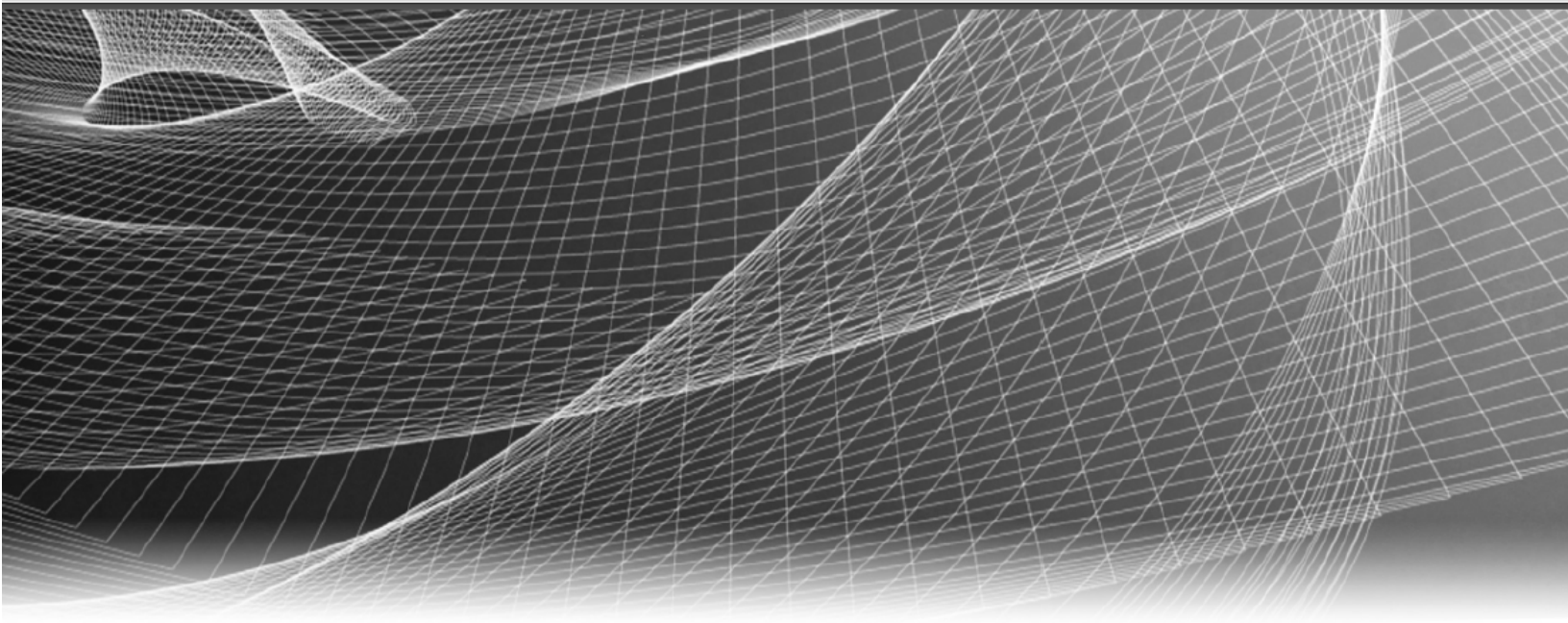


RSA Security Analytics

Reporting Engine Configuration Guide

for Version 10.6.5

RSA

EMC²

Contact Information

RSA Link at https://community.rsa.com contains a knowledgebase that answers common questions and provides solutions to known problems, product documentation, community discussions, and case management.

Trademarks

For a list of RSA trademarks, go to www.emc.com/legal/emc-corporation-trademarks.htm#rsa.

License Agreement

Third-Party Licenses

This product may include software developed by parties other than RSA. The text of the license agreements applicable to third-party software in this product may be viewed on the product documentation page on RSA Link. By using this product, a user of this product agrees to be fully bound by terms of the license agreements.

Note on Encryption Technologies

This product may contain encryption technology. Many countries prohibit or restrict the use, import, or export of encryption technologies, and current use, import, and export regulations should be followed when using, importing or exporting this product.

Distribution

EMC believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

February 2018

Contents

Reporting Engine Overview

This topic is an overview of the Reporting Engine. The Reporting Engine supports the definition and generation of reports and alerts that you maintain in the RSA Security Analytics Reporting and Alerting module views and dashlets. A Reporting Engine:

- Facilitates the delivery of selected data to the Reporting and Alerting module views (NetWitness meta data and IPDB event data).
- Stores rules definitions that govern how the data is represented in reports and alerts.
- Manages the alert queue by allowing you to enable and disable alerts.

  A Reporting Engine runs reports and alerts based on the data drawn from a data source so you must associate a data source, or multiple data sources, to a Reporting Engine. There are four types of data sources:

- IPDB Data Sources - The Internet Protocol Database (IPDB) data source contains both normalized and raw event messages. It stores all collected messages in a file system organized by event source (device), IP address, and time (year/month/day) with index files to facilitate searches (report and queries).
- NWDB Data Sources - The NetWitness Database (NWDB) data sources are Decoders, Log Decoders, Brokers, Concentrators, Archiver, and Collection.
- Warehouse Data Sources - The Warehouse data sources are Pivotal and MapR.
- Incident Management Data Sources - IMDB is used to generate reports on alerts and incidents. The IMDB data sources are Reporting Engine, ESA, Malware, ECAT, and Web Threat Detection. IMDB is used to store the alerts and incidents reports.

Configure Reporting Engine

This topic lists the major Reporting Engine configuration tasks for a data source. The following checklist points to the tasks that are required to configure a Reporting Engine and configure a data source so that you can use it with Reporting Engine. The tasks are listed in the order in which you must perform them.

You must ensure that the data sources are deployed and configured in Security Analytics. See Step 2 Add a Service to a Host.

Step	Description
1	Step 1. Add a Reporting Engine to your Security Analytics deployment.
2	Step 2. Configure Reporting Engine Settings
3	Step 3. Configure Reporting Engine Data Sources and Configure Data Source Permissions.
4	Step 4. Configure Output Actions.
5	Step 5. Configure Task Scheduler for a Reporting Engine

With the basic configuration, you can perform these additional tasks as needed:

- Check Live for the latest data source content and deploy it on a regular basis. (see Step 4 Manage Live Resources topic in the in *Live Service Management Guide*).
- (Optional) Add Additional Space for Large Reports.

Topics

- Step 5. Configure Task Scheduler for a Reporting Engine
- Step 4. Configure Output Actions

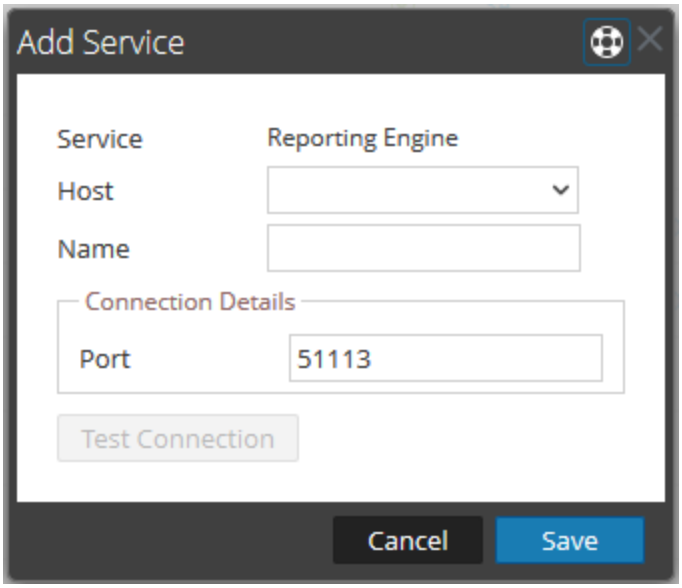
Step 1. Add a Reporting Engine

Ensure that the Reporting Engine service is deployed on Security Analytics.

To add a Reporting Engine:

1. In the **Security Analytics menu**, select **Administration** > **Services**.
2. Click + > **Reporting Engine**.
3. In the Add Service dialog, do the following:
   a. Enter the host for the Reporting Engine.
   b. Enter the name for the Reporting Engine.

      The following illustration is an example to add a Reporting Engine service to a Broker host (for example, 10.31.205.50).



      When you add a Reporting Engine service, Security Analytics defaults to the correct REST Port (**51113**).

   c. If you want to use a different port other than the default port, type the port number.
4. Click **Test Connection** to check the connection.

Next steps

You must specify the general parameters, data sources, and output actions.

Step 2. Configure Reporting Engine Settings

Ensure the Reporting Engine service is deployed on Security Analytics and the service is added.

To configure Reporting Engine service settings:

1. In the **Security Analytics** menu, select **Administration** > **Services**.
2. In the **Services** panel, select a **Reporting Engine** service.
3. Click  > **View > Config**.

   The Services Config View of Reporting Engine is displayed with the General tab highlighted. For more information on Reporting Engine General tab, see Reporting Engine: General Tab.
4. Edit the Reporting Engine service settings and click **Apply**.

   The service settings are configured on Reporting Engine.

Next steps

Step 3. Configure Reporting Engine Data Sources

Step 3. Configure Reporting Engine Data Sources

This topic tells you how to:

- Add a Data Source to a Reporting Engine
- Set a Data Source as the Default Source

Add a Data Source to a Reporting Engine

This section contains the following procedures:

- Basic Setup
- Enable Jobs
- Enable Kerberos Authentication

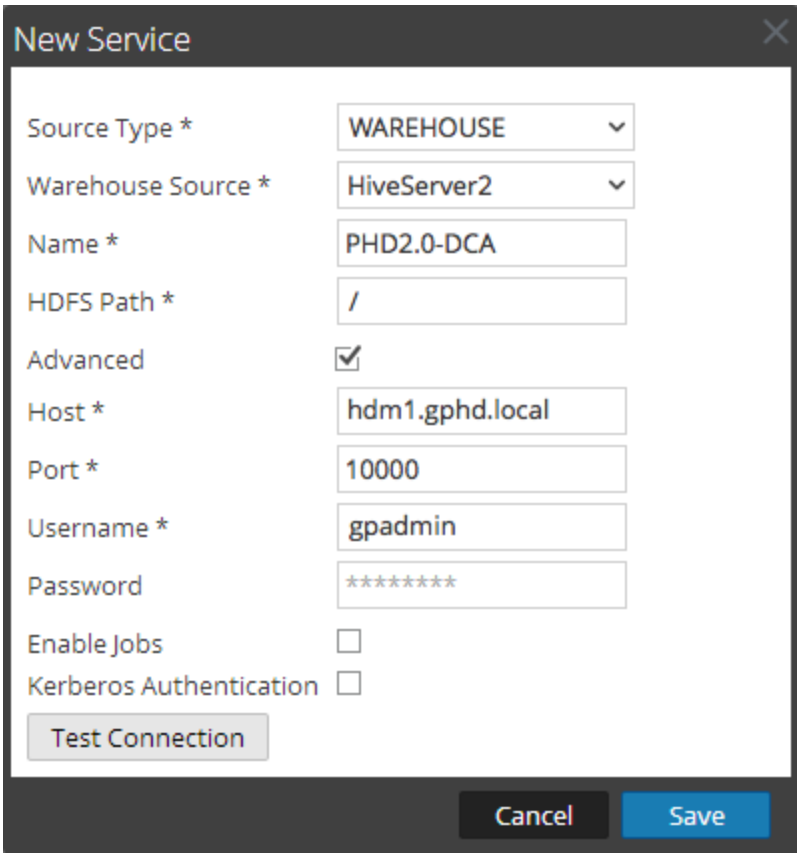
Basic Setup

To associate a data source with a Reporting Engine:

1. In the **Security Analytics menu**, select **Administration** > **Services**.
2. In the **Services Grid**, select a **Reporting Engine** service.
3. Click  **> View > Config**.

   The Services Config View of Reporting Engine is displayed.
4. On the **Sources** tab, click  > **New Service**.

   The **New Service**dialog is displayed.



5. Fill in the fields as follows:

   a. In the **Source Type** drop-down menu, select **Warehouse**.

   b. In the **Warehouse Source** drop-down menu, select the warehouse data source.

   c. In the **Name** field, enter the name of the Warehouse data source.

   > **Note:** Make sure you do not use special characters such as &,' , ", < and > while adding the data source. If you use special characters in the name field, the update to the Reporting Engine fails.

   d. In the **HDFS Path** field, enter the HDFS root path to which the Warehouse Connector writes the data.

   For example:
   If **/saw** is the local mount point for HDFS that you have configured while mounting NFS on the device where you have installed the Warehouse Connector service to write to SAW, for more information, see **Mount the Warehouse on the Warehouse Connector** in the *RSA Analytics Warehouse (MapR) Configuration Guide*.

   If you have created a directory named **Ionsaw01** under **/saw** and provided the corresponding Local Mount Path as **/saw/Ionsaw01**, then the corresponding HDFS root path would be **/Ionsaw01**.

The **/saw** mount point implies to / as the root path for HDFS. The Warehouse Connector writes the data **/Ionsaw01** in HDFS. If there is no data available in this path, the following error is displayed:

"No data available. Check HDFS path"

Make sure that **/Ionsaw01/rsasoc/v1/sessions/meta** contains avro files of the meta data before performing test connection.

e. Select **Advanced** checkbox to use the advanced settings, and fill in the **Database URL** with the complete JDBC URL to connect to the HiveServer2.

For example:
If kerberos is enabled in hive then the JDBC url will be:

jdbc:hive2://<host>:<port>/<db>;principal=<Kerberos serverprincipal>

If SSL is enabled in hive then the JDBC url will be:

jdbc:hive2://<host>:<port>/<db>;ssl=true;sslTrustStore=<trust_store_path>;trustStorePassword=<trust_store_password>

For more information on HIVE server clients, see https://cwiki.apache.org/confluence/display/Hive/HiveServer2+Clients.

f. If not using the advanced settings, enter the values for the **Host** and **Port**.

- In the **Host** field, enter the IP address of the host on which HiveServer2 is hosted.

  Note: You can use the virtual IP address of Mapr only if HiveServer2 is running on all the nodes in the cluster.

- In the **Port** field, enter the HiveServer2 port of the Warehouse data source. By default, the port number is **10000**.

g. In the **Username** and **Password**field, enter the JDBC credentials used to access HiveServer2.

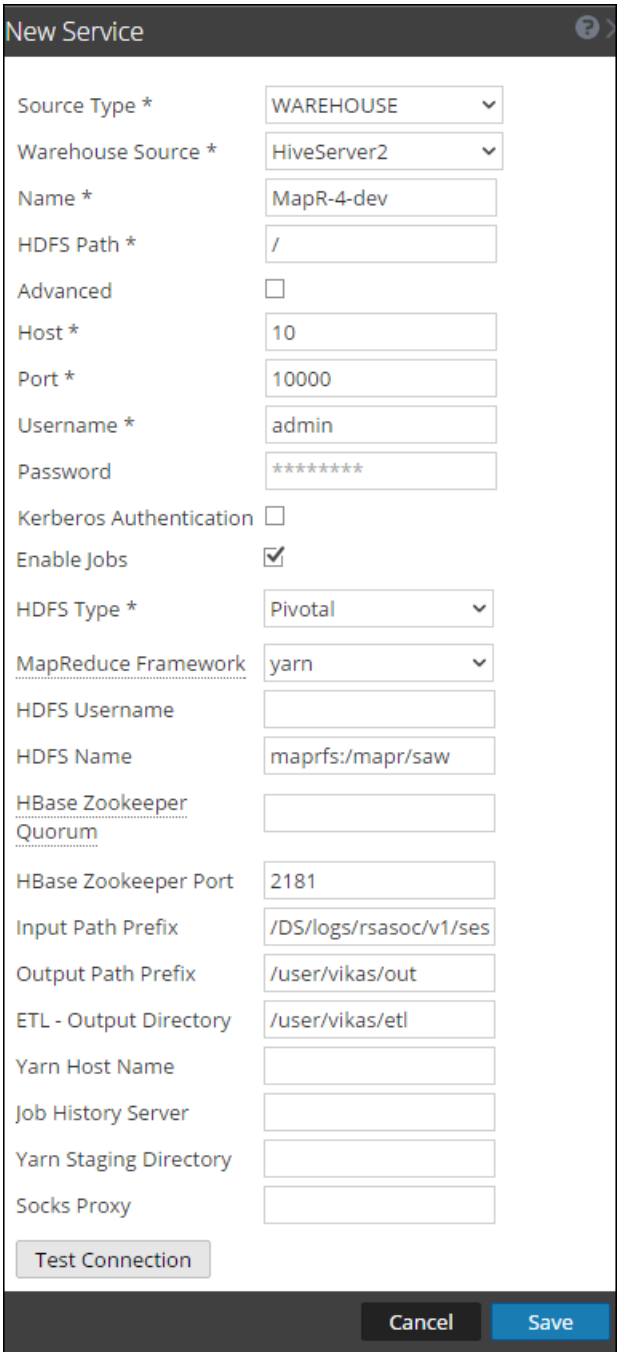
Note: You can also use LDAP mode of authentication using Active Directory. For instructions to enable LDAP authentication mode, see Enable LDAP Authentication.

Continue to the next section, **Enable Jobs**, if you want to run warehouse analytics reports. If you do not want to run warehouse analytics reports, skip to **Enable Kerberos Authentication**.

Enable Jobs

To run warehouse analytics reports, perform this procedure.

1. Select the **Enable Jobs** checkbox.



2. Fill in the fields as follows:

a. Select the type of HDFS from the **HDFS Type** drop-down menu.

- If you select the Pivotal HDFS type, enter the following information:

Field	Description
HDFS Username	Enter the username that Reporting Engine should claim when connecting to Pivotal. For standard pivotal DCA clusters, this would be 'gpadmin'.
HDFS Name	Enter the URL to access HDFS. For example, hdfs://hdm1.gphd.local:8020.
HBase Zookeeper Quorom	Enter the list of host names separated by a comma on which the ZooKeeper servers are running.
HBase Zookeeper Port	Enter the port number for the ZooKeeper servers. The default port is 2181.
Input Path Prefix	Enter the output path of the Warehouse Connector (`/sftp/rsasoc/v1/sessions/data/<year>/<month>/<date>/<hour>`) until the year directory. For example, `/sftp/rsasoc/v1/sessions/data/`.
Output Path Prefix	Enter the location where the data science job results are stored in HDFS.
Yarn Host Name	Enter the Hadoop yarn resource-manager host name in the DCA cluster. For example, **hdm3.gphd.local**.
Job History Server	Enter the Hadoop job-history-server address in the DCA cluster. For example, **hdm3.gphd.local:10020**.
Yarn Staging Directory	Enter the staging directory for YARN in the DCA cluster. For example, `/user`.

Field	Description
Socks Proxy	If you are using the standard DCA cluster, most of the hadoop services will be running in a local private network, not reachable from Reporting Engine. Then, you must run a socks proxy in the DCA cluster and allow access from outside to the cluster. For example, **mdw.netwitness.local:1080**.

- If you select the MapR/HDP HDFS type, enter the following information:

Field	Description
Client Host Name	The user can populate the public ip address of any one of the MapR/ HDP warehouse hosts.
Client Host User	Enter a UNIX username in the given host that has access to execute map-reduce jobs on the cluster. The default value for MapR is 'mapr' and for HDP is 'root'.
Client Host Password	(Optional for MapR) To setup password-less authentication, copy the public key of the “rsasoc” user from **/home/rsasoc/.ssh/id_rsa.pub** to the “authorized_keys” file of the warehouse host located in **/home/mapr/.ssh/authorized_keys**, with the assumption that “mapr” is the remote UNIX user. (Mandatory for HDP) Enter the root password.
Client Host Work Dir	Enter a path that the given UNIX user (for example, “root”) has write access to. **Note:** The work directory is used by Reporting Engine to remotely copy the Warehouse Analytics jar files and start the jobs from the given host name. You must not use “/tmp” to avoid filling up of the system temporary space. The given work directory will be remotely managed by Reporting Engine.

Field	Description
HDFS Name	Enter the URL to access MapR HDFS. For example, to access a specific cluster, maprfs:/mapr/<cluster-name> . Enter the URL to access HDP HDFS. For example, to access a specific host, hdfs://<host-name>:8020, where <host-name> is '*sandbox.hortonworks.com*'.
HBase Zookeeper Port	Enter the port number for the ZooKeeper servers. The default port is 5181.
Input Path Prefix	Enter the output path (`/rsasoc/v1/sessions/data/<year>/<month>/<date>/<hour>`) until the year directory. For example, `/rsasoc/v1/sessions/data/`.
Input Filename	Enter the file name filter for avro files. For example, **sessions-warehouseconnector**.
Output Path Prefix	Enter the location where the data science job results are stored in HDFS.

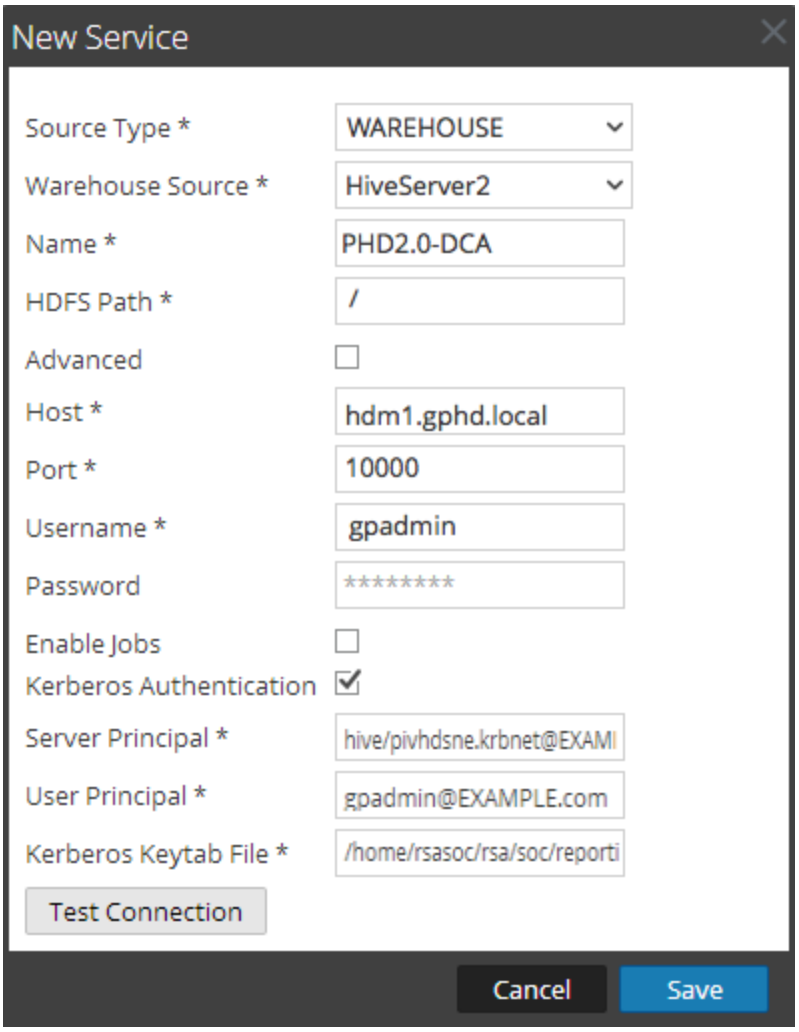
b. Select the MapReduce Framework as per the HDFS type.

> **Note:** For HDFS type MapR, select MapReduce framework as Classic. For HDFS type Pivotal, select MapReduce Framework as Yarn.

Next, enable Kerberos authentication.

Enable Kerberos Authentication

1. Select **Kerberos Authentication** checkbox, if the Warehouse has Kerberos enabled Hive server.



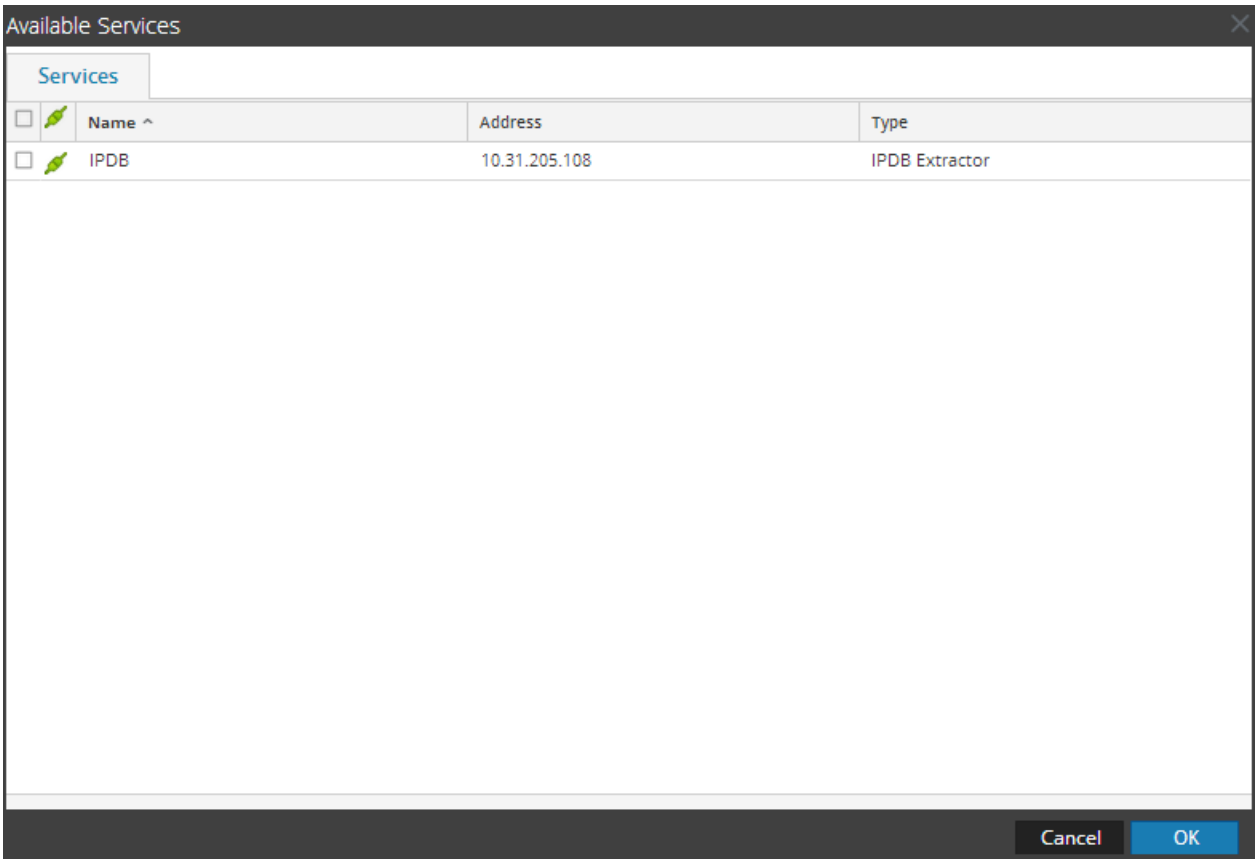
2. Fill in the fields as follows:

Field	Description
Server Principal	Enter the Principle used by the hive server to authenticate with the Kerberos Key Distribution Center (KDC) Server.
User Principal	Enter the Principle that Hive JDBC client uses to authenticate with the KDC server for connecting the Hive server. For example, **gpadmin@EXAMPLE.COM**.
Kerberos Keytab File	View the Kerberos keytab file location configured in the Hive Configuration panel on the Reporting Engine: General Tab. **Note:** Reporting Engine supports only the data sources configured with the same Kerberos credentials, like, User Principal and key tab file.

3. Click **Test Connection** to test the connection with the values entered.
4. Click **Save**.

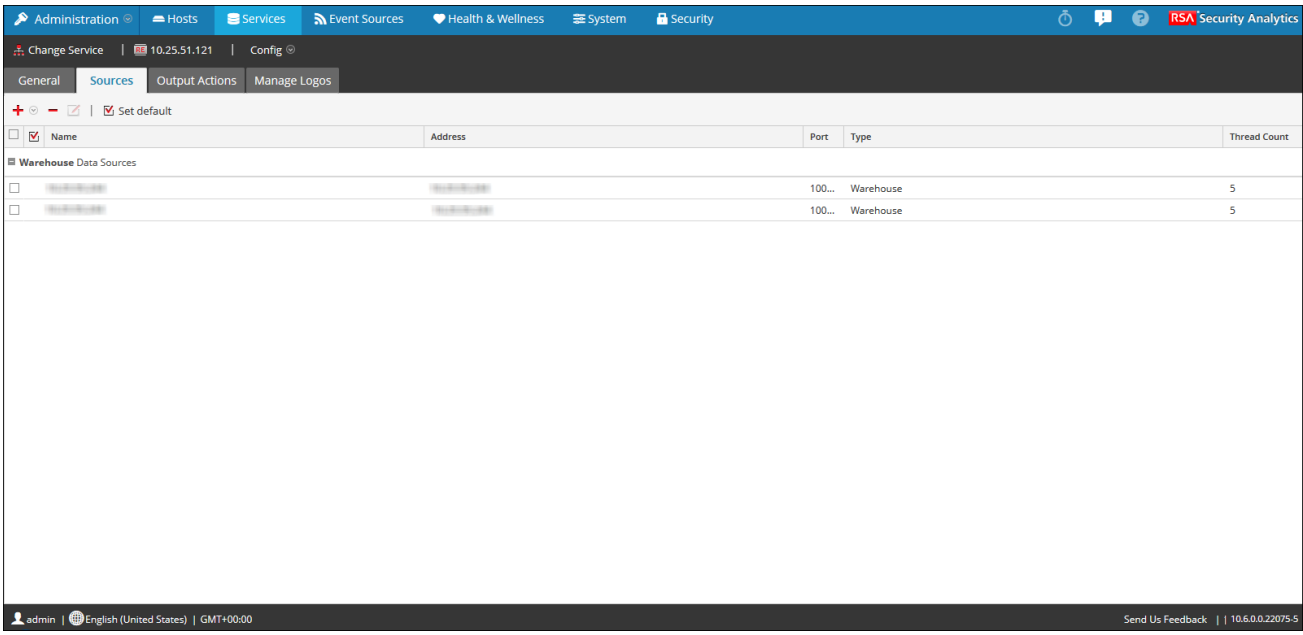
   The added Warehouse data source is displayed in the Reporting Engine Sources tab.
5. Click > **Available Services**.

   The Available Services dialog box is displayed.



6. In the Available Services dialog box, select the service that you want to add as data source to the Reporting Engine and click **OK**.

   Security Analytics adds this as a data source available to reports and alerts against this Reporting Engine.



Note: This step is relevant only for an Untrusted model.

Set a Data Source as the Default Source

To set a data source to be the default source when you create reports and alerts:

1. In the **Security Analytics menu**, select **Dashboard > Administration > Services**.
2. In the **Services Grid**, select a **Reporting Engine** service.
3. Select  **> View > Config**.

   The Services Config View of Reporting Engine is displayed.
4. Select the **Sources** tab.

   The **Services Config View** is displayed with the Reporting Engine Sources tab open.
5. Select the source that you want to be the default source (for example, Broker).
6. Click the **Set Default** checkbox.

   Security Analytics defaults to this data source when you create reports and alerts against this Reporting Engine.

Next steps

- Add Warehouse as a Data Source to Reporting Engine
- Enable LDAP Authentication

- (Optional) Add Archiver as Data Source to Reporting Engine
- (Optional) Add Collection as Data Source to Reporting Engine
- (Optional) Add Workbench as Data Source to Reporting Engine
- (Optional) Integrate ECAT Information Into Reports
- Configure Data Source Permissions

Add Warehouse as a Data Source to Reporting Engine

This topic provides instructions on how to:

- Add a Incident Management Data Source to Reporting Engine
- Set Incident Management Data Source as the Default Source

Prerequisites

Make sure that:

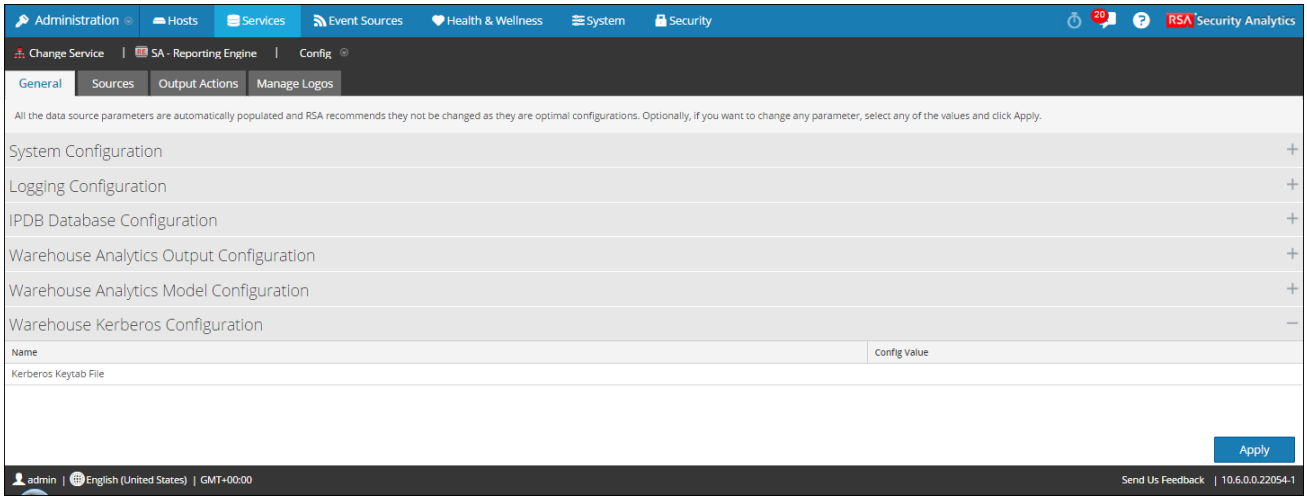
- Hive server is in running state on all the Warehouse nodes. You can use the following command to check the status of the hive server:

  ```
  status hive2 (MapR deployments)
  service hive-server2 status (Pivotal HD deployments)
  ```

- Warehouse Connector is configured to write data to the warehouse deployments.
- If Kerberos authentication is enabled for HiveServer2, make sure that the keytab file is copied to the `/home/rsasoc/rsa/soc/reporting-engine/conf/` directory in the Reporting Engine Host.

  Note: Make sure that the **rsasoc** user role has read permissions to read the keytab file.

  Also, make sure that you update the keytab file location in the **Kerberos Keytab File** parameter in the Reporting Engine Service Config View as shown below.



- The default Kerberos configuration file is located at, `/etc/kbr5.conf` in the Reporting Engine. You can modify the configuration file to provide details for Kerberos realms and other parameters related to Kerberos.
- Added the host name (or FQDN) and IP address of the Pivotal nodes and Warehouse Connector to the DNS server. If the DNS server is not configured the add the host name (or FQDN) and IP address of the Pivotal nodes and Warehouse Connector to the `/etc/hosts` file in the host on which the Warehouse Connector service is installed.

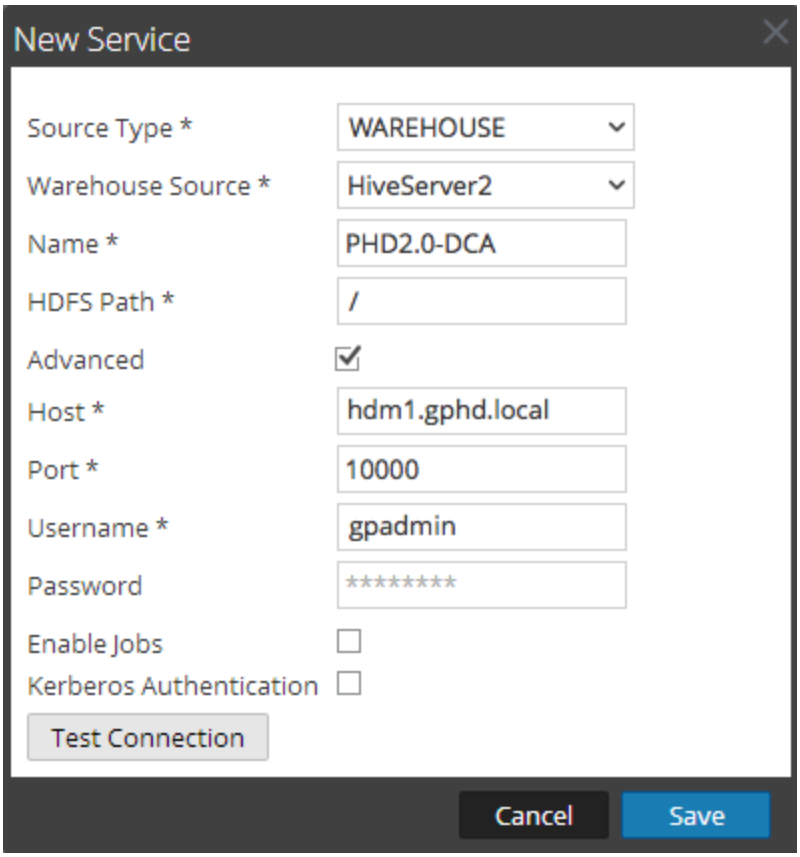
Procedure

Perform the following steps to associate a Warehouse data source with Reporting Engine:

1. In the **Security Analytics** menu, select **Administration** > **Services**.
2. In the **Services** grid, select the **Reporting Engine** service.
3. Click  > **View** > **Config**.
4. Click the **Sources** tab.

   The **Service Config** view is displayed with the Reporting Engine **Sources** tab open.
5. Click  and select **New Service**.

   The **New Service** dialog is displayed.



6. In the **Source Type** drop-down menu, select **Warehouse**.
7. In the **Warehouse Source** drop-down menu, select the warehouse data source.
8. In the **Name** field, enter the name of the Warehouse data source.
9. In the **HDFS Path** field, enter the HDFS root path to which the Warehouse Connector writes the data.

   For example:
   If **/saw** is the local mount point for HDFS that you have configured while mounting NFS on the device where you have installed the Warehouse Connector service to write to SAW, for more information, see **Mount the Warehouse on the Warehouse Connector** in the *RSA Analytics Warehouse (MapR) Configuration Guide*.

   If you have created a directory named **Ionsaw01** under **/saw** and provided the corresponding Local Mount Path as **/saw/Ionsaw01**, then the corresponding HDFS root path would be **/Ionsaw01**.

   The **/saw** mount point implies to / as the root path for HDFS. The Warehouse Connector writes the data **/Ionsaw01** in HDFS. If there is no data available in this path, the following error is displayed:

   "No data available. Check HDFS path"

Make sure that **/lonsaw01/rsasoc/v1/sessions/meta** contains avro files of the meta data before performing test connection.

10. Select **Advanced** checkbox to use the advanced settings, and fill in the **Database URL** with the complete JDBC URL to connect to the HiveServer2.

    For example:
    If kerberos is enabled in hive then the JDBC url will be:

    jdbc:hive2://<host>:<port>/<db>;principal=<Kerberos serverprincipal>

    If SSL is enabled in hive then the JDBC url will be:

    jdbc:hive2://<host>:<port>/<db>;ssl=true;sslTrustStore=<trust_store_path>;trustStorePassword=<trust_store_password>

    For more information on HIVE server clients, see https://cwiki.apache.org/confluence/display/Hive/HiveServer2+Clients.

11. If not using the advanced settings, enter the values for the **Host** and **Port**.

    - In the **Host** field, enter the IP address of the host on which HiveServer2 is hosted.

      Note: You can use the virtual IP address of Mapr only if HiveServer2 is running on all the nodes in the cluster.

    - In the **Port** field, enter the HiveServer2 port of the Warehouse data source. By default, the port number is **10000**.

12. In the **Username** and **Password**field, enter the JDBC credentials used to access HiveServer2.

    Note: You can also use LDAP mode of authentication using Active Directory. For instructions to enable LDAP authentication mode, see Enable LDAP Authentication.

13. To run warehouse analytics reports, see Enable Jobs in Step 3. Configure Reporting Engine Data Sources.

14. Enable Kerberos authentication: see Enable Kerberos Authentication in Step 3. Configure Reporting Engine Data Sources.

15. If you want set the added Warehouse data source as default source for the Reporting Engine, select the added Warehouse data source and click 

.

Result

Security Analytics adds the Warehouse as a data source available to reports and alerts against this Reporting Engine.

(Optional) HIVE Configuration For Reporting Engine

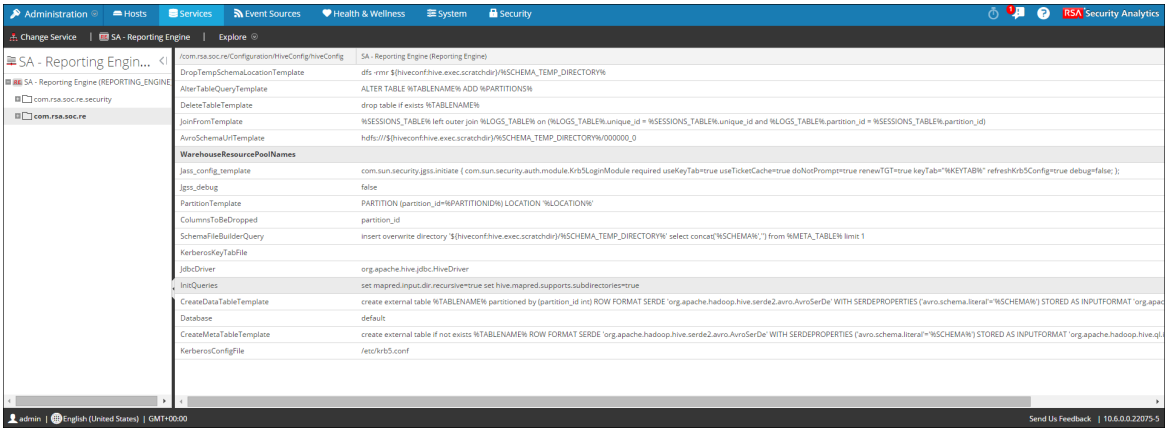
This topic explains the different HIVE configurations that are performed on Reporting Engine to set up the Warehouse on Hive Configuration.

Procedure

Perform the following steps to configure Hive for Reporting Engine:

1. In the **Security Analytics** menu, select **Administration > Services**.
2. In the **Services** panel, select a **Reporting Engine** service.
3. Select  > **View** > **Explore**

   The Services Config View of Reporting Engine is displayed.
4. Select **com.rsa.soc.re > Configuration > HiveConfig > hiveconfig**



Field	Description
JoinFromTemplate	The template used for thecreation of temporary tables that use **Raw Log** in the Rule
HiveDriverClass	Class name for HIVE JDBC Driver
Database	Default database to connect to the HIVE Server

Field	Description
InitQueries	List of HIVE Queries to be run before creating temporary hive tables. Suitable for setting HIVE properties. **Note:** Queries will not be executed for Advanced Warehouse Rules. For Expert rules, the responsibilty lies on the Query author.
CreateDataTableTemplate	Template used to create External Tables that are used to run Data Queries on AVRO files.
CreateMetaTableTemplate	Template used to create External Tables that are used to read the Schema information available in Warehouse.
SchemaFileBuilderQuery	In case the Table Creation query exceeds 4000 Characters, push the resulting AVRO Schema into a temporary AVRO file and put the location of that file as Schema for External table.
DropTempSchemaLocationTemplate	The query to be used for deleting the external table once query execution completes.
AvroSchemaUrlTemplate	The location of Schema file for Large table definitions.
ColumnsToBeDropped	The columns which are trimmed after reading results. These columns are not store in results.
Jassconfigtemplate	To authentication kerberos in HIVE Server.
KerberosConfigFile	To authentication kerberos in HIVE Server.
Jgss_debug	To authentication kerberos in HIVE Server.
KerberosKeyTabFile	To authentication kerberos in HIVE Server.
WarehouseCTASTemplate	When running a report with CTAS option dened, this denes how the resulting table is created.

Field	Description
ExcludedCustomTables	In case, reporting on Custom Tables are enabled, Reporting Engine will not allow reporting on tables whose name matches with any one of these Regex.
CustomTablesEnabled	Enables Reporting Engine to allow Rules to be defined on Custom tables.
HiveQueryLengthLimitation	In case there is a limitation on the query length that can be sent to HIVE Server to change the number as required.
EnableSmallSplitBasedSchemaLiteralCreation	This option makes Reporting Engine to split the creation of external tables in small query steps. **Note:** Enable this option only if required by your HIVE Serve distribution.
LargeSchemaFileBuilderQuery	Template used in case "EnableSmallSplitBasedSchemaLiteralCreation" is enabled. **Note:** To be used in advanced corner cases only
WarehouseResourcePoolNames	In case your Hadoop Distribution supports org.apache.hadoop.mapred.FairScheduler or org.apache.hadoop.mapred.CapacityTaskScheduler, populate this field with comma separated names of your pools. **Note:** When conguring a new Schedule of a warehouse Report, SA UI will give the option to run the Report under that particular pool.
PartitionTemplate	Template to create partition definition.
AlterTableQueryTemplate	Query template to add a partition to a External Data Table.

Enable LDAP Authentication

This topic provides instructions on how to enable LDAP mode of authentication using Active Directory for HiveServer2.

Procedure

Perform the following steps to enable LDAP authentication for HiveServer2:

1. Log on to the RSA Analytics Warehouse appliance as root user.
2. Navigate to /opt/mapr/hive/hive-0.11/conf.new/ directory. Type the following command and press ENTER:

   cd /opt/mapr/hive/hive-0.11/conf.new/
3. Edit the file **hive-site.xml**. Type the following command and press ENTER:

   vi hive-site.xml
4. Add the following properties under `<Configuration>` tag:

   ```
   <property>
       <name>hive.server2.authentication</name>
       <value>LDAP</value>
   </property>
   <property>
       <name>hive.server2.authentication.ldap.url</name>
       <value>LDAP_URL</value>
   </property>
   ```

   Where `LDAP_URL` is the URL of the LDAP Server.
5. Restart HiveServer2.

Result

You can now log on HiveServer2 using the LDAP credentials.

(Optional) Add Archiver as Data Source to Reporting Engine

This topic provides instructions on how to add Archiver as data source to Reporting Engine to generate report for the data collected by Archiver.

Prerequisites

Ensure that you have:

1. Installed the Security Analytics Archiver host in your network environment. For more information, see **Step 1. Add or Update a Host** in the *Hosts and Services Getting Started Guide*.
2. Installed and configured Log decoder in your network environment. For more information, see **Step 2. Add Log Decoder as a Data Source to Archiver** in the *Archiver Configuration Guide*.
3. Added Reporting Engine as a service to your Security Analytics deployment. For more information, see Step 1. Add a Reporting Engine.
4. Added Archiver as a service to your Security Analytics deployment. For more information, see **Step 1. Add the Archiver Service** in the *Archiver Configuration Guide*.
5. Applied license to the Archiver service.

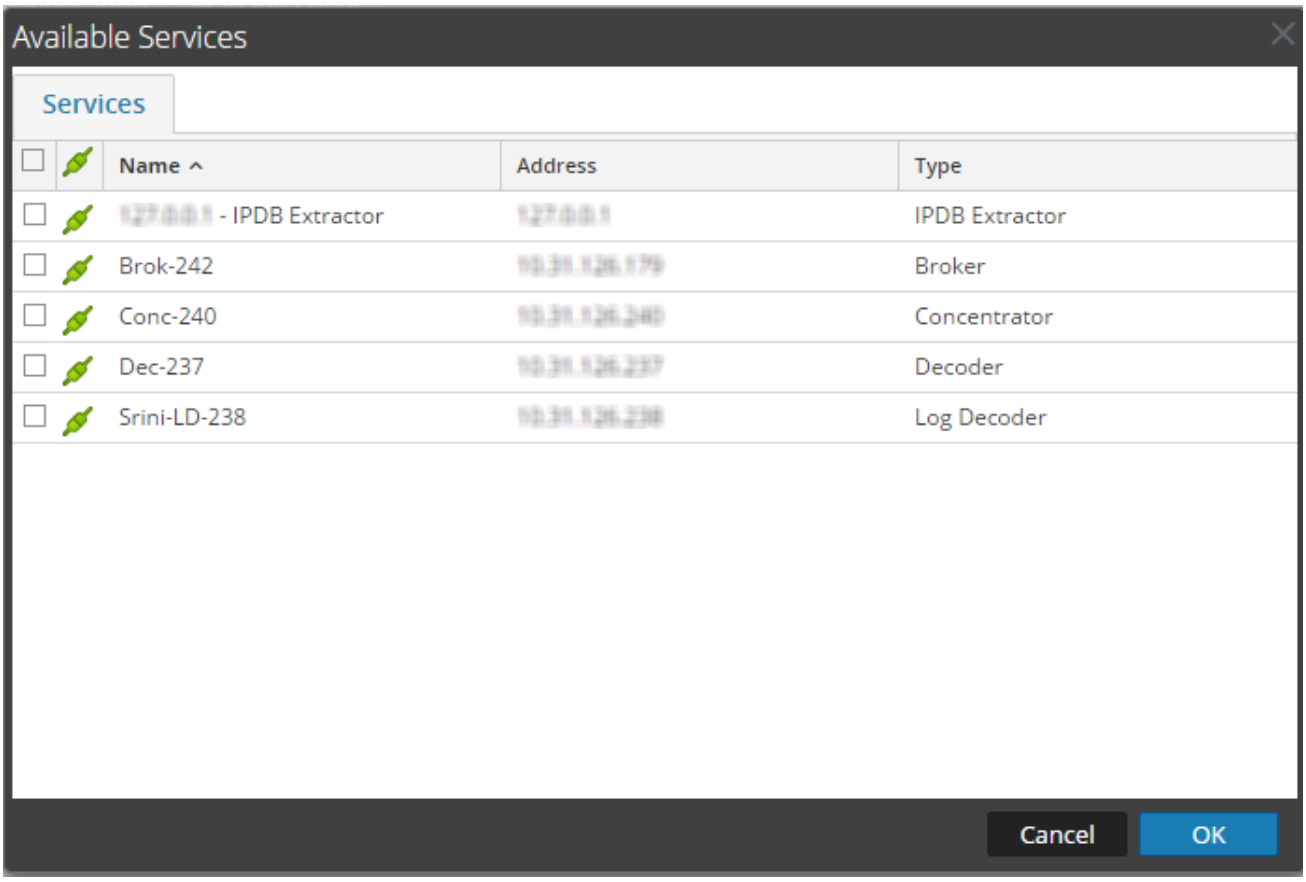
Associate Archiver data source with Reporting Engine

To associate Archiver data source with Reporting Engine:

1. In the **Security Analytics** menu, select **Administration** > **Services**.
2. In the **Services**panel, select the **Reporting Engine** service.
3. Click  > **View** > **Config**.

   The Services Config View of Reporting Engine is displayed.
4. Select the **Sources** tab.
5. Click  and select **Available Services**.

   The Available Services dialog is displayed.



6. Select the Archiver service and click **OK**.

   The service authentication dialog box is displayed.

   Note: The services with the Trust Model enabled must be added individually. You are prompted to provide a username and password for the selected service.

7. Type the Username and Password for the Archiver.
8. Click **OK**.

   The selected Archiver is listed in the **Aggregate Services** pane.

Result

You can now create reports on the data collected by Archiver.

(Optional) Add Collection as Data Source to Reporting Engine

This topic provides information on how to add collection as a data source to Reporting Engine.

Prerequisites

Ensure that you have:

- Installed a Workbench service on a Reporting Engine host.
- Backed up data in a known location on your local host, if you are adding a collection using the data restored from the backed up data.

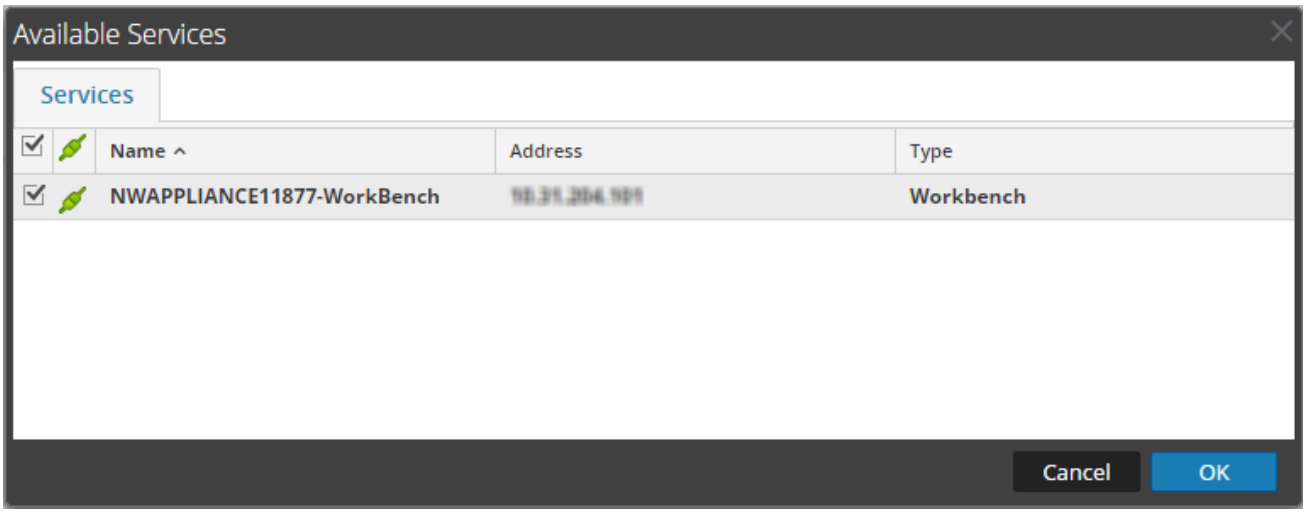
Procedure

Perform the following steps to associate Collection as a data source with Reporting Engine:

1. In the **Security Analytics** menu, select **Administration** > **Services**.
2. In the **Services**panel, select a **Reporting Engine** service.
3. Click  > **View** > **Config**.

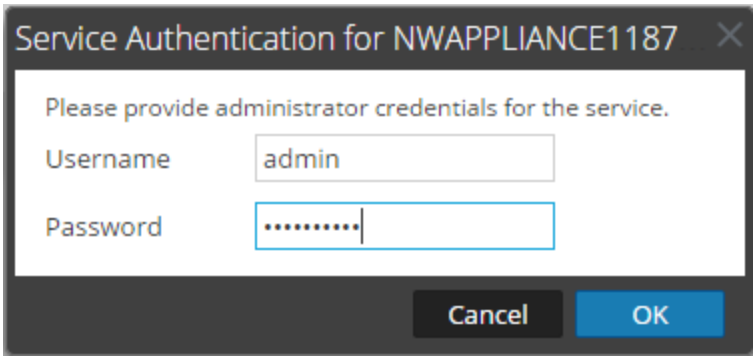
   The Services Config View of Reporting Engine is displayed.
4. Select the **Sources** tab.
5. Click  and select **Available Services**.

   The Available Services dialog is displayed.



6. Select the Workbench service and click **OK**.

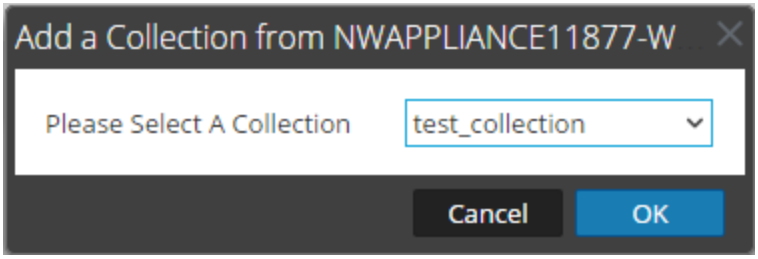
   The Service Authentication dialog for the selected service is displayed.



Note: The services with the Trust Model enabled must be added individually. You are prompted to provide a username and password for the selected service.

7. Type the username and password for admin credentials for the service.
8. Click **OK**.

   The add collection dialog is displayed.



9. Select a collection from the drop-down list and click **OK**.

   The workbench service is now added as a data source to the Reporting Engine.

Result

You can now create reports on the data collected by Collection.

(Optional) Add Workbench as Data Source to Reporting Engine

This topic provides instructions on how to add Workbench service as a data source to Reporting Engine to generate report for the data collected by Workbench.

Prerequisites

Make sure you have:

1. Added Workbench as a service to your Security Analytics deployment. For more information, see **Step 1. Add Workbench Service** in the *Archiver Configuration Guide*.
2. Added a Collection on the Workbench service.

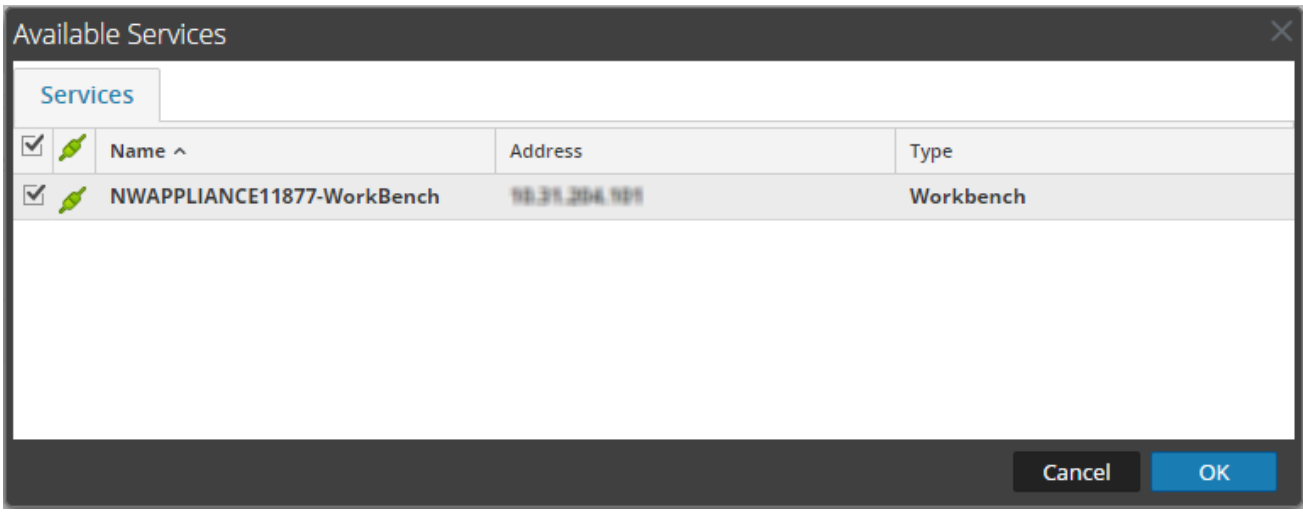
Procedure

Perform the following steps to add Workbench as a data source to Reporting Engine:

1. In the **Security Analytics** menu, select **Administration** > **Services**.
2. In the **Services**panel, select a **Reporting Engine** service.
3. Select  > **View** > **Config**.

   The Services Config View of Reporting Engine is displayed.
4. Select the **Sources** tab.
5. Click  and select **Available Services**.

   The Available Services dialog is displayed:



6. Select the Workbench service and click **OK**.

The workbench service is now added as a data source to the Reporting Engine.

Note: The services with the Trust Model enabled must be added individually. You are prompted to provide a username and password for the selected service.

Result

You can now create reports on the data collected by Workbench.

(Optional) Integrate ECAT Information Into Reports

This topic provides instructions to add ECAT information into Reports. *RSA ECAT Integration Guide* provides an overview of ECAT integration into RSA Security Analytics.

Prerequisites

You must have configured the ECAT alerts via syslog into a Log Decoder (see Configure ECAT Alerts Via Syslog into a Log Decoder topic in *RSA ECAT Integration Guide*).

Integrate ECAT Information into Reports

To integrate ECAT information into Reports:

1. In **Reporting Engine**> **View**> **Config**> **Sources**, add the Concentrator that is consuming data from the Log Decoder as a data source.

   ECAT meta is populated in Reporting Engine.

2. Run reports by selecting the appropriate meta.

Step 4. Configure Output Actions

This topic describes how you can configure output actions for a Reporting Engine.This topic provides information on how to configure output actions.

To configure output actions for a Reporting Engine:

1. In the **Security Analytics menu**, select **Administration** > **Services**.
2. In the **Services Grid**, select a **Reporting Engine**service.
3. Click  > **View**> **Config**.

   The Services Config View of Reporting Engine is displayed.
4. In the **Output Actions** tab, edit the output action settings for each of the configurations:
   - SMTP
   - SNMP
   - Syslog
   - SFTP
   - URL
   - Network Share

   For more information on each of the configurations, see Reporting Engine Output Actions.
5. Click **Apply**.

The output actions are configured on Reporting Engine.

Step 5. Configure Task Scheduler for a Reporting Engine

You can configure queues and pools in the reporting engine to schedule Warehouse reports. For more information on Task Schedulers, see **Task Scheduler for Warehouse Reporting** in the *Reporting Guide*.

Prerequisites

Make sure that you have identified the following:

- Scheduler type and pools or queues you want to use. You can configure only one scheduler for the Reporting Engine. By default the Fair Scheduler is configured.
- Names of the queues or pools, and the resources given to each queue and pool.

  Note the following:
- SA does not support multiple queues or pools per cluster. RSA recommends that you either provide unique names to queues or pools in all the clusters or use the same queue or pool names in both the clusters. If cluster size is large, there may be more than 3 pools or queues.
- If you are using an unsupported scheduler, the Reporting Engine will not set any property for the jobs that it launches.
- If the name of the pool or queue does not exist in the cluster, then Capacity Scheduler will use the default queue for the report. The Fair Scheduler may not execute the rule or it will create a new pool with the lowest share. This is based on the value specified for the Fair Scheduler property **mapred.fairscheduler.allow.undeclared.pools**.
- If you do not specify a pool or queue, the job launched by the test rule is in the **mapr** pool or the **default** queue. RSA recommends that you configure a pool mapr with low (around 1/10 of total capacity) share with **maxRunningJobs = 2** so that these rules do not disrupt running reports. Ensure that you do not specify this pool name for any reports.

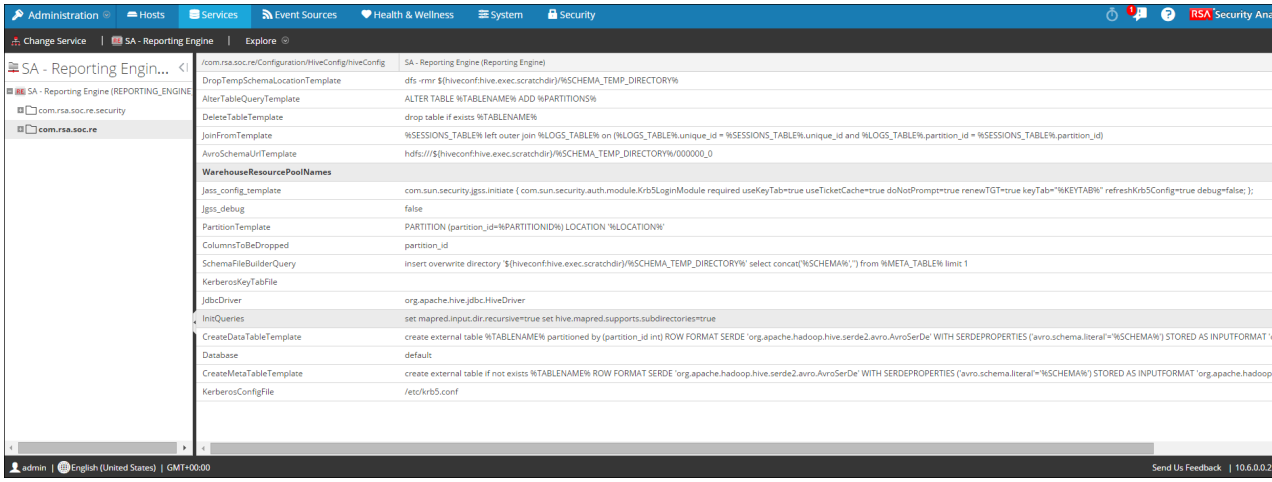
Specify the Pools and Queues

To specify the pools and queues:

1. In the **Security Analytics menu**, select **Administration** > **Services**.
2. Select **Reporting Engine** and click  > **View > Explore**.

3. Navigate through **com.rsa.soc.re** > **Configuration** > **HiveConfig** > **hiveconfig** > **WarehouseResourcePoolNames**.

4. In the **WarehouseResourcePoolNames** field, enter the pool or queue names separated by spaces. For example, to configure four pools or queues with the names pool1, pool2, wrong and default, enter the names separated by a space.



Additional Procedures for Configuring the Reporting Engine

This topic is a collection of additional procedures for Reporting Engine. Use this section when you are looking for instructions to perform a specific task after the initial setup of Reporting Engine.

Topics

Add Additional Space for Large Reports

This topic provides instructions to add additional disk space to the Reporting Engine for large reports. If large compliance reports have to generated for IPDB or Warehouse, the Reporting Engine disk space might get consumed quicker than expected. In such cases, you can mount any external storage such as SAN or NAS for storing reports.

The directories that tend to fill up disk space are **resultstore** and **formattedReports** under the Reporting Engine home directory. It is recommended to move only these two directories to SAN or NAS and replace the original locations with soft links pointing to the new locations. It is also recommended to leave the remaining directories in the local disk itself for reliable and high I/O performance.

To move disk space for the Reporting Engine to external storage:

Note: The following steps assume that the Reporting Engine home directory is located at **/home/rsasoc/rsa/soc/reporting-engine/** and the external storage is mounted under **/externalStorage/**.

1. Stop Reporting Engine service as a root user.

   stop rsasoc_re

2. Switch to `rsasoc` user.

   su rsasoc

3. Change to RE home directory.

   cd /home/rsasoc/rsa/soc/reporting-engine/

4. Move the resultstore directory to a mounted external storage. Type the following command and press ENTER:

   mv resultstore /externalStorage

5. Move the formattedReports directory to a mounted external storage. Type the following command and press ENTER:

   mv formattedReports /externalStorage

6. Create a softlink for resultstore. Type the following command and press ENTER:

   ln -s /externalStorage/resultstore /home/rsasoc/rsa/soc/reporting-engine/resultstore

7. Create a softlink for formattedReports. Type the following command and press ENTER:

   ln -s /externalStorage/formattedReports /home/rsasoc/rsa/soc/reporting-engine/formattedReports

8. Exit the `rsasoc` user.

   exit

9. Start Reporting Engine service as a root user.

```
start rsasoc_re
```

Note: If the external storage is offline, you cannot perform the following tasks:
1) Execute Reports or Reporting Alerts
2) View existing Reports or Reporting Alerts
However, you can create new Reporting objects such as Reports and Charts, and access Charts and Live Dashboard created for charts. Therefore, you must ensure that the external storage is reliable and has the required space.

Additionally, if you want to store reports beyond 100 days, change the retention configuration appropriately in the Step 2. Configure Reporting Engine Settings.

Configure Data Privacy for Reporting Engine

This topic provides information about configuring data sources for Reporting Engine using the **Sources** tab of the **Services > View > Config** view.

With the addition of the Data Privacy feature to Security Analytics 10.6 and above, access to sensitive meta in SA Core services can be restricted by configuring separate data sources for Data Privacy Officer (DPO) users and non-DPO users, and limiting access to those data sources by assigning appropriate permissions.

In the Services Config view, you can add each Core service as two separate data sources: one with a service account having privileges equivalent to a DPO and the other with a service account having privileges equivalent to any other user. Then, to limit access to those data sources based on roles, you can assign read access or no access to those data sources for individual roles. To limit access to Warehouse data sources, you can do the same.

For more information, see Configure Data Source Permissions.

Note: A user assigned to the Data_Privacy_Officers role (or an equivalent custom role), can create an alert and configure a report or alert output actions in the Reporting module. In an environment where data privacy features of Security Analytics are enabled and one or more meta keys are configured as protected, these actions can result in the following:
- When an alert is created by a DPO user, any protected or sensitive meta involved in the alert is automatically available in Incident Management. This may inadvertently provide all the users of Incident Management module access to the sensitive meta values, regardless of their roles. One option to prevent this is to disable publishing into Incident Management from Reporting.
- When an Output Action is configured by a DPO user, either sensitive meta values, reports with sensitive meta values or both, may become available to target users or destinations of that Output Action, regardless of the role assigned to the target user.

It is strongly recommended that DPO users completely avoid creating alerts or configuring output actions for a report or alert in the Reporting module. If they do such configuration, the above implications must be carefully considered.

Security Analytics Core services (for example, Concentrator, Broker, or Archiver) support the ability to restrict meta data based on the configured user role. To make use of the data privacy feature for Reporting Engine, you can configure two separate service accounts against Core. One service account for general purpose reporting that does not include any sensitive data and the other account for privileged users with access to all data including sensitive data. The access to restricted meta data for the two service accounts is configured as part of the data privacy plan on each Core service.

In Reporting Engine, you can add each Core service as two separate data sources (one being the regular data source and the other a privileged data source) using the two separate service accounts. You can configure Reporting Engine to allow only users with privileged roles to access the sensitive data source. Hence, Reporting Engine can connect to a NWDB Data source in two ways:

- Using a service account with DPO role.
- Using a service account without a DPO role.

Note: You can also add two or multiple data sources for the same Core service.

After adding two data sources with different service accounts for the same Core service, you can configure data source permissions to manage access to these data sources. For more information, see Configure Data Source Permissions.

Note: If the content is changed to utilize the transformed meta key, the hash value of the original meta is displayed in its place when viewing reports, charts and alerts.

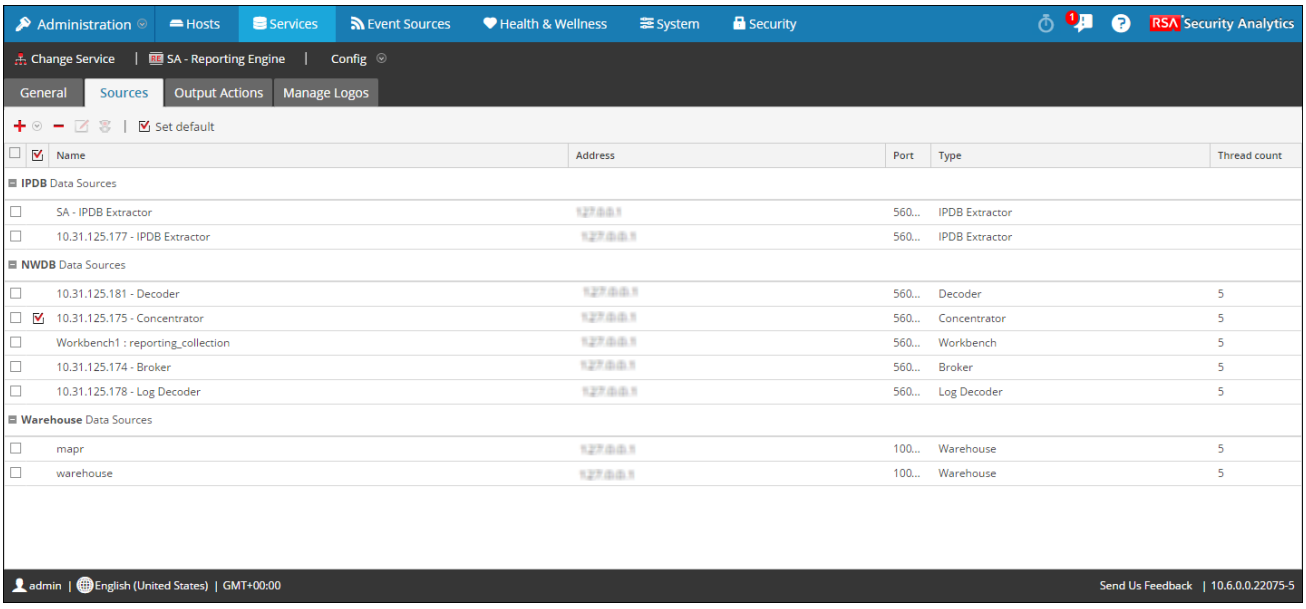
Add a NWDB Data Source with Different Service Accounts

To add a NWDB data source with different service accounts:

1. In the **Security Analytics** menu, select **Administration >Services**.
2. In the **Services** panel, select a **Reporting Engine** service.
3. Click  **> View > Config**.

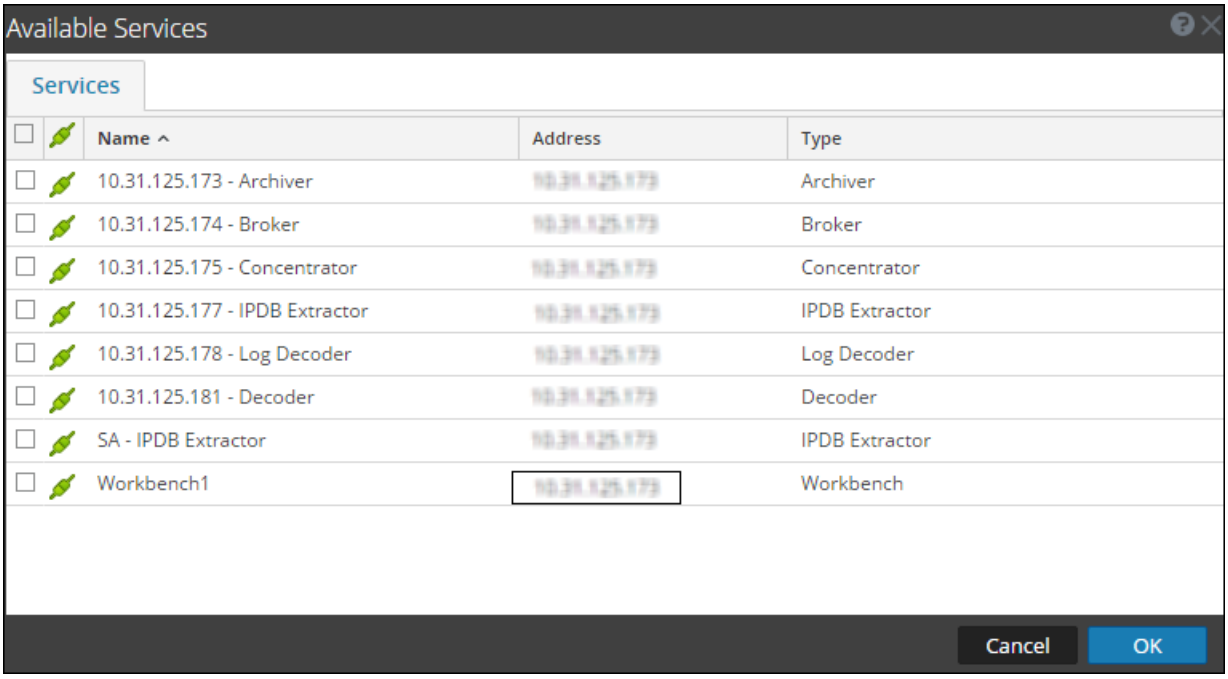
   The Services Config view of Reporting Engine is displayed.
4. Select the **Sources** tab.

   The Services Config View is displayed with the Reporting Engine Sources tab open.



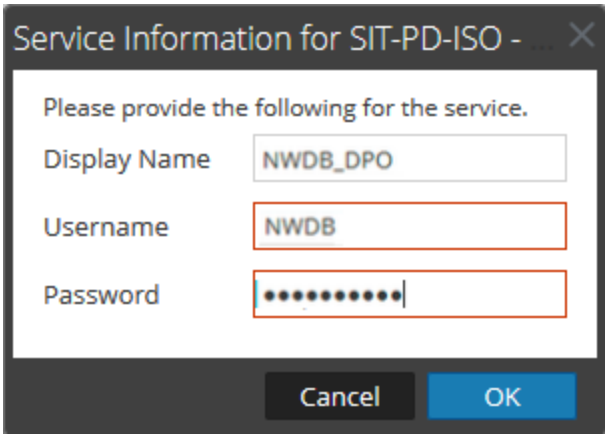
5. Click  and select Available Services.

The Available Services dialog is displayed. All services are listed, including those that have already been added Reporting Engine.



6. Select the required service and click **OK**.

   The Service Information dialog for the selected service is displayed.



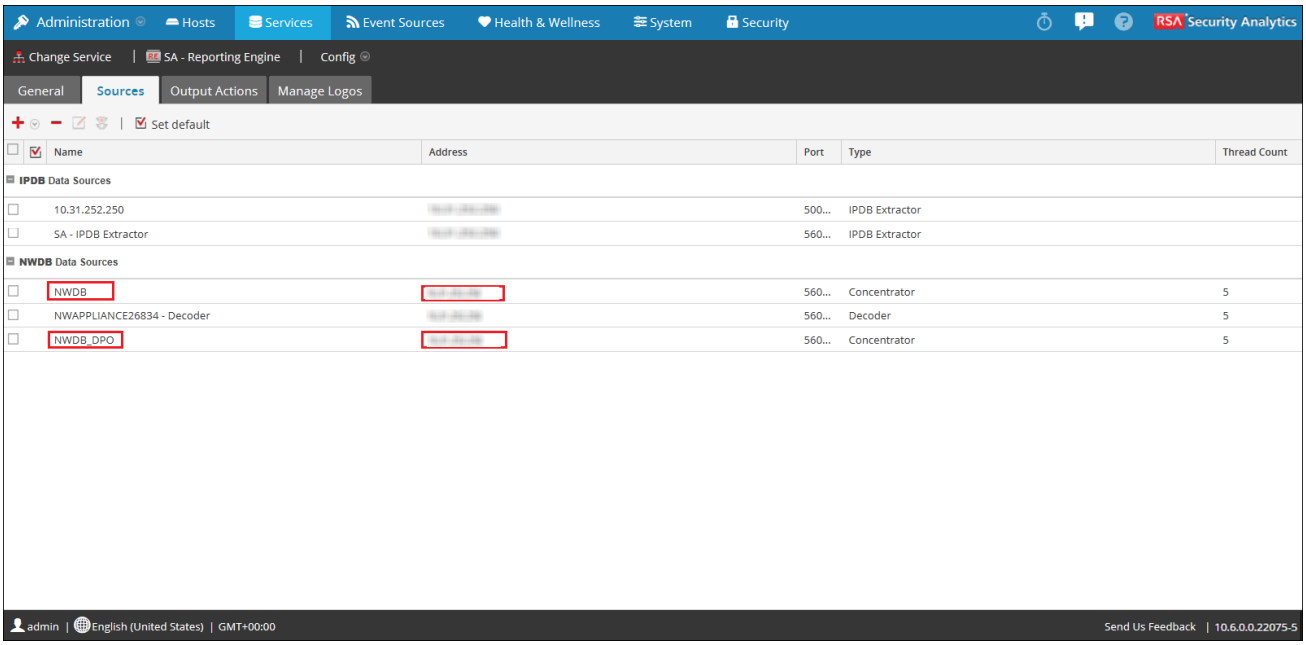
Note: Security Analytics prompts you to provide a username and password for the selected service. To limit access to sensitive data, DPO users must use their credentials while adding the source instead of using the admin credentials. These credentials need to be applied to the host even if using trusted connections between the Security Analytics server and Security Analytics Core hosts.

   Repeat the step for Non-DPO data source.

7. Type the username and password for the required service account.

8. Click **OK**.

   The required service is added as a data source to the Reporting Engine. Two data sources are added to Reporting Engine for the same Core device.



Next steps

After adding multiple data sources with different service accounts for the same Core device, you can configure data source permissions to manage access to these data sources.

Configure Data Source Permissions

This topic provides information about configuring data source permissions using the Sources tab of the Services Config view for the Reporting Engine. You can manage access control to the data sources by setting the data source permissions. Now, with the ability to add more than one data source for the same Core service, you can configure different permissions to each data source of the same Core service. For example, data privacy officers (DPO) can create a Warehouse source using their credentials, and that will allow them to execute reports against the Warehouse while restricting everyone else from being able to use that source.

Note: On update, the permissions for NWDB, Warehouse, and IMDB data sources are automatically set based on the permissions of the reporting objects. For example, if the role had the permissions set as **Read Only**/**Read & Write** for any reporting object, then that role is automatically assigned read only permission for all the data sources that existed in previous release. If no permission is set for the role, then the data source permission is automatically set to No Access. Permissions are not applicable for IPDB data sources.

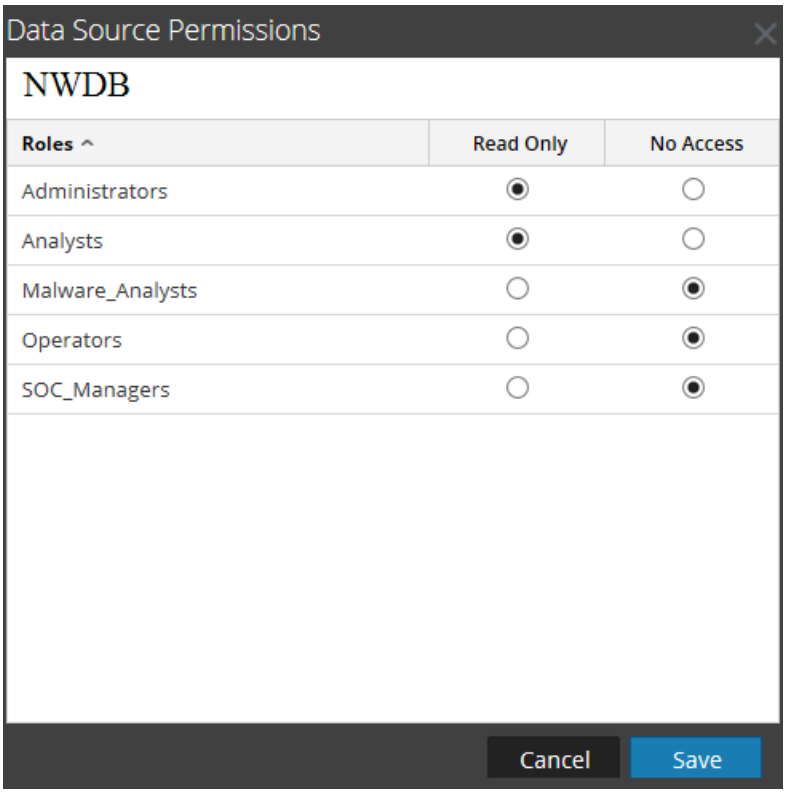
To configure permissions to data sources:

1. In the **Security Analytics** menu, select **Administration** > **Services**.
2. In the **Services** panel, select a **Reporting Engine** service.
3. Click  > **View** > **Config**.

   The Services Config view of Reporting Engine is displayed.
4. Select the **Sources** tab.

   The Service Config View is displayed with the Reporting Engine Sources tab open.
5. Select the data source for which you want to configure permissions by selecting the checkbox.
6. Click  .

   The Data Source Permissions dialog is displayed.



7. Modify the access permission for different users based on the type of service account of the data source. The permission can be either **Read Only** or **No Access**.
8. Click **Save**.

   The required permissions are configured for the data source.

Next steps

After creating the data sources and configuring the user permissions to these data sources, you can now use these data sources to perform the following tasks for Reporting module:

- **Define a Rule**
- **Test a Rule**
- **Schedule Reports**
- **Add an Alert**
- **Add a Chart**
- **Test a Chart**

Note: You cannot use IMDB to generate Charts and Lists.

For more information, see the above topics in the *Reporting Guide*.

Configure Workbench

This topic provides high-level tasks to configure the Security Analytics Workbench.

Prerequisites

Ensure that you have:

- Installed the Security Analytics Workbench service in your network environment.
- Added a collection on the Workbench service.

Procedure

Refer the following table to configure Workbench:

Tasks	Reference
1. Add a RSA Archiver host with a Reporting Engine service.	See **Step 1: Add or Update a Host** in the *Hosts and Services Getting Started Guide*.
2. Add the Workbench service onto a Reporting Engine in your Security Analytics deployment.	See **Add Workbench Service** below.
3. Add Workbench as data source to Reporting Engine.	See **Step 3: Add Workbench as Data Source to Reporting Engine** in the *Archiver Configuration Guide*.

Add Workbench Service

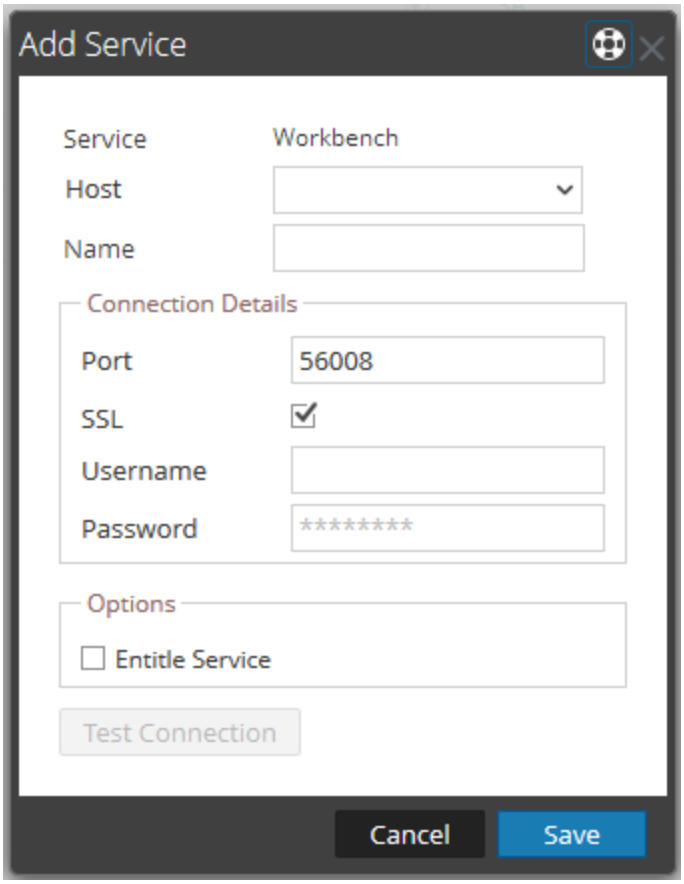
The Workbench service is installed on a Reporting Engine. The data that is to be restored must be restored on the Workbench service.

Note: Ensure that you have added a Reporting Engine service and applied license to it.

Tto add the Workbench service:

1. In the **Security Analytics** menu, select **Administration** > **Services**.
2. In the Services panel, click + > **Workbench**.

The Add Service dialog is displayed.



3. Provide the following details.

Field	Description
Host	Select a Reporting Engine host.
Name	Type a name for the service.
Port	Default port is 50007
SSL	Select **SSL** if you want Security Analytics to communicate with the service using SSL. The security of data transmission is managed by encrypting information and providing authentication with SSL certificates. **Note:** If you select SSL, ensure SSL is enabled in the System Configuration panel.
Username	Type the Username for the service.

Field	Description
Password	Type the password for the service.

4. Click **Test Connection** to determine if Security Analytics connects to the service.
5. When the result is successful, click **Save**.

   The added service is now displayed in the services panel.

Note: If the test is unsuccessful, edit the service information and retry.

Reporting Engine References

This topic introduces the Services Config view for the Reporting Engine, which has parameters that specifically pertain to the Reporting Engine.

You can specify the following configurations for the Reporting Engine:

- General Configurations
- Sources
- Output Actions
- Manage Logos

Note: In an earlier version of Security Analytics, Audit Configuration for Reporting Engine was configured using Audit Configuration tab of the Services Config view (**Administration > Services > Reporting Engine >**  **> View > Config > Audit Configuration**).

Audit Configuration is now available in the Global Auditing Configuration Panel (**Administration > System > Global Auditing**). For more information, see the **Configure Global Audit Logging** and **Global Audit Logging Configurations Panel** topics in the *System Configuration Guide*.

Topics

Reporting Engine: General Tab

This topic introduces the Services Config view > General tab for the Reporting Engine. The General tab for the Reporting Engine service in the Services Config view controls several settings that can tune the performance of a service and specify the user credentials for the service. These settings are used for the Reporting Engine service exclusively.

Procedure

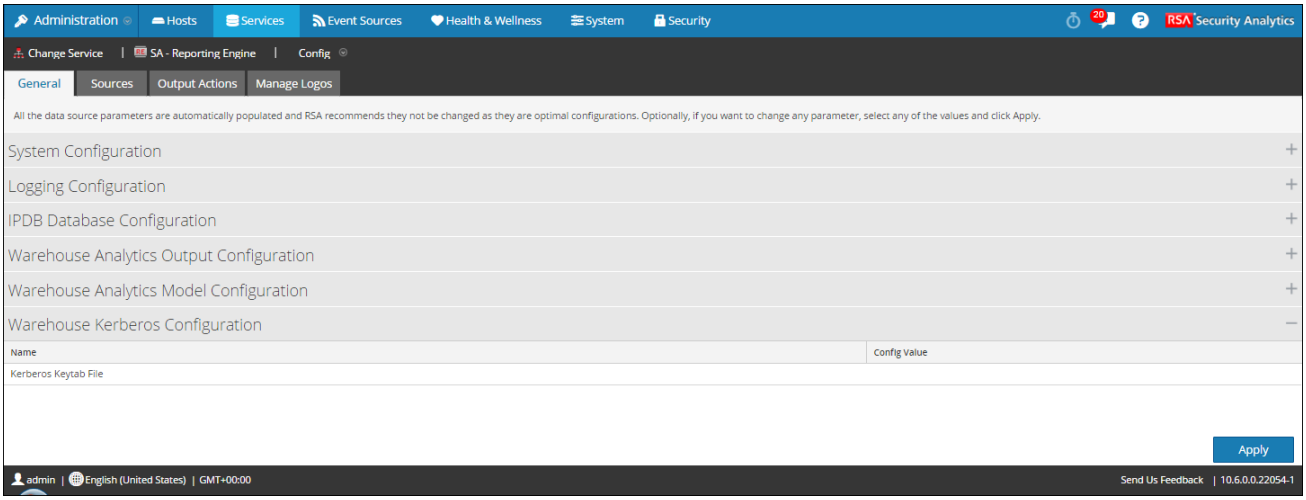
The required permission to access this view is **Manage Services**.

To access this view:

1. In the **Security Analytics** menu, click **Administration** > **Services**.
2. In the **Services** grid, select a **Reporting Engine** service.
3. Click  > **View** > **Config**.

   The Services Config view is displayed with the Reporting Engine **General** tab open.

An example of the General tab for a IPDB Extractor service is displayed.



Features

The Reporting Engine **General** tab includes six panels:

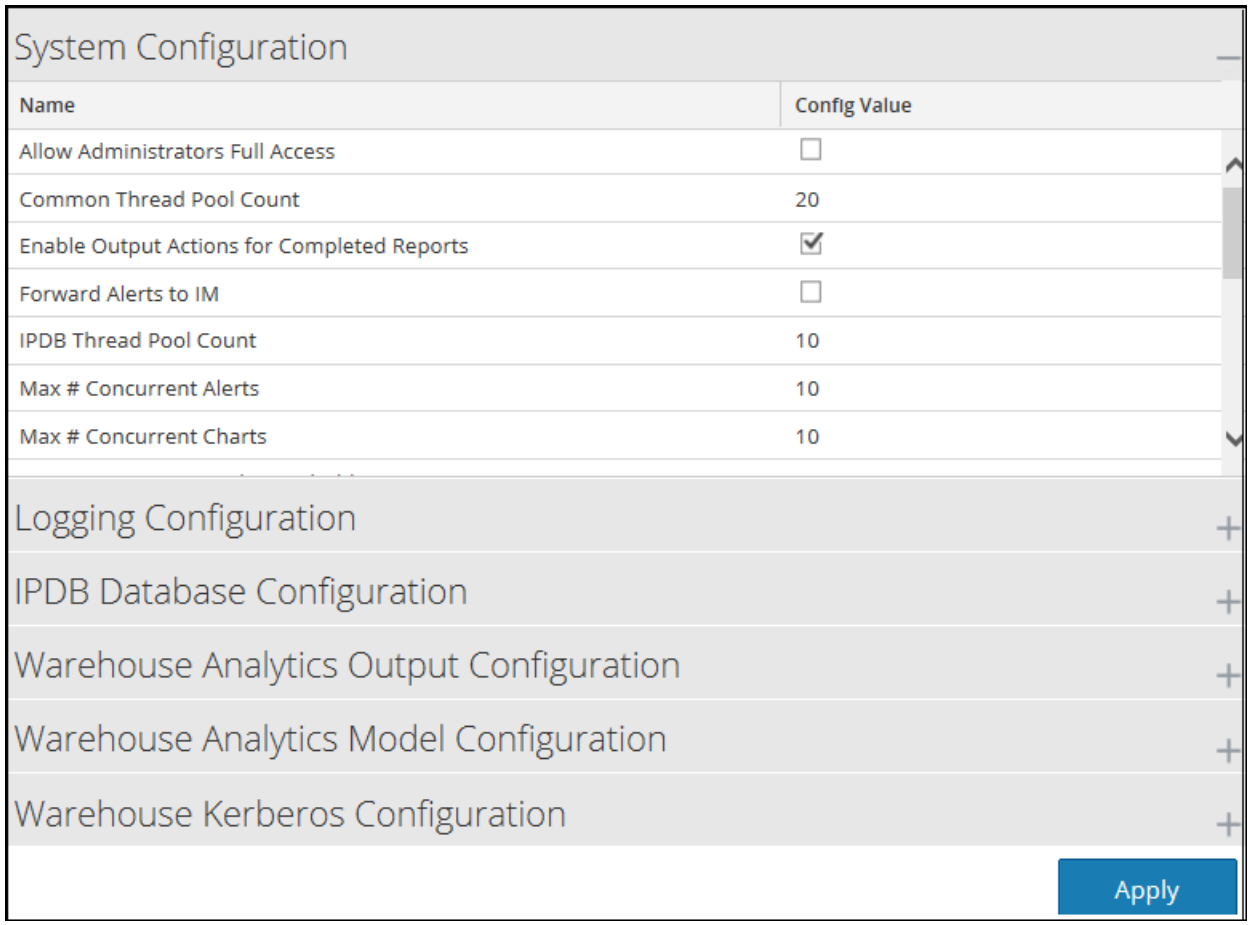
- System Configuration
- Logging Configuration

- IPDB Database Configuration
- Warehouse Analytics Output Configuration
- Warehouse Analytics Model Configuration
- Warehouse Kerberos Configuration

System Configuration

The System Configuration panel parameters for the Reporting Engine manage service configuration for a Reporting Engine service. When you add a Reporting Engine service, default values are in effect. RSA designed the default values to accommodate most environments and recommends that you do not edit these values because it may adversely affect performance.

The following figure shows the fields that can be configured in the System Configuration panel:



The following table describes the System Configuration panel features.

Name	Config Value
Allow Administrators Full Access	Select the checkbox if you want to access all the RE objects (Reports, Rule, Charts, Schedule, and List) created by other users (non-admin). By default, this is not enabled. **Note:** If you enable the checkbox and then disable it, the access on all RE objects that was enabled by checking the checkbox will not be accessible. But, if you have defined the access on specific objects via Permissions window (**Reports > Manage > RE Object >**  **> Permissions**), enabling/disabling this checkbox will not have impact on these objects.
Common thread pool count	The number of thread pools assigned for executing common tasks on the Reporting Engine. A valid value is an integer (**20** default).
Enable Output Actions for Completed Reports	Select the checkbox to process the output actions only for reports with all rule executions successful. By default, this is enabled. If disabled the output actions are processed for all scenarios (completed, partial, failure).
Forward Alerts to IM	Select the checkbox to forward all the alerts to Incident Management. By default, this is not enabled.
IPDB thread pool count	The number of thread pools assigned for executing IPDB tasks on the Reporting Engine. A valid value is an integer (**10** default).
Max# of Concurrent Alerts	The maximum number of alerts that can be run simultaneously. This has a direct impact on the RSA service against which the alerts are run, as each alert consumes a query thread on the RSA service. A valid value is an integer (**10** default).
Max # of Concurrent Charts	The maximum number of charts that can be run simultaneously. A valid value is an integer (**10** default).

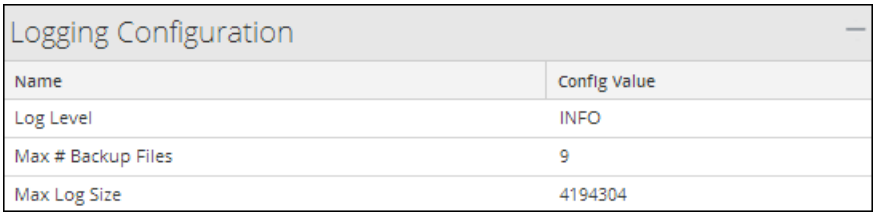
Name	Config Value
Max # of Concurrent LookupAndAdd Queries	The maximum number of parallel LookupAndAdd Queries that can be run per NWDB rule. A valid value is an integer (**2** default). When you increase this value, for better performance, you must ensure the NWDB data source is configured to handle the parallel queries.
Max # Concurrent List Value Reports	The maximum number of list value reports per schedule that can be generated in parallel. A valid value is an integer (**1** default).
Max # List Value Reports	The maximum number of list value reports generated, irrespective of the number of values in the list. A valid value is an integer (**10000** default).
Max rows stored per Rule (Billions)	The maximum number of rows that a rule can fetch when queried. A valid value is an integer (**100** default).
NWDB Info Queries Time Out	The info queries time out in seconds for NWDB server. A valid value is an integer (**0** default).
NWDB Maximum aggregate Rows	The maximum number of rows that is returned when an aggregation is used in the NWDB rule. A valid value is an integer (**1000** default).
NWDB Query Time out	The time out in seconds for NWDB server to time out the rule execution, if it cannot process the result in configured time. The default value is set to 0 which implies that there is no time out. A valid value is an integer.
Process output actions for successful reports only	Select this checkbox to process output actions only for reports whose all rule executions are successful. When you de-select this checkbox, output action will be triggered for partial, completed, and failed reports. **Note:** This is applicable for all output actions except for dynamic list output actions.

Name	Config Value
Retain Alert history for # days	The maximum number of days to retain the alert history and alert status. A valid value is an integer (**100** default).
Retain Chart history for # days	The maximum number of days to retain the chart history and chart status. A valid value is an integer (**30** default).
Retain Report history for # days	The maximum number of days the system retains report history and report status. A valid value is an integer (**100** default).
Schedule Thread pool count	The number of thread pools assigned for scheduled tasks (for example, clearing history) on the Reporting Engine. A valid value is an integer (**5** default).

Logging Configuration

The Logging Configuration panel parameters for the Reporting Engine manages logging configuration for a Reporting Engine service. When you add a Reporting Engine service, default values are in effect. RSA designed the default values to accommodate most environments and recommends that you do not edit these values because it may adversely affect performance.

The following figure shows the fields that can be configured in the Logging Configuration panel.



The following table describes the Logging Configuration panel features.

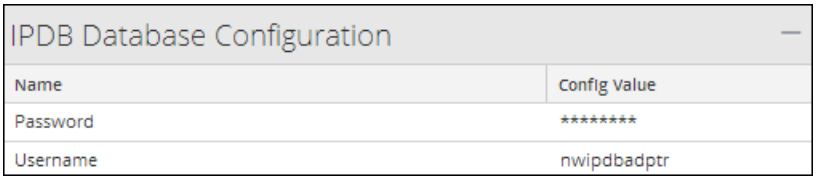
Name	Config Value
Log Level	The logging level that determines the scope of information included in log files. Possible values are: • **ERROR** • **WARN** • **INFO** (default) • **DEBUG** • **ALL**
Maximum # Backup Files	The maximum number of backup log files the system retains. A valid value is an integer (**9** default).
Max Log Size	The maximum size (in bytes) of the primary log file. A valid value is an integer (**4194304** default).

For more information on Reporting Engine logging, see Reporting Engine Log File Parameters.

IPDB Database Configuration

The IPDB Database Configuration panel provides a way to specify the IPDB password when implementing the IPDB on this Reporting Engine.

The following figure shows the fields that can be configured in the IPDB Database Configuration panel:



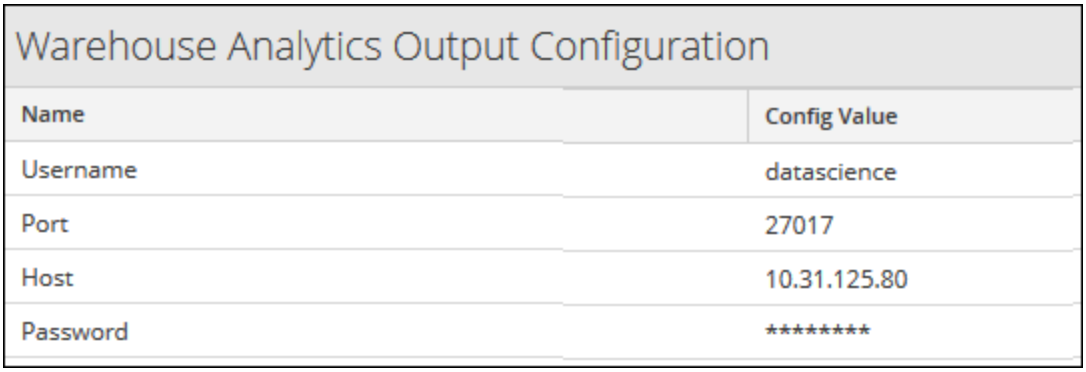
The following table describes the IPDB Database Configuration panel features.

Name	Config Value
Password	The password for **nwipdbadptr** user. RSA inserts a temporary password that you must replace with the actual IPDB password when you implement the IPDB on this Reporting Engine.
User Name	**nwipdbadptr** You cannot edit this field.

Warehouse Analytics Output Configuration

The Warehouse Analytics Output Configuration panel provides a way to specify the Warehouse Analytics Output configuration on this Reporting Engine.

The following figure shows the fields that can be configured in the Warehouse Analytics Output Configuration panel:



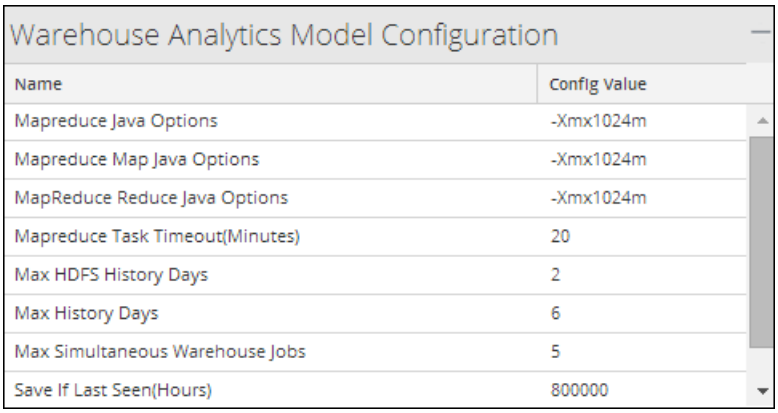
The following table describes the Warehouse Analytics Output Configuration panel features.

Name	Config Value
Name	**Config Value**
Username	The username for the warehouse analytics user.
Port	The port for the output Mongo DB used by warehouse analytics.
Host	The host for the output Mongo DB used by warehouse analytics.
Password	The password for the warehouse analytics user.

Warehouse Analytics Model Configuration

The Warehouse Analytics Model Configuration panel provides a way to specify the Warehouse Analytics Model configuration on this Reporting Engine.

The following figure shows the fields that can be configured in the Warehouse Analytics Model Configuration panel:



The following table describes the Warehouse Analytics Model Configuration panel features:

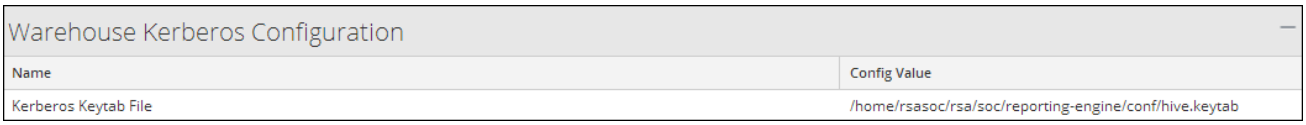
Name	Config Value
Mapreduce Java Options	The JVM Parameters for Hadoop MapReduce task tracker child JVM. By default, the value is **-Xmx1024m**.
Mapreduce Map Java Options	The parameter which controls the JVM parameters for Map jobs inside the Hadoop cluster. By default, the value is **-Xmx1024m**.
MapReduce Reduce Java Options	The parameter which controls the JVM parameters for Reduce jobs inside the Hadoop cluster. By default, the value is **-Xmx1024m**.
Mapreduce Task Timeout (Minutes)	The number of minutes before a task is terminated when a MapReduce framework titles it as non-responsive or idle. A valid value is an integer (**20** default).
Max HDFS History Days	The maximum number of days to maintain the temporary and output files of the job in HDFS. A valid value is an integer (**2** default).
Max History Days	The maximum number of days to maintain the job output in Mongo DB. A valid value is an integer (**6** default).
Max Simultaneous Warehouse Jobs	The parameter which controls the maximum number of parallel jobs executed through the Warehouse Analytics framework. A valid value is an integer (**1** default).

Name	Config Value
Save If Last Seen (Hours)	The parameter to save the keys from the job output is they were not seen in the last 'n' hours. A valid value is an integer (**800000** default).
Threshold Score	The parameter to save the keys from the job output to watchlists for use by ESA only if the score is greater than 'n'. A valid value is an integer (**55** default).

Warehouse Kerberos Configuration

The Warehouse Kerberos Configuration panel provides a way to specify the Kerberos Keytab file on this Reporting Engine.

The following figure shows the field that can be configured in the Warehouse Kerberos Configuration panel:



The following table describes the Kerberos Configuration panel features:

Name	Config Value
Kerberos Keytab File	The Kerberos keytab file location. For example, /home/rsasoc/rsa/soc/reporting-engine/conf/hive.keytab.

Reporting Engine Manage Logos Tab

This topic introduces the logo configuration tasks available in the Services Config View > Manage Logos tab for the Reporting Engine. The Manage Logos tab in the Services Config view helps manage the logos associated with the Reporting Engine. The Manage Logos tab consists of a single panel with a toolbar and a grid that lists the logos.

You can upload the logos that you can use in the report. After you upload the logo, you can set any logo as a default logo which will be automatically used in all scheduled reports. You can choose to override the default logo with any other logo listed in this tab when you schedule a report. For more information, see Select a Logo Dialog.

The supported image formats are:

- .jpg
- .png
- .gif

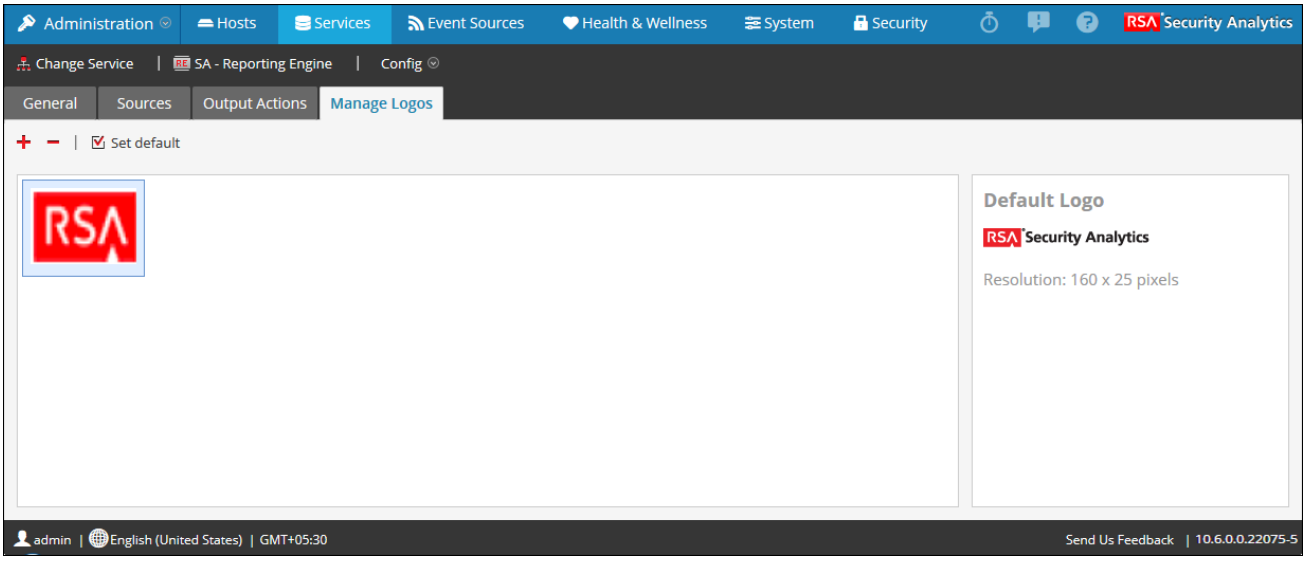
Note: The logo to be uploaded should not exceed 500 KB.

The required permission to access this view is Manage Services.

To access this view:

1. In the **Security Analytics**menu, select **Administration**> **Services**.
2. In the **Services Grid**, select a **Reporting Engine**service.
3. Select  > **View** > **Config**.
4. Select the **Manage Logos** tab.

The **Services Config View** is displayed with the Reporting Engine **Manage Logos** tab open.



You can perform the following actions on the Manage Logos Tab.

Icon	Actions
+	Add new logos from the local directory of the system to the Reporting Engine. **Note:** The logo size cannot exceed 500 KB. The logos chosen must be of the following file types: * .jpg * .gif * .png
−	Removes logos from the Reporting Engine. **Note:** By performing (Ctrl+click), you can select multiple logos to delete.
Set default	Sets the default logo for a Reporting Engine. This is the logo Security Analytics defaults to in the **Logo** panel of the Schedule a Report view. **Note:** If no default logo is selected, the RSA logo is displayed.

Reporting Engine Output Actions

This topic introduces the service configuration parameters available in the Output Actions tab of the Services Config view for the Reporting Engine. Output action is the action configured for a report or an alert execution. The output action can be configured from the Output Actions tab in the Services Config view for the Reporting Engine. This tab consists of the following panels:

- SA Configuration
- Simple Mail Transfer Protocol (SMTP)
- Simple Network Management Protocol (SNMP)
- Syslog
- Simple File Transfer Protocol (SFTP)
- Uniform Resource Locator (URL)
- Network Share

Each of these output actions serve certain purposes. For instance, Syslog output action is used specifically for Reporting Engine Alerts, whereas, SFTP, URL, and Network Share output action is used specifically for Reporting Engine Reports.

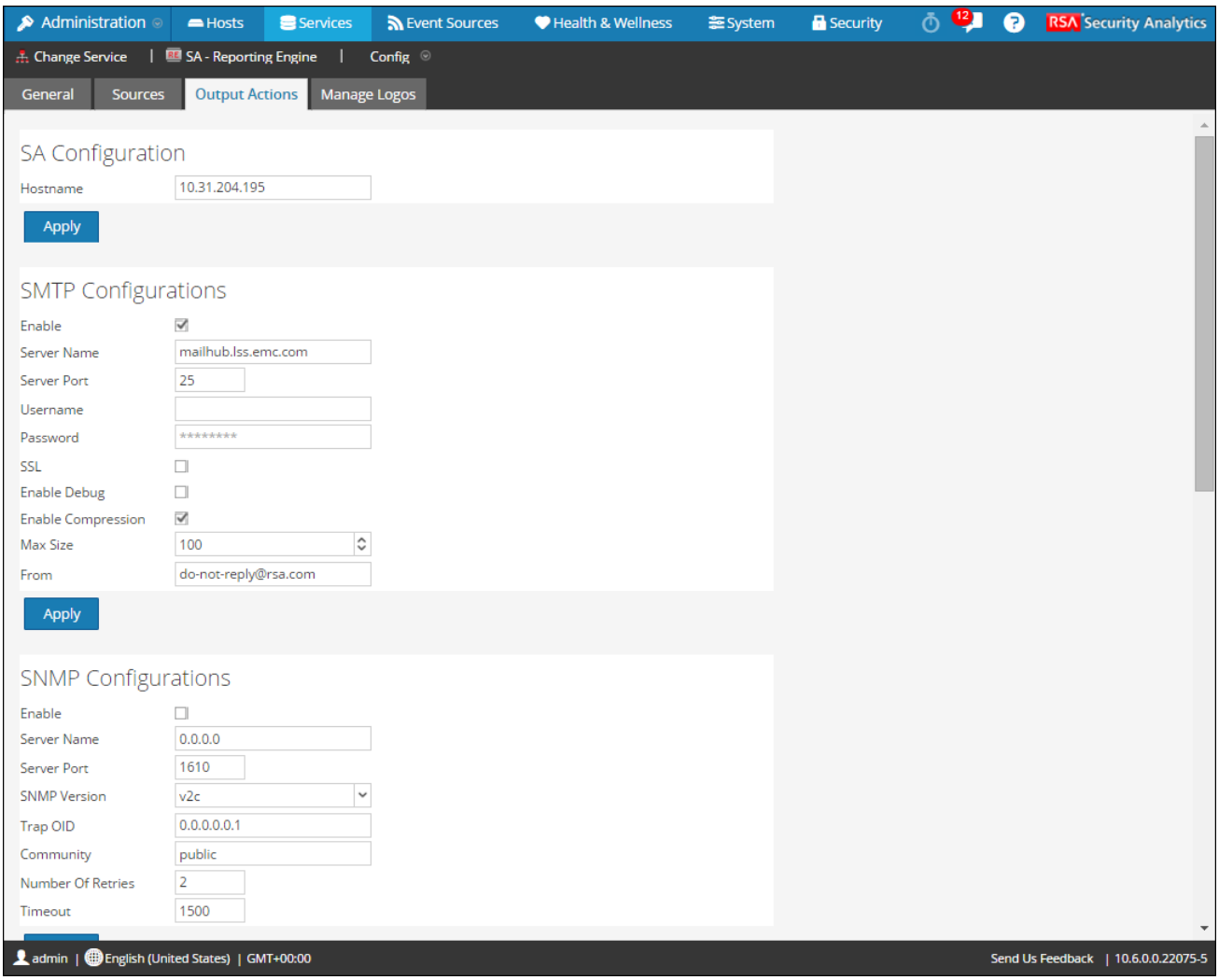
The required permission to access this view is **M anage Services**.

To access this view:

1. In the **Security Analytics** menu, select **Administration** > **Services**.
2. In the **Services Grid**, select a **Reporting Engine** service.
3. Click  > **View** > **Config**.
4. Click the **Output Actions**tab.

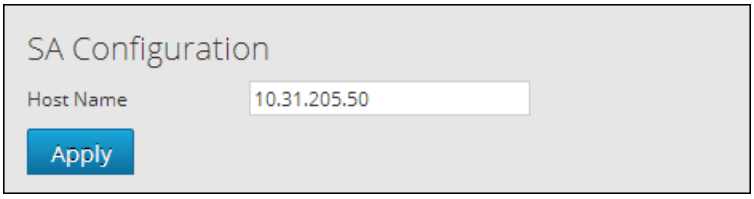
   The **Services Config View** is displayed with the Reporting Engine **Output Actions** tab

open.



SA Configuration

The following figure shows the SA Configuration on the Output Actions Tab.



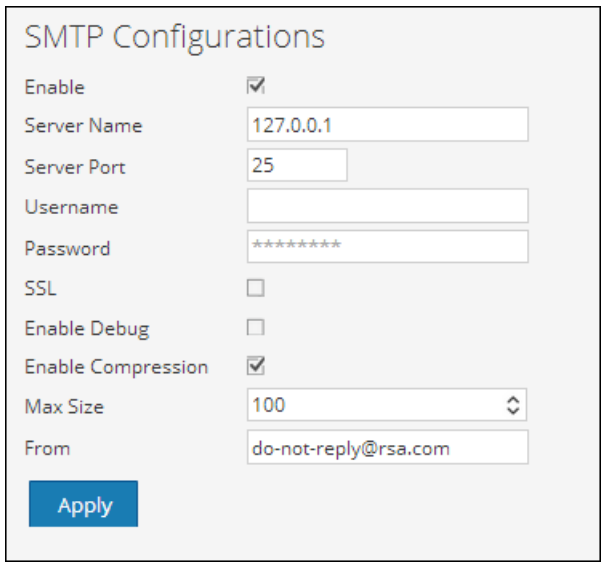
The following parameters identify the Security Analytics host that is associated with the Reporting Engine.

Name	Config Value
Host Name	IP Address or Hostname of the Security Analytics server. You must specify this parameter for all kind of deployments so that you can refer to this address to create investigation links to Security Analytics from Reports, Alerts, and so on. The Security Analytics uses this parameter to correctly generate: • SMTP Output Action • SNMP Output Action • Syslog Output Action • SFTP Output Action • URL Output Action • Network Share Output Action • Hyperlinks for meta values in Report PDFs
Apply	Update the configuration.

SMTP

Once an execution is completed, an email notification is sent to the user based on the SMTP configuration.

The following figure shows the SMTP Configuration on the Output Actions Tab.



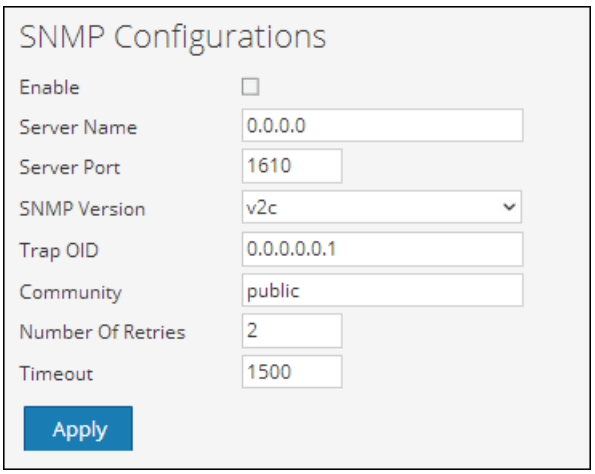
The following parameters manage SMTP (email) output action configuration for a Reporting Engine service. When you add a Reporting Engine service, default values are in effect. You must modify the **Config Values** of these parameters according to the requirements of your enterprise.

Name	Config Value
Enable	Check this box to enable SMTP as an output action for both alert and report from this Reporting Engine. Default value is Enable.
Server Name	Specify the hostname or IP Address of the server on which the target SMTP server runs. Default value is **0.0.0.0**.
Server Port	Specify the SMTP server port number. Default value is **25**.
Username	Specify the username of your SMTP account. Default value is blank.
Password	Specify the password of your SMTP account.
SSL	Check this box to use Secure Socket Layer (SSL) to communicate with the SMTP server. Default value is do not use SSL.
Enable Debug	Check this box to enable debugging. Default value is do not enable debug.
Enable Compression	Check this box to enable compression. Default value is enable compression. If this value is enabled, the output files will have ".zip" extension.
Max Size	Specify the maximum size of attachments that can be sent. Default value is 100.
From	Specify the email address from which Security Analytics sends all messages. Default value is do-not-reply@ rsa.com.
Apply	Update the configuration.

SNMP

Once an execution is completed, a trap notification is sent to the user based on the SNMP configuration.

The following figure shows the SNMP Configuration on the Output Actions Tab.



The following parameters manage SNMP (messages to network-attached services) output action configuration for a Reporting Engine service. When you add a Reporting Engine service, default values are in effect. You must modify the **Config Values** of these parameters according to the requirements of your enterprise.

Name	Config Value
Enable	Check this box to enable SNMP output action as an output for alert messages from this Reporting Engine. Default value is Disable.
Server Name	Specify the hostname or IP Address of the server on which the target SNMP server runs. Default value is **0.0.0.0**.
Server Port	Specify the port number of the server on which the target SNMP server listens for faults and exceptions. Default value is **1610**.
SNMP Version	Specify the version number of the SNMP protocol Security Analytics uses to send SNMP traps.
Trap OID	Specify the object identification number that identifies the type of trap to send. Default value is **0.0.0.0.0.1**.
Community	Specify the SNMP group to which Security Analytics belongs. The default value is **public**.
Number Of Retries	Specify the maximum number of times Security Analytics tries to resend the alert message through SNMP. Default value is **2**.

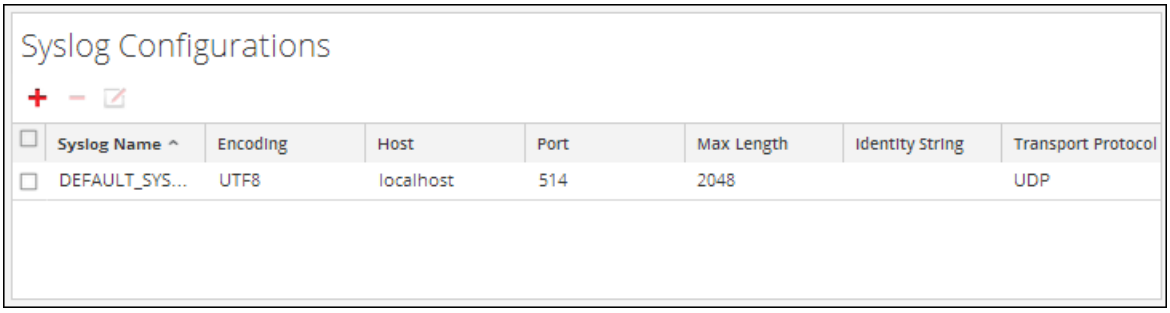
Name	Config Value
Timeout	Specify the number of seconds after which Security Analytics times out (stops trying to send SNMP alerts). Default value is **1500**.
Apply	Update the configuration.

Syslog

Once an execution is completed, all notifications are sent via Syslog messages to a particular host based on the Syslog configuration. Multiple Syslog servers can be configured on the Syslog Configuration panel.

Note: After upgrade to 10.4, the Syslog configuration available from previous versions would be migrated and saved as "DEFAULT_SYSLOG".

The following figure shows the Syslog Configuration on the Output Actions Tab.



The following table lists the operations in the Syslog Configuration section.

Operation	Description
+	Create a Syslog configuration.
−	Delete a Syslog configuration.
✎	Edit a Syslog configuration.

The following parameters manage syslog output action configuration for a Reporting Engine service. When you add a Reporting Engine service, you can define values for this output configuration, as no default values are available for this configuration. You must modify the **Config Values** of these parameters according to the requirements of your enterprise.

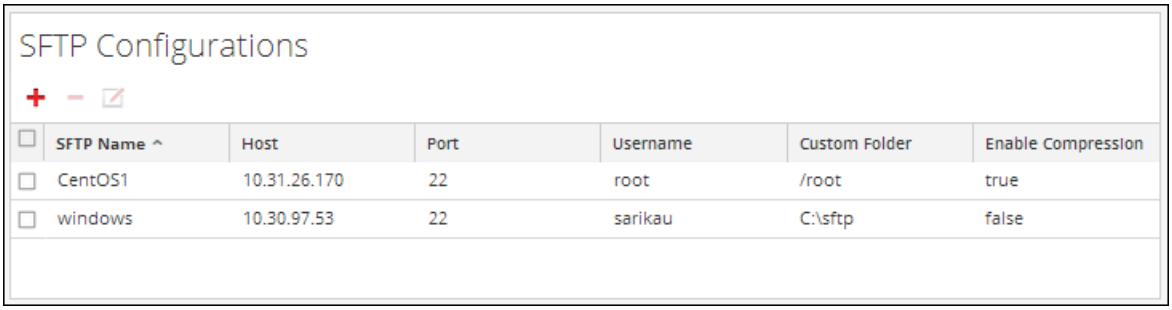
Name	Config Value
Syslog Name	The name of the Syslog configuration. **Note:** You cannot create a Syslog configuration with a name that already exists in the Reporting Engine Syslog configuration list.
Encoding	Specify the internationalization encoding for Syslog messages. Default value is **UTF8**.
Server Name	Specify the hostname or IP Address of the server on which the target Syslog process runs. Default value is blank.
Server Port	Specify the port number of the server on which the target Syslog server listens for faults and exceptions. Default value is **514**.
Max Length	Specify the maximum size (in bytes) of each Syslog alert message. Default value is **2048**. If **UDP** is the transport type and the Syslog message size is greater than 1024 bytes, you must configure a Syslog server that supports message sizes greater than 1024 bytes.
Identity String	Specify the string Security Analytics inserts as a prefix in all Syslog alert messages. Default value is blank.
Include Local Hostname	Check this box to include the local hostname in all Syslog alert messages. Default value is do not include local hostname.
Truncate Message	Check this box to truncate all Syslog alert messages. Default value is do not truncate Syslog messages.
Use Identity	Check this box to use the IDENT protocol. Default value is does not use this protocol.
Include Local Timestamp	Check this box to include the local timestamp in all Syslog alert messages. Default value is do not include local timestamp.
Transport Protocol	Specify the transport type for Syslog message delivery. There are three parts to the Syslog transport type: UDP, TCP, and SECURE_TCP. Default value is **UDP**.

Name	Config Value
Syslog Message Delimiter	Specify the delimiter for the Syslog message. There are three delimiters: CR, LF, CRLF. Default value is **CR**. **Note:** This field populates when you select TCP or SECURE_TCP as the transport protocol.
Trust Store Password	Specify the password for the Trust store. **Note:** This field populates when you select SECURE_TCP as the transport protocol.
Key Store Password	Specify the password for the Key store. **Note:** This field populates when you select SECURE_TCP as the transport protocol.
Save	Save the configuration.

SFTP

Once an execution is completed, you can send or transfer files to a remote location based on the SFTP configuration.

The following figure shows the SFTP Configuration on the Output Actions Tab.



The following table lists the operations in the SFTP Configuration section.

Operation	Description
+	Create an SFTP configuration.
−	Delete an SFTP configuration.

Operation	Description
	Edit an SFTP configuration.

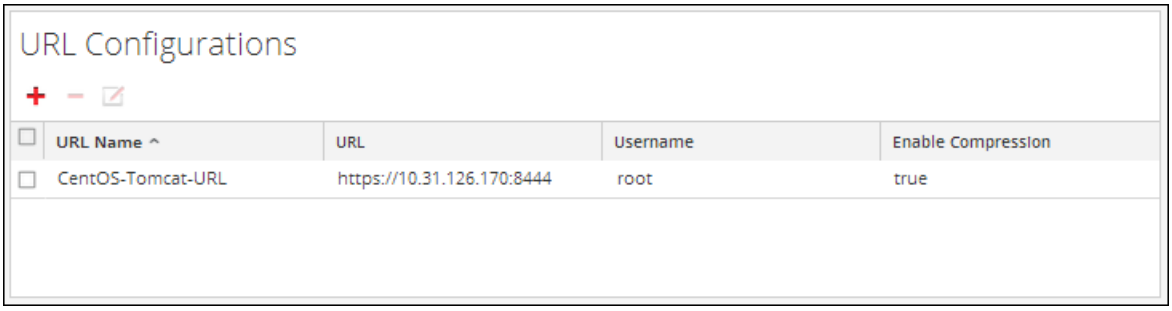
The following parameters manage SFTP (file transfer to a local drive) output action configuration for a Reporting Engine service. When you add a Reporting Engine service, you can define values for this output configuration, as no default values are available for this configuration. You must modify the **Config Values** of these parameters according to the requirements of your enterprise.

Name	Config Value
SFTP Name	The name of the SFTP configuration. **Note:** You cannot create an SFTP configuration with a name that already exists in the Reporting Engine SFTP configuration list.
Host	The IP Address or Hostname of the Reporting Engine server associated with the file transfer.
Port	If you want to use a different port than the default port, enter a port number. Default value is **22**.
Username	Specify the username for the SFTP configuration.
Password	Specify the password for the SFTP configuration.
Custom Folder	Select an SFTP location where you want to transfer the file to. You can use the pre-defined Windows or Linux directory structure in the custom folder path. For example, **/root/Downloaded_Files**. **Note:** If the directory does not exist, RE will create the directory in the custom folder path and copy files to this directory.
Enable Compression	Select this checkbox to enable compression. Default value is enable compression. If this value is enabled, the output files will have ".zip" extension.

URL

Once an execution is completed, the output files are published to a URL based on the URL configuration.

The following figure shows the URL Configuration on the Output Actions Tab.



The following table lists the operations in the URL Configuration section.

Operation	Description
+	Create a URL configuration.
−	Delete a URL configuration.
✎	Edit a URL configuration.

The following parameters manage URL (file transfer to a URL) output action configuration for a Reporting Engine service. When you add an Reporting Engine service, you can define values for this output configuration, as no default values are available for this configuration. You must modify the **Config Values** of these parameters according to the requirements of your enterprise.

Name	Config Value
URL Name	The name of the URL configuration. **Note:** You cannot create a URL configuration with a name that already exists in the Reporting Engine URL configuration list.
URL	The URL address associated with the file transfer.
Username	Specify the username for the URL configuration.
Password	Specify the password for the URL configuration.

Name	Config Value
Enable Compression	Select this checkbox to enable compression. Default value is enable compression. If this value is enabled, the output files will have ".zip" extension.

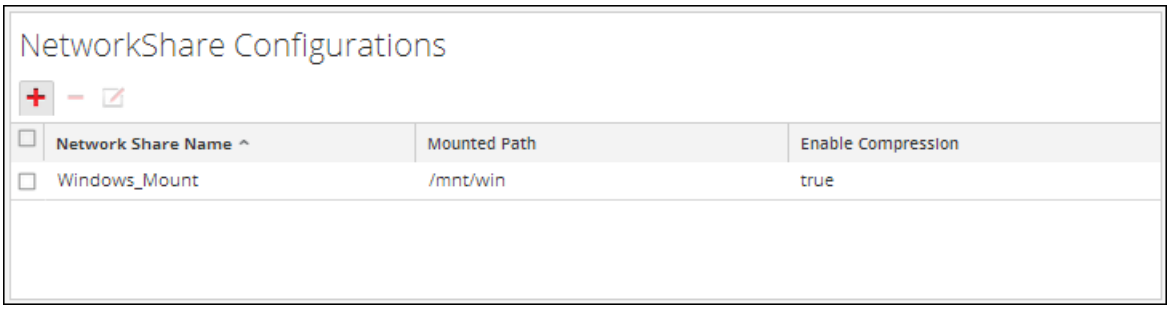
After the URL is configured, the files will be copied under the "URL_OUTPUT_ACTION" directory and the following parameters are sent to the server along with the compressed file.

Name	Config Value
filename	The name of the file.
filesize	The file size in bytes.
filetype	The file type associated with the file.
filechecksum	The number computed from a file that can be used to confirm that this is the one you expect and has been downloaded and stored properly.
hashingalgorithm	The hashing algorithm used to calculate the file checksum.
reportname	The name of the downloaded report.
executionid	The execution id associated with the report execution.
reportexecutionstarttime	The start time the report was executed.
status	The report creation status.
status description	The status description.

Network Share

Once an execution is completed, you can transfer the output files to a mounted path or shared location based on the Network Share configuration.

The following figure shows the Network Share Configuration on the Output Actions Tab.

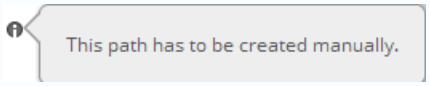


The following table lists the operations in the Network Share Configuration section.

Operation	Description
+	Create a Network Share configuration.
−	Delete a Network Share configuration.
✎	Edit a Network Share configuration.

The following parameters manage Network Share (file transfer to a shared location on the network) output action configuration for a Reporting Engine service. When you add a Reporting Engine service, you can define values for this output configuration, as no default values are available for this configuration. You must modify the **Config Values** of these parameters according to the requirements of your enterprise.

Name	Config Value
Network Share Name	The name of the Network Share. **Note:** You cannot create a Network Share configuration with a name that already exists in the Reporting Engine Network Share configuration list.
Mounted Path	The path (location) associated with the file transfer. You can use the pre-defined Linux directory structure in the mounted path. For example, **/mnt/win**. **Note:** The 'rsasoc' user must have read-write access to the specified Network Share mounted path.

Name	Config Value
	Click to view how the mounted path is created. This pop-up notifies that you must manually create the mounted path.
Enable Compression	Select this checkbox to enable compression. Default value is enable compression. If this value is enabled, the output files will have ".zip" extension.

Reporting Engine Sources Tab

This topic introduces the services configuration parameters available in the Sources tab of the Services Config view for the Reporting Engine. The Sources tab for the Reporting Engine service in the Services Config view controls that data sources associated with a Reporting Engine. The Source tab consists of a single panel with a toolbar and a grid that lists the data sources associated with the Reporting Engine.

All procedures associated with this tab are available in Configure Reporting Engine or Additional Procedures for Configuring the Reporting Engine.

About the Data Sources

The data sources available to the Reporting Engine for which you are defining reports and defining alerts are:

- **IPDB Data Sources** - The Internet Protocol Database (IPDB) data source contains both normalized and raw event messages. It stores all collected messages in a file system organized by event source (service), IP address, and time (year/month/day) with index files to facilitate searches (report and queries).
- **NWDB Data Sources** - The NetWitness Database (NWDB) data sources are Decoders, Log Decoders, Brokers, Concentrators, Archiver, and Collection.

  Note: When a data privacy plan has been implemented to limit access to sensitive data on a data source, you must configure different service accounts in Reporting Engine for privileged and non-privileged users. To configure different service accounts for data privacy, you can add more than one NWDB data source. This procedure is available under Additional Procedures for Configuring the Reporting Engine.
- **Warehouse Data Sources** - The Warehouse data sources are Pivotal and MapR.
- **IMDB Data Source** - The Incident Management Data Base data sources are Reporting Engine, ESA, Malware, ECAT, and Web Threat Detection. IMDB is used to store the alerts and incidents reports.

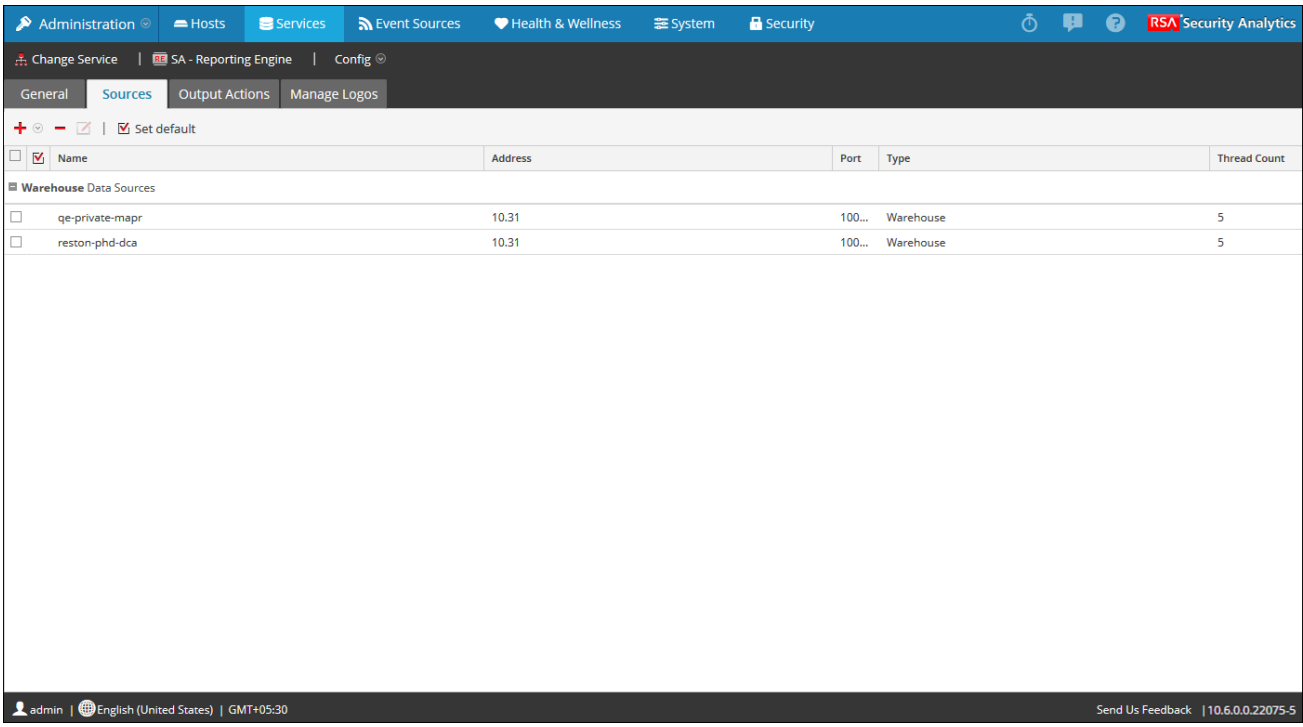
If you set a source as the default data source, Security Analytics uses that source when you create reports and alerts unless you choose to override it with one of the other sources listed in this tab.

Note: You can manage access control to NWDB and Warehouse Data Sources. For more information, see Additional Procedures for Configuring the Reporting Engine.

To access this view:

1. In the **Security Analytics** menu, select **Administration** > **Services**.
2. In the **Services Grid**, select a **Reporting Engine** service.
3. Click  > **View** > **Config**.
4. Select the **Sources** tab.

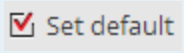
   The **Service Config View** is displayed with the Reporting Engine **Sources** tab open.



Features

You can perform the following actions on the Sources tab:

Icon	Actions
+	Adds new services as data sources for Reporting Engine. To add a Warehouse as a data source, see Add Warehouse as a Data Source to Reporting Engine. Add existing services ((Optional) Add Archiver as Data Source to Reporting Engine, (Optional) Add Workbench as Data Source to Reporting Engine, (Optional) Add Collection as Data Source to Reporting Engine) as data sources for Reporting Engine.

Icon	Actions
	Removes data sources from a Reporting Engine.
	Configures Data Source Permissions. This is enabled only for NWDB and Warehouse Data Sources. For more information, see Configure Data Source Permissions.
	Sets the default data sources for a Reporting Engine. This is the source to which Security Analytics defaults in the **Datasource** field of the following views: • Rule Definition view. • Create/Modify Alert view.

The data sources are listed under the different categories as follows:

- IPDB Data Sources category : Security Analytics displays the IPDB Extractor service data sources.
- NWDB Data Sources category, Security Analytics displays the NetWitness data sources.
- Warehouse Data Sources category : Security Analytics displays the Warehouse data sources.

Column	Description
	Clicking the check box selects the data source. After you select it, you can use toolbar to remove the source or set the source as the default.
Name	Displays the name of the data source.
Address	Displays the IP Address of the data source.
Port	Displays the port of the data source.
Type	Displays the service type of the data source.
Thread Count	Displays the thread pool size used for executing rules on the data source. For IPDB data source, this column is blank, instead the thread pool size is displayed in the **General** tab using the **IPDB thread pool count** parameter.

Reporting Engine Log File Parameters

This topic describes how you can access the Reporting Engine log files. The Reporting Engine stores the following logs in the **rsasoc/rsa/soc/reporting-engine/log** directory:

- Current logs in the **reporting-engine.log**file.
- Backup copies of previous logs in the **reporting-engine.log.*** file.
- All UNIX script logs in the files that have the following syntax: **reporting-engine.sh_** ***timestamp*.log**(for example, **reporting-engine.sh_20120921.log**)

The Reporting Engine rarely writes command line error messages to the **rsasoc/nohup.out**file.

The Reporting Engine appends the log messages and output written by upstart daemon and the commands used to start the reporting-engine to the **/var/log/secure** directory.

An upstart log file is a system log file so only the root user can read it. The Reporting Engine generates log files, retains backup copies of previous log files, stores UNIX script log files and appends upstart log files to another directory.