NetWitness® Platform

Version 12.5.0.0

Reporting Engine Configuration Guide

NETWITNESS
Platform

Contact Information

NetWitness Community at https://community.netwitness.com contains a knowledge base that answers common questions and provides solutions to known problems, product documentation, community discussions, and case management.

Trademarks

RSA and other trademarks are trademarks of RSA Security LLC or its affiliates ("RSA"). For a list of RSA trademarks, go to https://www.rsa.com/en-us/company/rsa-trademarks. Other trademarks are trademarks of their respective owners.

License Agreement

This software and the associated documentation are proprietary and confidential to RSA Security LLC or its affiliates are furnished under license, and may be used and copied only in accordance with the terms of such license and with the inclusion of the copyright notice below. This software and the documentation, and any copies thereof, may not be provided or otherwise made available to any other person.

No title to or ownership of the software or documentation or any intellectual property rights thereto is hereby transferred. Any unauthorized use or reproduction of this software and the documentation may be subject to civil and/or criminal liability. This software is subject to change without notice and should not be construed as a commitment by RSA.

It is advised not to deploy third-party repos or perform any change to the underlying NetWitness Operating System that is not part of the supported NetWitness version. Any such change outside of the NetWitness approved image may result in a service or functionality conflict and require a reimage of the NetWitness system to bring NetWitness back to an optimized functional state. In the event a third-party repo is deployed, or other non-supported change is made by the customer without NetWitness approval, the customer takes full responsibility for any system malfunction until the issue can be remediated through troubleshooting efforts or a reimage of the service.

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 NetWitness Community. 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

Use, copying, and distribution of any RSA Security LLC or its affiliates ("RSA") software described in this publication requires an applicable software license.

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

THE INFORMATION IN THIS PUBLICATION IS PROVIDED "AS IS." RSA MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Miscellaneous

This product, this software, the associated documentations as well as the contents are subject to NetWitness' standard Terms and Conditions in effect as of the issuance date of this documentation and which can be found at https://www.netwitness.com/standard-form-agreements/.

September, 2024

Contents

How Reporting Engine Works

NetWitness Reporting Engine is a service on the NetWitness Admin Server. It facilitates the data extraction from different data sources to generate reports for compliance and analysis. Reporting Engine stores the definitions of the charts, rules, reports and alerts that are used to generate reports, charts and alerts.

Reporting Engine configuration includes configuring the data sources, definitions of outputs or notifications and parameters to improve the performance of data extraction and report, chart, and alert generation.

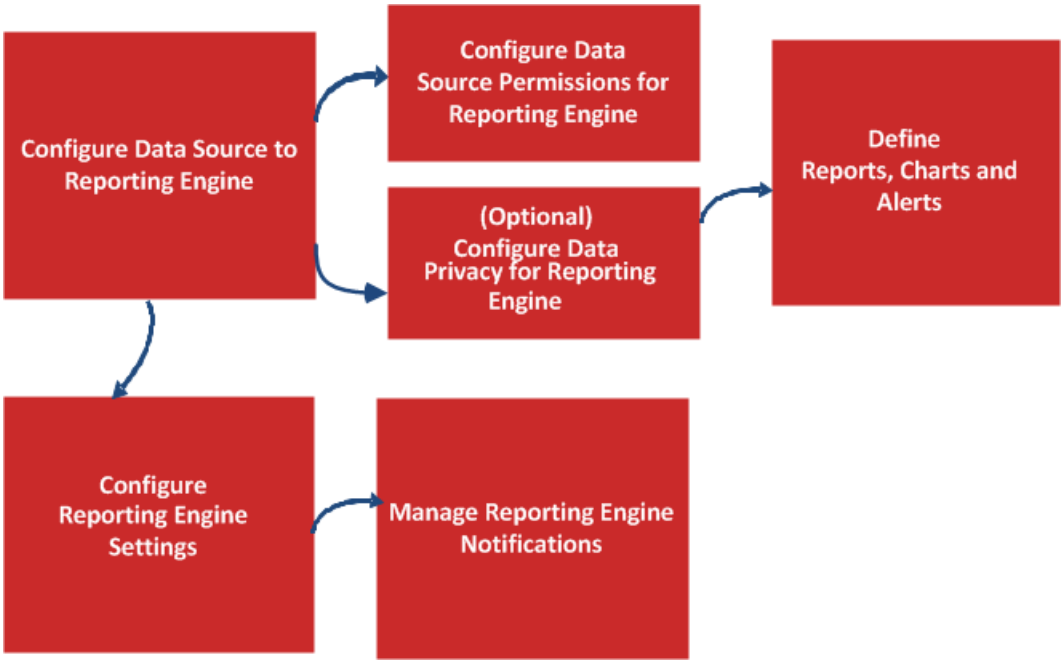
When you install the NetWitness, Reporting Engine is automatically installed as a service. This enables the Reports, Charts, and Alerts to be maintained in the NetWitness and be available to view, download reports as PDF or CSV format, download charts as PDF and be added as dashlets.

For the Reporting Engine to run reports and alerts based on the data drawn from a data source, you must associate a data source, or multiple data sources to a Reporting Engine. There are three types of data sources:

- NWDB - The NetWitness Database (NWDB) data sources are Decoders, Log Decoders, Brokers, Concentrators, Archiver, and Collection. Reporting Engine supports the generation of reports, alerts, and charts.
- Warehouse - The Warehouse data sources are Horton Works and MapR which collects information from the Warehouse Connector and generates reports and alerts. This data source generates Reports only.
- Respond - Respond is used to generate reports on alerts and incidents. This data source generates Reports only.

Workflow

The following workflow shows an overview of the Reporting Engine configuration which enables the user to generate Reports, Charts, and Alerts.



Configure the Reporting Engine

On installation of the NetWitness Server, the Reporting Engine service is automatically available and some parameters are pre-populated with default values to achieve optimal results.

Make sure that the data sources are deployed and configured in the NetWitness. For more information, see "Add Service or Edit Service Dialog" topic in the *Host and Service Configuration Guide*.

You can perform the following tasks:

- Check Live for the latest data source content and deploy it on a regular basis. (For more information, see "Manage Live Resources" topic in the in *Live Services Management Guide*).
- (Optional) Add Additional Space for Large Reports.

Configure the Data Sources

You must configure NWDB, Warehouse, and Respond to generate Reports, Charts, and Alerts. Optionally, you can also configure Archiver, Collection, and Workbench data sources.

IMPORTANT: If you change the admin password on a NetWitness service that is used as a Reporting Engine data source, you must remove and then re-add the service as a data source.

Note: To execute Reports and Charts on an Analyst UI, make sure the admin adds the data sources to each Reporting Engine instance from the admin node using the relevant procedure described in this topic.

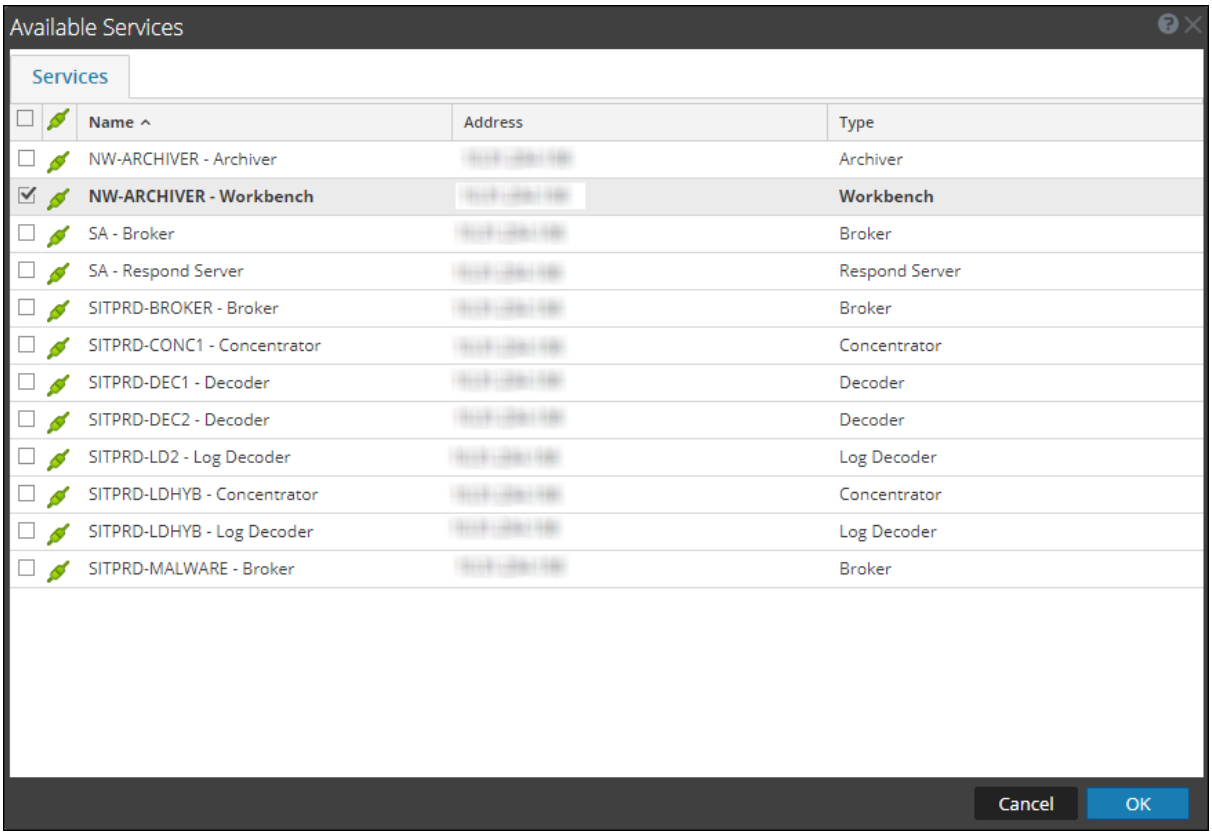
Configure a NWDB Data Source

To add a NWDB data source:

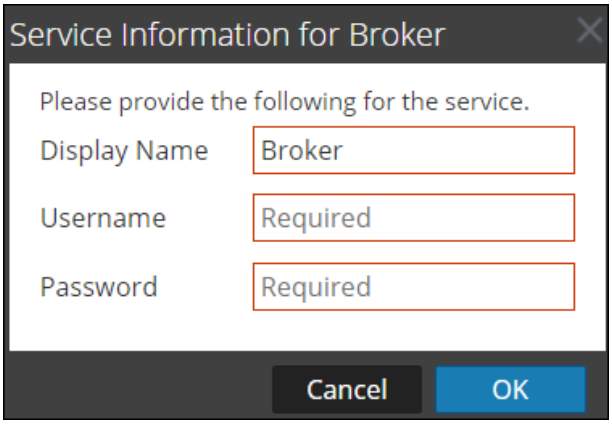
1. Go to  **(Admin) > Services**.
2. In the **Services**, select **Reporting Engine** service.
3. Click  > **View** > **Config**

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

   The **Available Services** dialog is displayed.



5. Select a NWDB service you want to add and click **OK**.
6. In the Service Information for Broker dialog, enter the service information for the service and click **OK**. In this example, we are adding a Broker service.



7. The service is displayed in the Sources tab when it is successfully added.

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.

Configure a Warehouse Data Source

You can add the warehouse data source to Reporting Engine, so that you can extract the data from the required services, store them in MapR or Horton works and generate Reports and Alerts. The procedure to configure Warehouse as a data source differs. To extract data from a Warehouse data source, you must configure it using the following procedure.

Note: Warehouse Connector is still supported, as it is reporting against a warehouse in NetWitness.

Prerequisite

Make sure you:

- Add a Warehouse Data Source to Reporting Engine.
- Set Warehouse Data Source as the Default Source.
- HIVE server is in running state on all the Warehouse nodes. Use the following command to check the status of the HIVE server:

  ```
  status hive2 (MapR deployments)
  service hive-server2 status (Horton Works 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 `/var/netwitness/re-server/rsa/soc/reporting-engine/conf/` directory in the Reporting Engine Host.

  Note: The `rsasoc` user should have read permissions for the keytab file. For more information, see Configure Data Source Permissions.

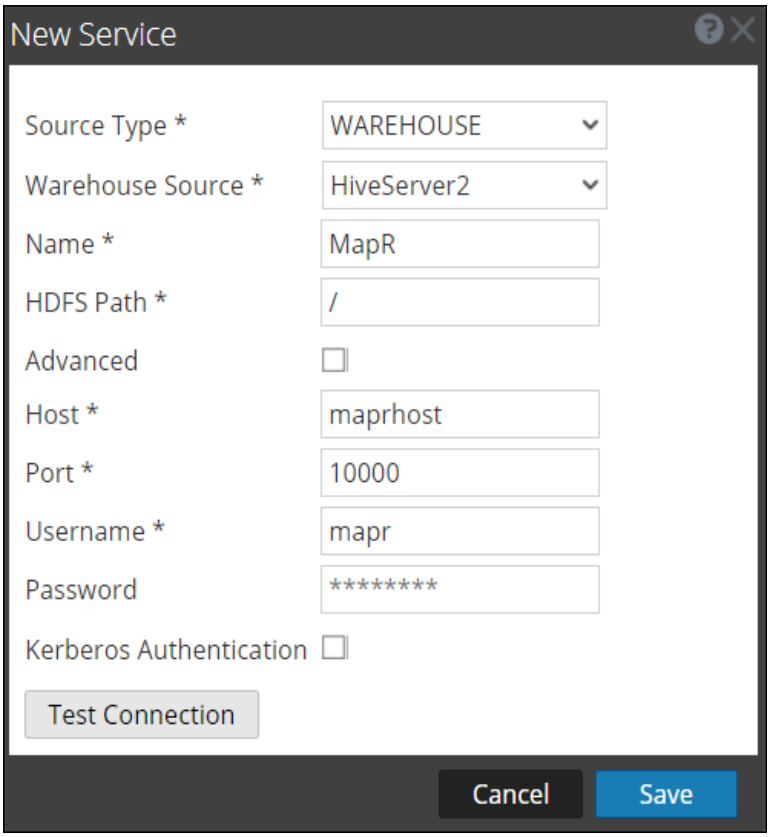
  Also, make sure that you update the keytab file location in the **Kerberos Keytab File** parameter in the Reporting Engine Service Config View. For more information, see Reporting Engine General Tab.

To add Warehouse data source for MapR:

1. Go to **(Admin) > Services**.
2. In the **Services** list, select the **Reporting Engine** service.
3. Click > **View** > **Config**.

   The **Service Config** view is displayed with the **General** tab open.
4. Click the **Sources** tab.
5. In the **Sources** tab, 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 host 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. And if you have installed the Warehouse Connector service to write to SAW. For more information, see "Mount the Warehouse on the Warehouse Connector" topic in the *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 the **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. Enable Kerberos authentication: see Enable Kerberos Authentication.
14. If you want set the added Warehouse data source as default source for the Reporting Engine, select the added Warehouse data source and click Set default.

To add Warehouse data source for Horton Works (HDP):

Note: Make sure you download the `hive-jdbc-1.2.1-with-full-dependencies.jar`. This jar contains the driver file of HIVE 1.2.1 which connects to Reporting Engine for Hive 1.2.1 Hiveserver2.

1. SSH to the NetWitness server.
2. In the `/opt/rsa/soc/reporting-engine/plugins/` folder, take a backup of the following jar:

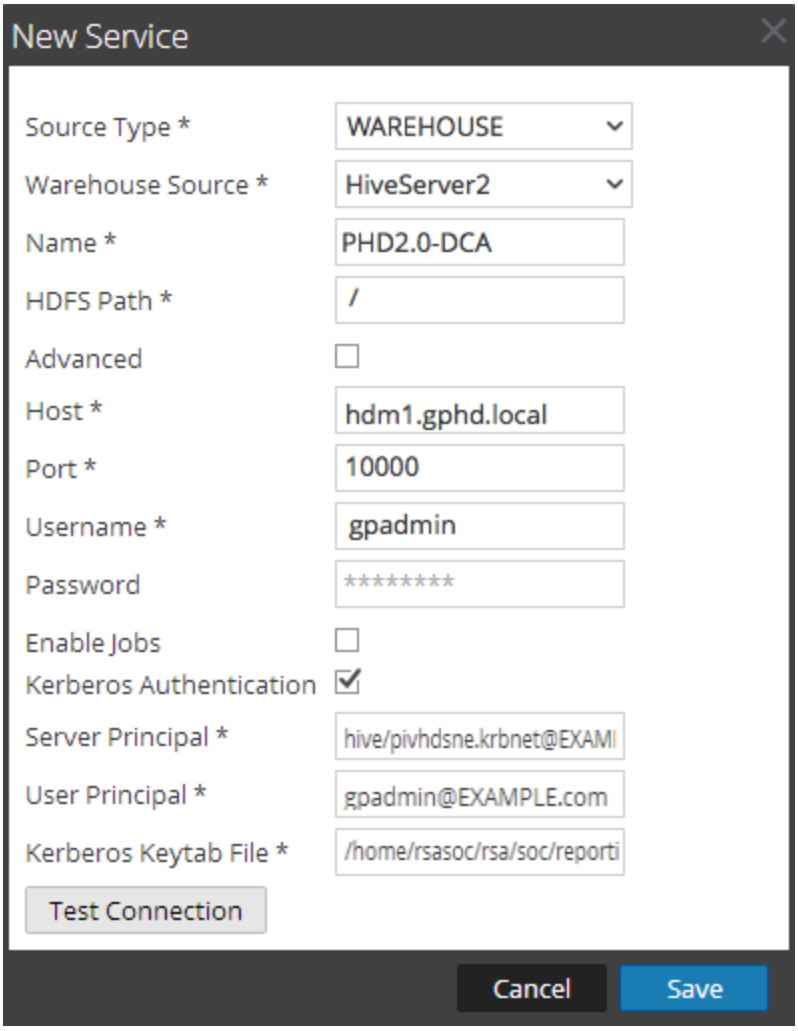
   `hive-jdbc-0.12.0-with-full-dependencies.jar` or `hive-jdbc-1.0.0-mapr-1508-standalone.jar`
3. Remove the following jar:

   `hive-jdbc-0.12.0-with-full-dependencies.jar` or `hive-jdbc-1.0.0-mapr-1508-standalone.jar`
4. In the /opt/rsa/soc/reporting-engine/plugins folder, copy the following jar using WinSCP:

   `hive-jdbc-1.2.1-with-full-dependencies.jar`
5. Restart the Reporting Engine service.
6. Log in to NetWitness UI.
7. Select the **Reporting Engine** service and select > **View** > **Explore**.
8. In the **hiveConfig**, set **EnableSmallSplitBasedSchemaLiteralCreation** parameter to **true**.

Enable Kerberos Authentication

1. Select **Kerberos Authentication** checkbox, if the Warehouse is Kerberos enabled HIVE server.



2. Fill in the fields as follows:

Field	Description
Server Principal	Enter the Principal used by the HIVE server to authenticate with the Kerberos Key Distribution Center (KDC) Server.
User Principal	Enter the Principal that HIVE JDBC client uses to authenticate with the KDC server for connecting the HIVE server. For example, gpadmin@EXAMPLE.COM.

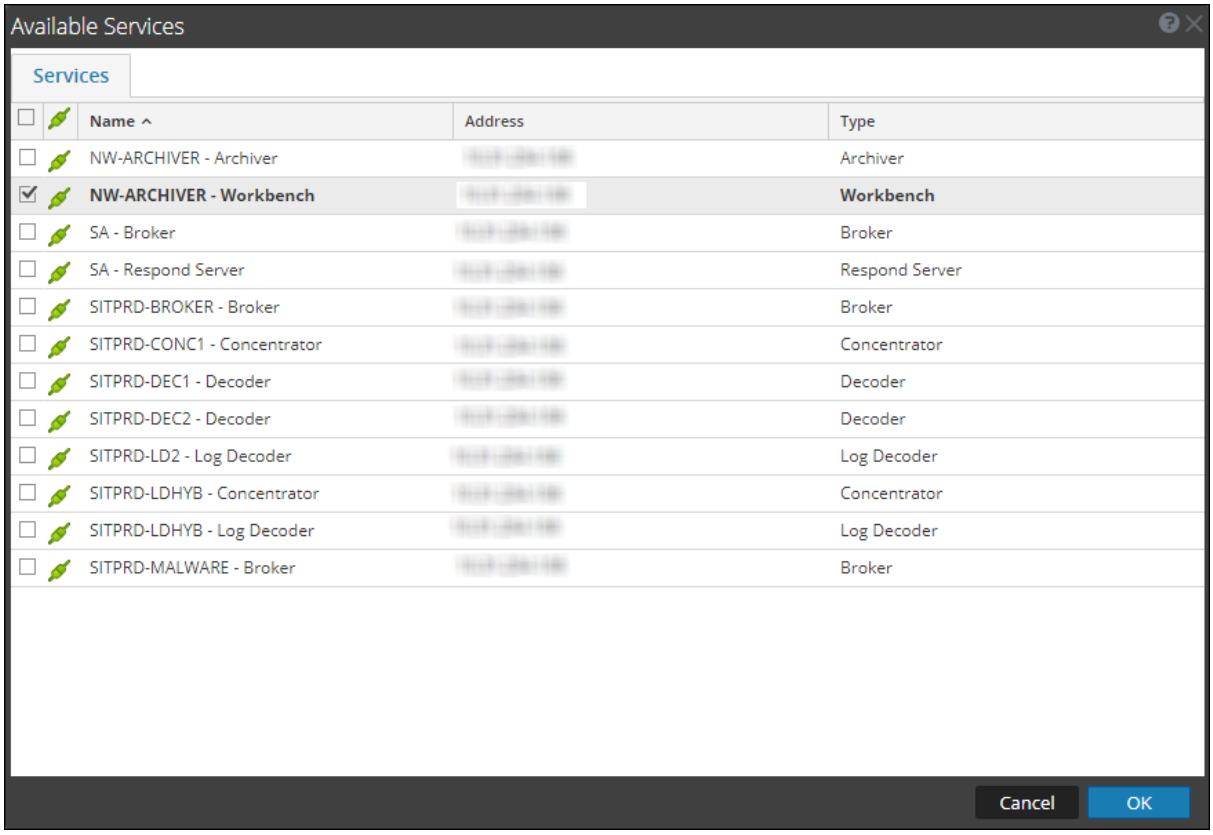
Field	Description
Kerberos Keytab File	View the Kerberos keytab file location configured in the HIVE Configuration panel on the Reporting Engine General Tab. **Note:** Reporting Engine supports only the data sources configured with the same Kerberos credentials, like, User Principal and key tab file.

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.

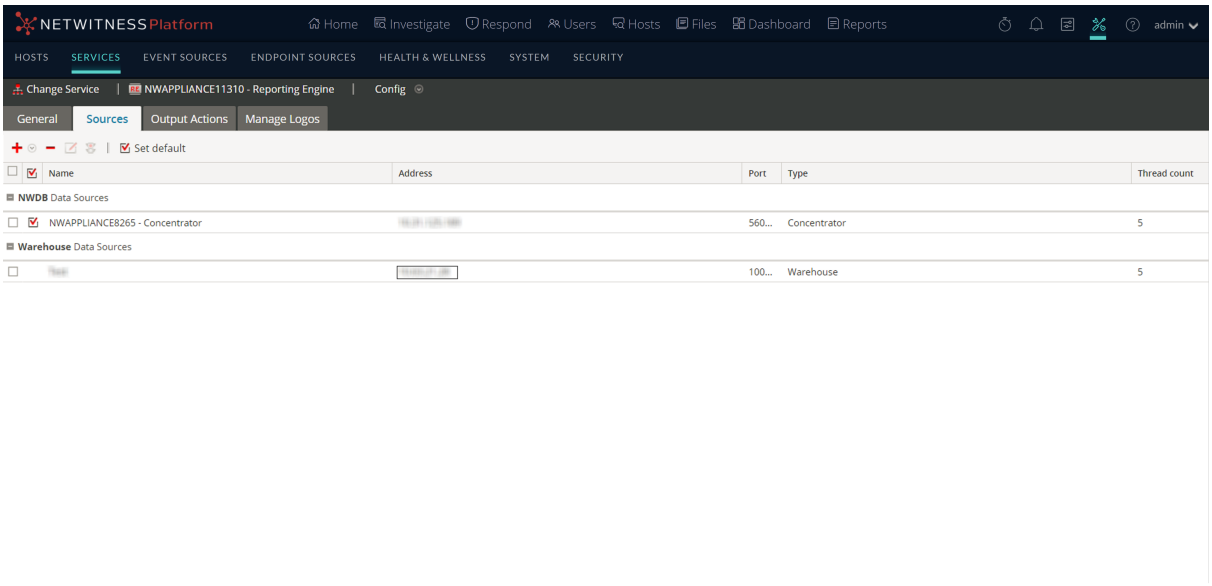
5. Click  > **Available Services**.

   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**.

   NetWitness 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. Go to **(Admin) > Services**.
2. In the **Services** list, 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.

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

(Optional) Add Workbench as Data Source

You must configure Workbench,to be able to use data from Workbench data source to generate Reports and Alerts. The following instructions describe 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:

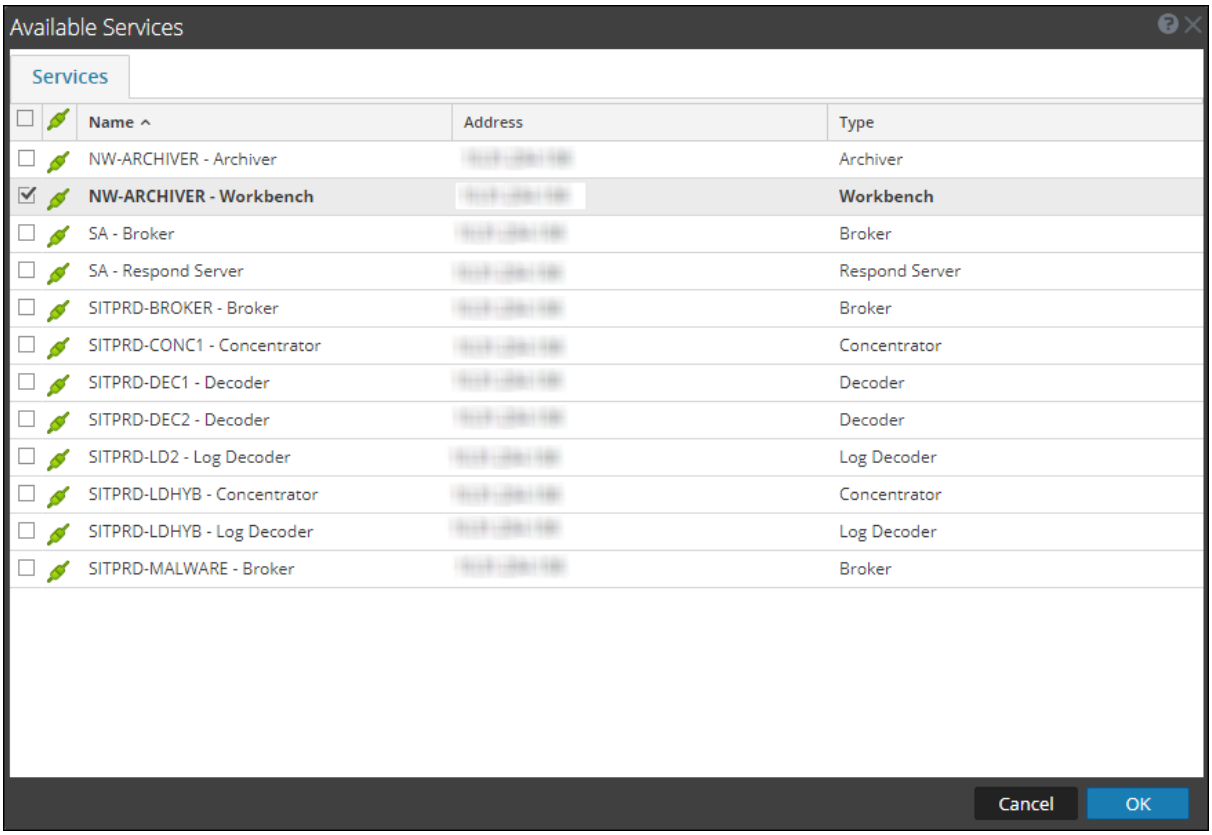
1. Added Workbench as a service to your NetWitness deployment. For more information, see the *Archiver Configuration Guide*.
2. Added a Collection on the Workbench service.

To add Workbench as a data source to Reporting Engine:

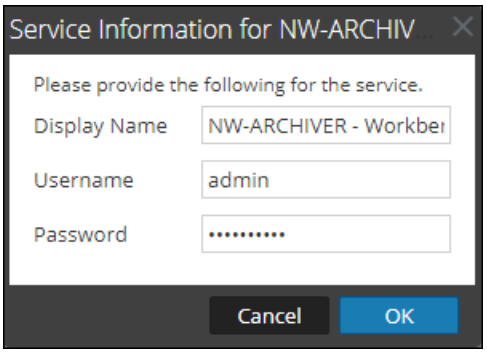
1. Go to  **(Admin) > Services**.
2. In the **Services** list, select a **Reporting Engine** service.
3. Select  > **View** > **Config**.

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

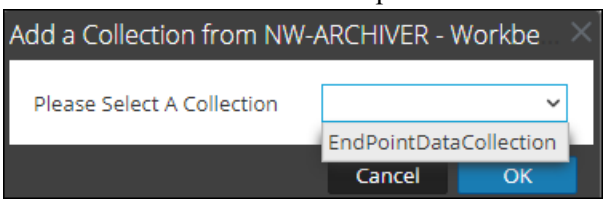
   The Available Services dialog is displayed:



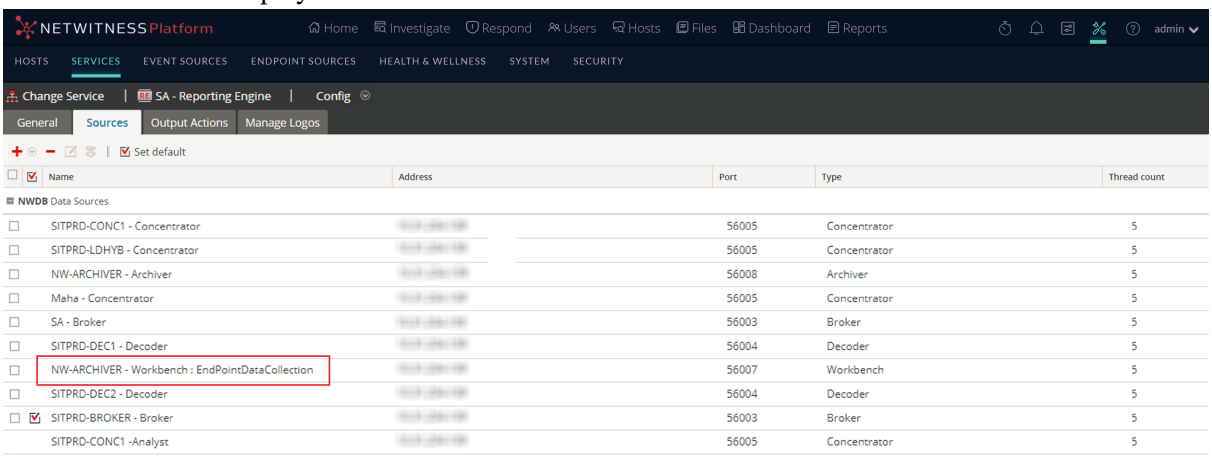
6. Select the Workbench service and click **OK**.
   A list of collections are displayed.
7. Enter the service information, and click **OK**



8. Select a collection from the dropdown.



9. The data source is displayed in the Sources tab.



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.

(Optional) Add Archiver as Data Source

You must configure Archiver, to be able to use data from Archiver data source to generate Reports and Alerts:

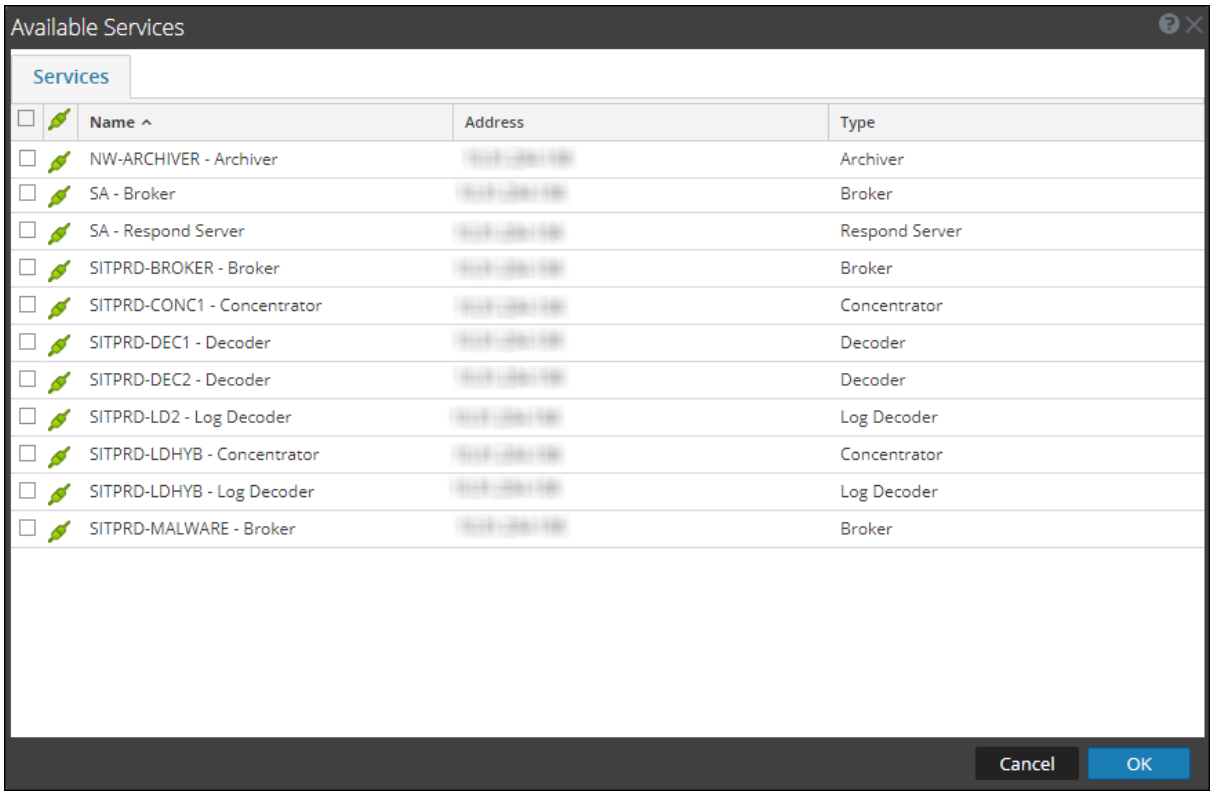
Prerequisites

Make sure that you have:

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

To add Archiver Data Source to Reporting Engine:

1. Go to  **(Admin) > Services**.
2. In the **Services** list, 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. Enter the Username and Password for the Archiver.
8. Click **OK**.

   The selected Archiver is listed in the Aggregate Services pane.

(Optional) Integrate Endpoint Information Into Reports

You can use the Endpoint data by using the following instructions to add the Endpoint information into Reports. The *Endpoint Integration Guide* provides an overview of Endpoint integration into NetWitness.

Prerequisites

Make sure that:

- You have configured the Endpoint alerts via syslog into a Log Decoder. For more information see, "Configure Endpoint Alerts Via Syslog into a Log Decoder" topic in *Endpoint Integration Guide*).

To integrate Endpoint information into Reports:

1. In **Reporting Engine**> **View**> **Config**> **Sources**.
2. Add the Concentrator that is consuming data from the Log Decoder as a data source.
   Endpoint meta is populated in Reporting Engine.
3. Run reports by selecting the appropriate meta.

(Optional) Add Collection as Data Source to Reporting Engine

You must configure Collection, to be able to use data from Collection data source to generate Reports, Charts, and Alerts:

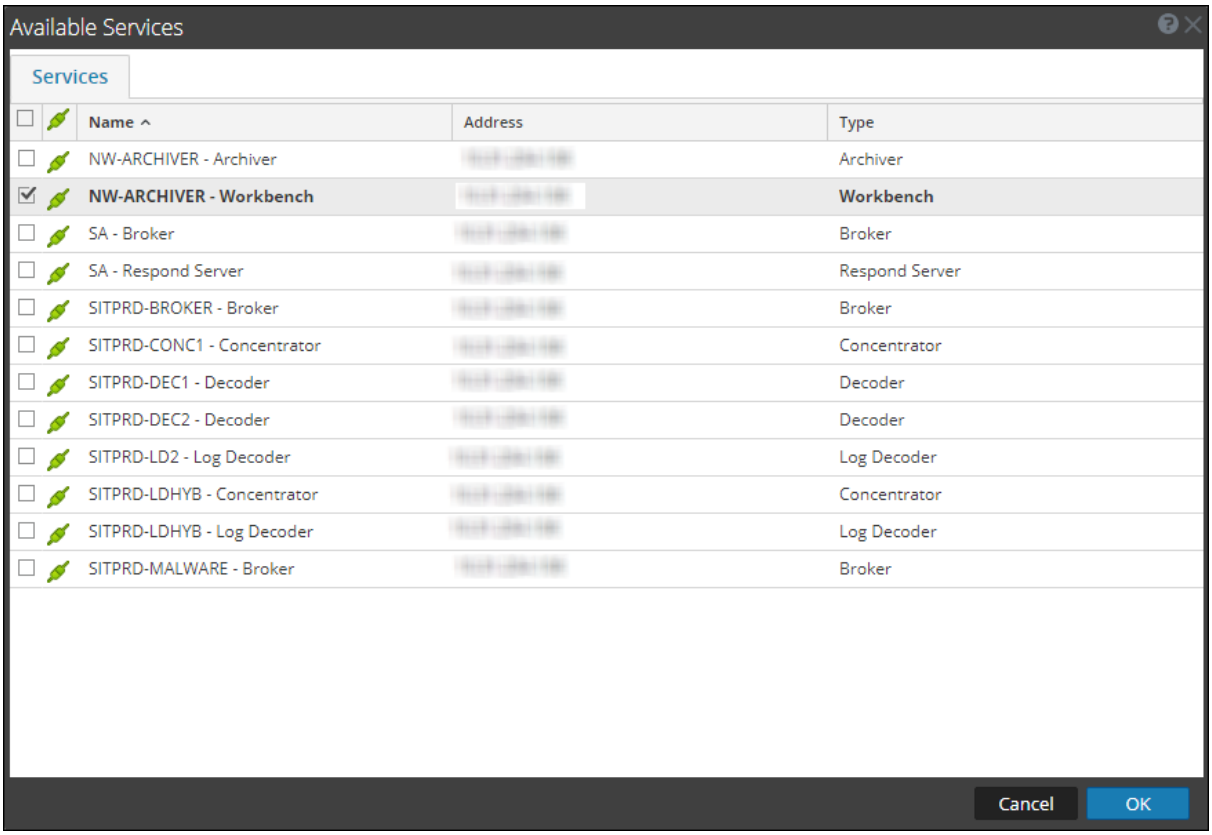
Prerequisites

Make sure 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.

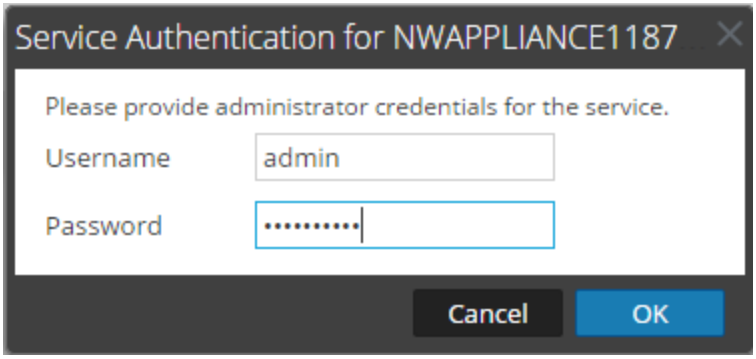
To associate a Collection as a data source with Reporting Engine:

1. Go to  **(Admin) > Services**.
2. In the **Services** list , 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**.

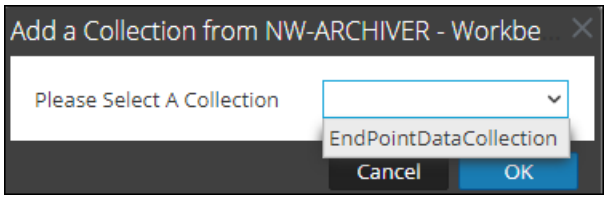
   The Service Authentication dialog for the selected service is displayed.



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. Enter 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.

Configure Data Privacy for the Reporting Engine

You can configure the data privacy for all data sources of Reporting Engine using the Sources tab of the **Services** > **View** > **Config** view.

With the addition of the Data Privacy feature to NetWitness, access to sensitive meta in NetWitness 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.or more information, see Configure Data Source Permissions.

Note: A user assigned to the `Data_Privacy_Officers` role (or an equivalent custom role), can create a report, chart and alert. Also, configure a report or alert output actions in the Reporting module. In an environment where data privacy features of NetWitness 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 Respond. This may inadvertently provide all the users of Respond module access to the sensitive meta values, regardless of their roles. One option to prevent this is to disable publishing into Respond 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.

NetWitness 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 services. 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.

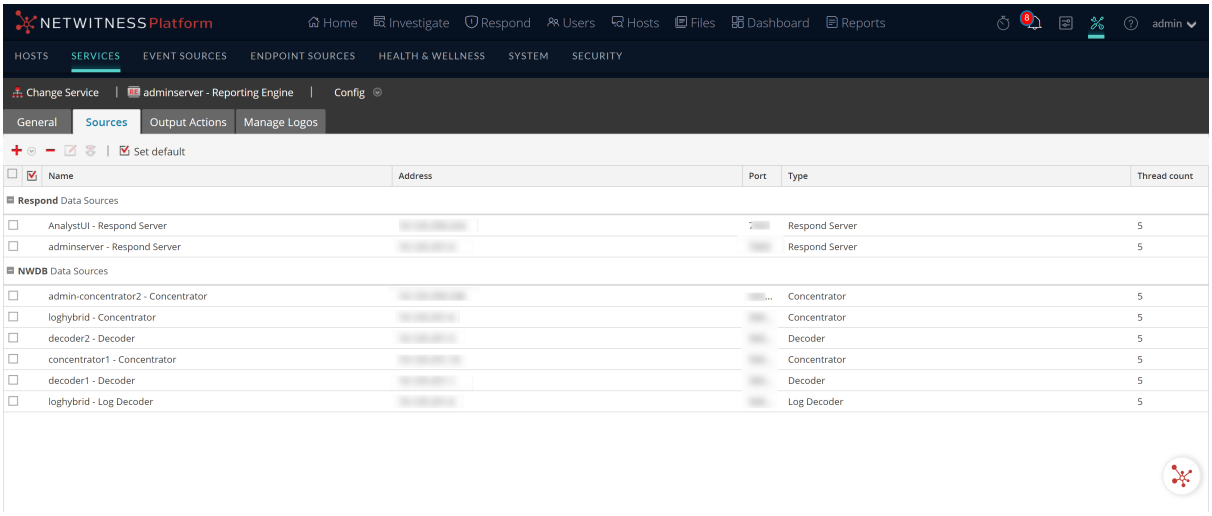
Add a NWDB Data Source with Different Service Accounts

To add a NWDB data source:

1. Go to **(Admin) > Services**.
2. In the **Services** list, select a **Reporting Engine** service.
3. Click **View** > **Config**.

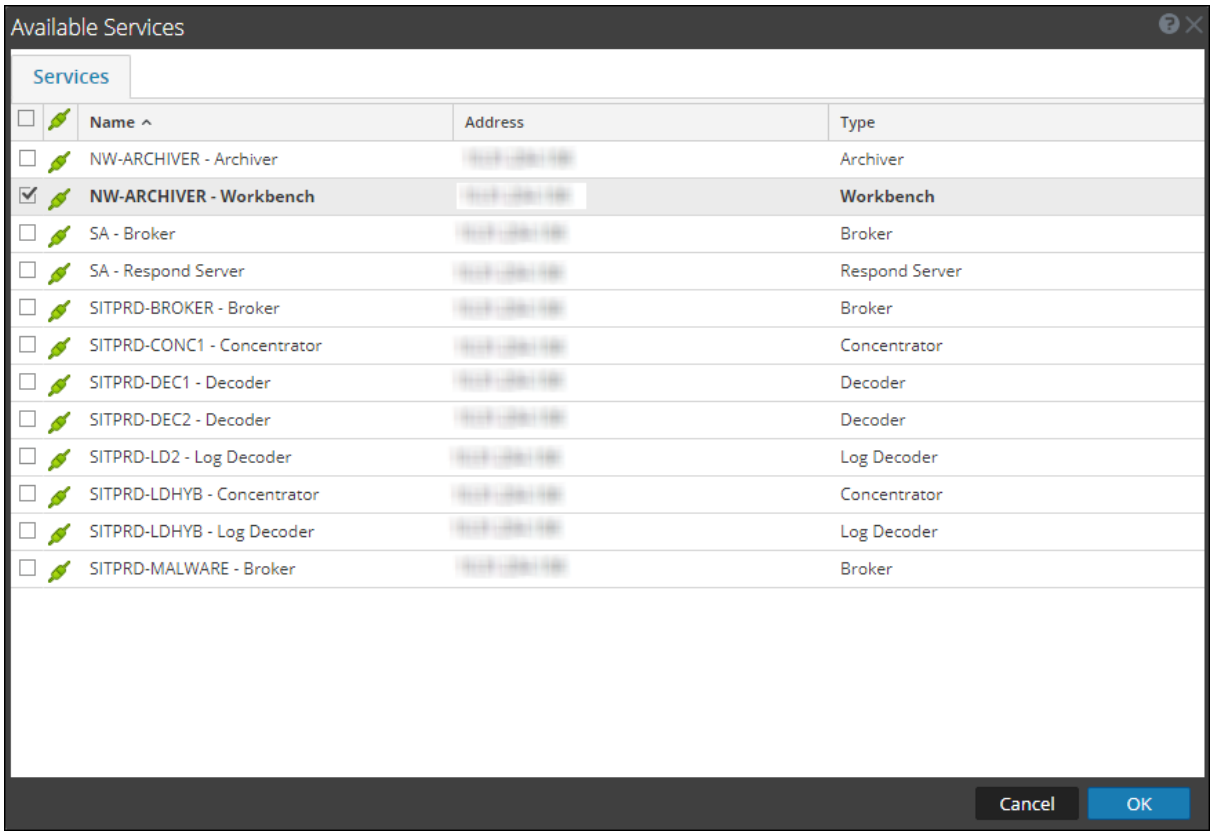
   The Services Config view of Reporting Engine is displayed.
4. Select the **Sources** tab.

   The Services Config View is displayed.



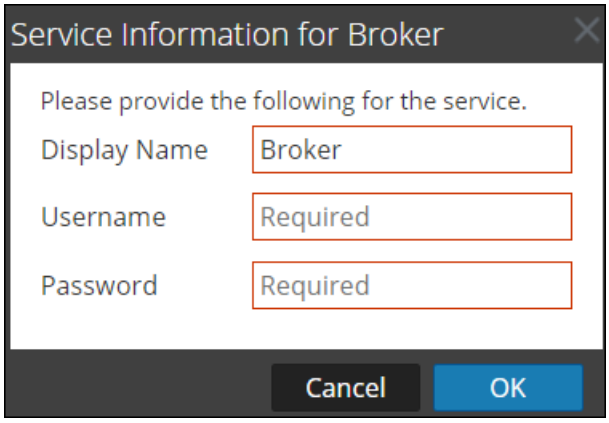
5. Click and select Available Services.

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



6. Select the checkbox next to the service and click **OK**.

   The Service Information dialog for the selected service is displayed.

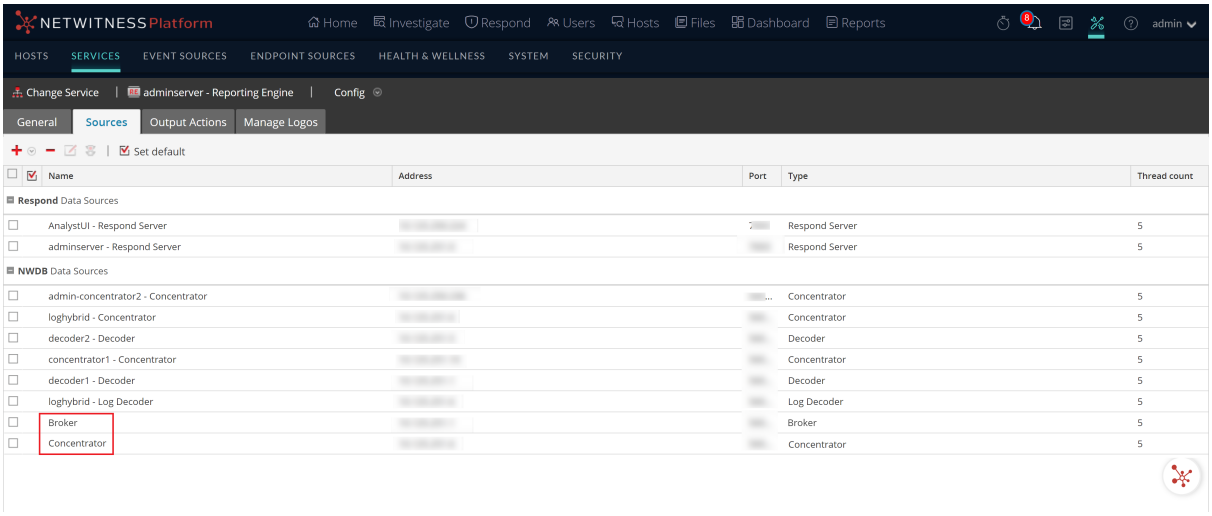


Note: NetWitness prompts you to provide a username and password for the selected service. To limit access to sensitive data, DPO users must use their credentials while adding the source instead of using the admin credentials. These credentials need to be applied to the host even if using trusted connections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

   Repeat the step for Non-DPO data source.

7. Enter 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.



Configure Data Source Permissions

You can configure data source permissions for Reporting Engine using the **Sources** tab of the **Services** > **Config** view. This helps 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 for each data source of the same Core service. For example, data privacy officers (DPO) can create a Warehouse source using their credentials, and that allows them to execute reports against the Warehouse while restricting everyone else from being able to use that source.

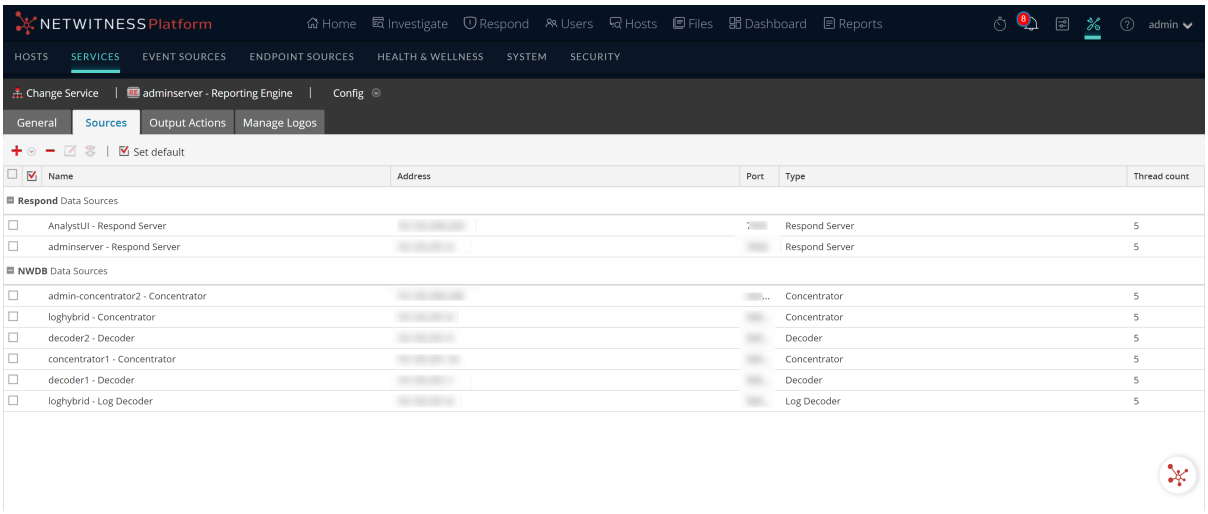
Note: The permissions for NWDB and Warehouse data sources are automatically set based on the permissions of the reporting objects. For example, if the role had the permissions set as **Read Only**/**Read & Write** for any reporting object, then that role is automatically assigned read only permission for all the data sources that existed. If no permission is set for the role, then the data source permission is automatically set to No Access.

To configure permissions to data sources:

1. Go to **(Admin) > Services**.
2. In the **Services** list, select a **Reporting Engine** service.
3. Click > **View** > **Config**.

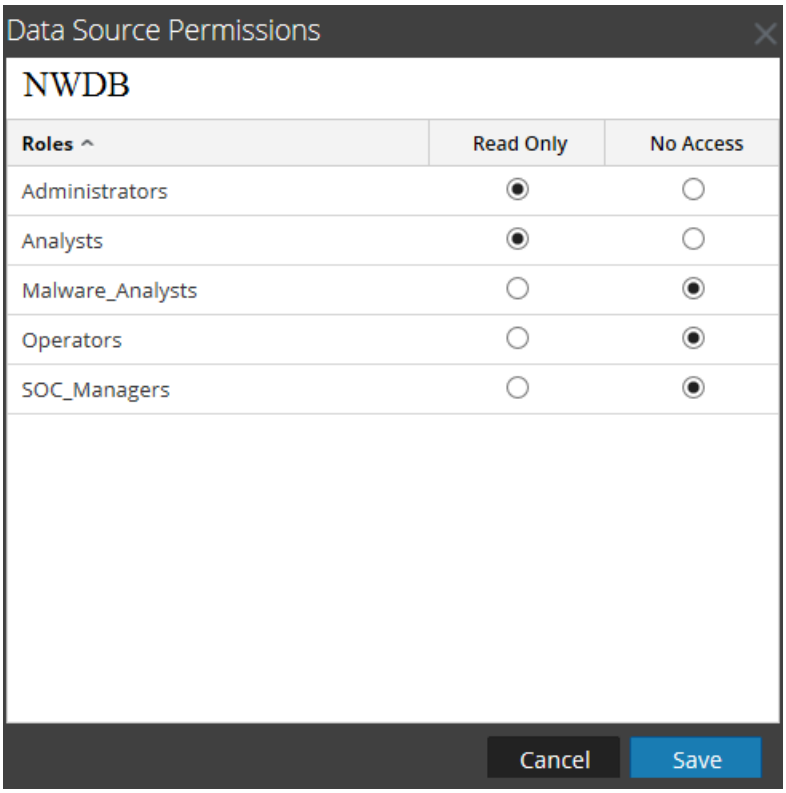
   The Services Config view of Reporting Engine is displayed.
4. Select the **Sources** tab.

   The Service Config View displays the Sources tab.



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. For more information, see the *Reporting Guide*.

Configure Reporting Engine Settings

After you configure the Reporting Engine and required data sources based on your requirements, you can modify some of the configurations to customize your Reports, Charts, and Alerts.

To configure the settings:

1. Go to  **(Admin) > Services**.
2. In the **Services** list, 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.

Enable LDAP Authentication

To enable LDAP mode of authentication using Active Directory for HiveServer2 for Warehouse data source, follow these steps.

1. Log on to the 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.

Add Additional Space for Large Reports

To add additional disk space to the Reporting Engine for large reports, follow the below steps. If large compliance reports have to be generated for 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.

Note: The following steps assume that the Reporting Engine home directory is located at `/var/netwitness/re-server/rsa/soc/reporting-engine/` and the external storage is mounted under `/externalStorage/`. Also, the 'rsasoc' user must have read-write access to the specified external storage path.

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

1. Stop Reporting Engine service as a root user.

   ```
   service rsasoc_re stop
   ```

2. Switch to `rsasoc` user.

   ```
   su rsasoc
   ```

3. Change to RE home directory.

   ```
   cd /var/netwitness/re-server/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 formatted Reports directory to a mounted external storage. Type the following command and press ENTER:

   ```
   mv formattedReports /externalStorage
   ```

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

   ```
   ln -s /externalStorage/resultstore /var/netwitness/re-
   server/rsa/soc/reporting-engine/resultstore
   ```

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

   ```
   ln -s /externalStorage/formattedReports /var/netwitness/re-
   server/rsa/soc/reporting-engine/formattedReports
   ```

8. Exit the `rsasoc` user.

   ```
   exit
   ```

9. Start Reporting Engine service as a root user.

   ```
   service rsasoc_re start
   ```

   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 for the service that you are using as a data source.

Accessing Reporting Engine Log Files

You can access the Reporting Engine log files which are stored in the following logs directory `/var/netwitness/re-server/rsa/soc/reporting-engine/logs/`

- 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 systemd system and the commands used to start the reporting-engine to the directory `/var/log/messages`.
A `/var/log/messages` log file is a system log file so only the root user can read it.

Configure Task Scheduler for a Reporting Engine

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

Prerequisites

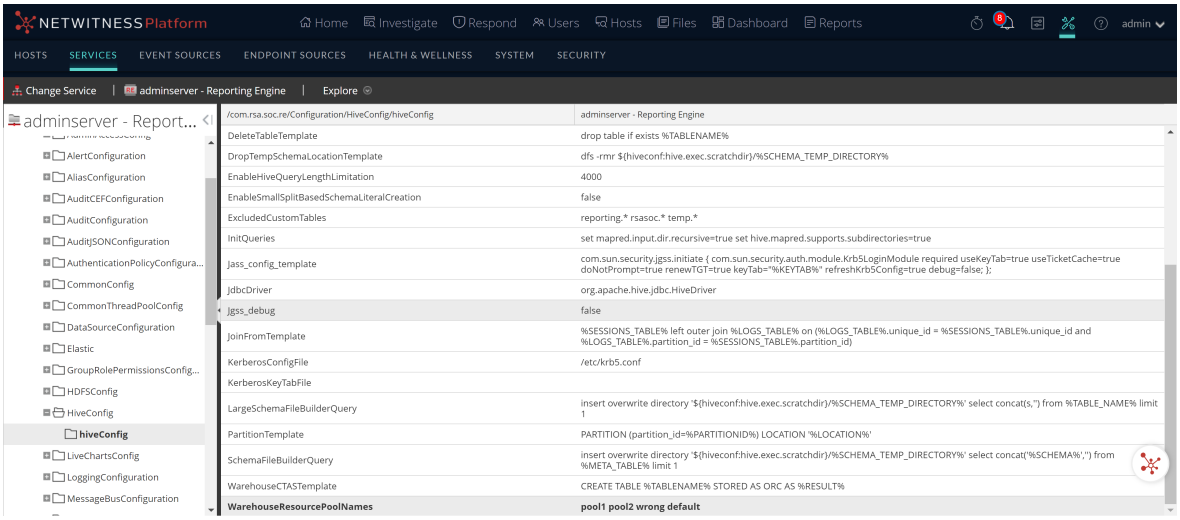
Make sure that you have identified the following:

- 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.
- NetWitness does not support multiple queues or pools per cluster. Netwitness 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 does 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 uses the default queue for the report. The Fair Scheduler may not execute the rule or creates 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. It 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. Make sure that you do not specify this pool name for any reports.

Specify the Pools and Queues

To specify the pools and queues:

1. Go to **(Admin) > Services**.
2. Select **Reporting Engine** and click > **View** > **Explore**.
3. Select **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.



Define Reports, Charts and Alerts

After you configure the Reporting Engine and the required data source based on your requirement, you can generate your Reports, Charts, and Alerts.

Define Reports

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

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

Define Charts

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 chart and Chart Groups
- Test a Chart
- Investigate Charts
- Manage Charts

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

Define Alerts

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 Alerting module:

- Configure Alerts
- Generate Alerts
- Add an Alert
- View an Alert

- View and Alert
- View Alerts Schedule
- Investigate an Alert

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

Configure Reporting Engine General Settings

After you add and configure the Reporting Engine service, the system settings are defined with default values to achieve optimal results. However, you can modify and customize the Reporting Engine notifications based on your requirement by navigating to the **General** tab in the **Services** > **Config** view for a Reporting Engine.

Access the General Tab

You need to open the General tab to configure the general parameters for Reporting Engine.

To access this view:

1. Go to  **(Admin) > Services**.
2. In the Services list, select a **Reporting Engine** service.
3. Click **View** > **Config**.
4. Select the **General** tab.
5. Click **Apply** after you edit the parameters.

After you navigate to the General tab, you can modify the following parameters.

- System Configuration
- Logging Configuration
- Warehouse Kerberos Configuration

For more information see, General tab for details on the configuration parameters.

Troubleshooting Reporting Engine Configuration

Problem	Solution
When the NetWitness Server IP address is changes, the Reporting Engine datasource configuration does not get updated with the new IP	You must manually configure the new IP. Perform the following manual steps to configure the new IP address: 1. Login in NetWitness Platform. 2. Go to  **(Admin) > Services** > **Reporting Engine** > **View** > **Config**. 3. Click the **Output Actions** tab. 4. Add the new IP address in the **Hostname** field. 5. Click **Apply**. 6. Click the **Sources** tab and add the data sources again.

References

You can customize and make optimum use of the service by modifying the Reporting Engine settings in the **Services** > **Config** view, which has parameters that specifically pertain to the Reporting Engine.

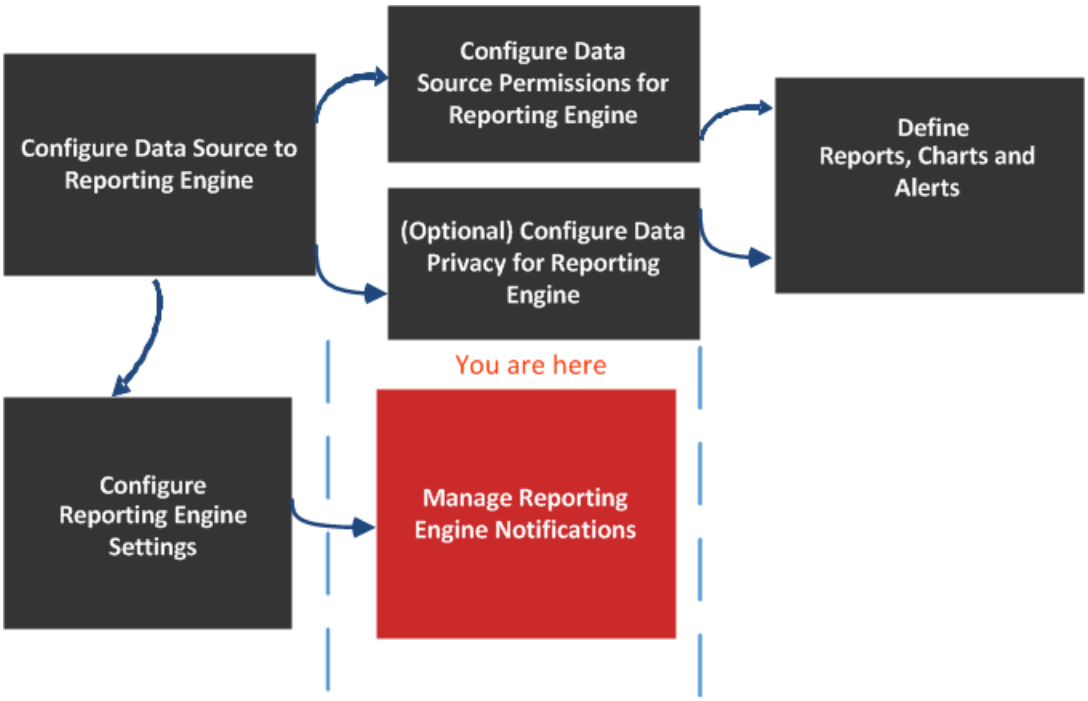
See the following sections for details:

- Reporting Engine General Tab
- Reporting Engine Sources Tab
- Reporting Engine Output Actions Tab
- Reporting Engine Manage Logos Tab

Reporting Engine General Tab

The General tab for the Reporting Engine service controls several settings that can tune the performance of a service and specify the user credentials for the service. Navigate to Services > View > Config > Reporting Engine > General. These settings are used for the Reporting Engine service exclusively.

The required permission to access this view is Manage Services.



What do you want to do?

Role	I want to ...	Refer to...
Administrator	Configure Data Source to Reporting Engine	Configure the Data Sources
Administrator	Configure Data Source Permissions for Reporting Engine	Configure Data Source Permissions
Administrator	Configure Data Privacy for Reporting Engine	Configure Data Privacy for the Reporting Engine
Administrator	Define Reports, Charts, and Alerts	Define Reports, Charts and Alerts
Administrator	Configure Reporting Engine Settings	Configure Reporting Engine Settings
Administrator / SOC Manager	Configure System Settings*	Configure Reporting Engine General Settings

Role	I want to ...	Refer to...
Administrator / SOC Manager	Configure Logging*	Configure Reporting Engine General Settings
Administrator / SOC Manager	Configure Warehouse Kerberos*	Configure Reporting Engine General Settings

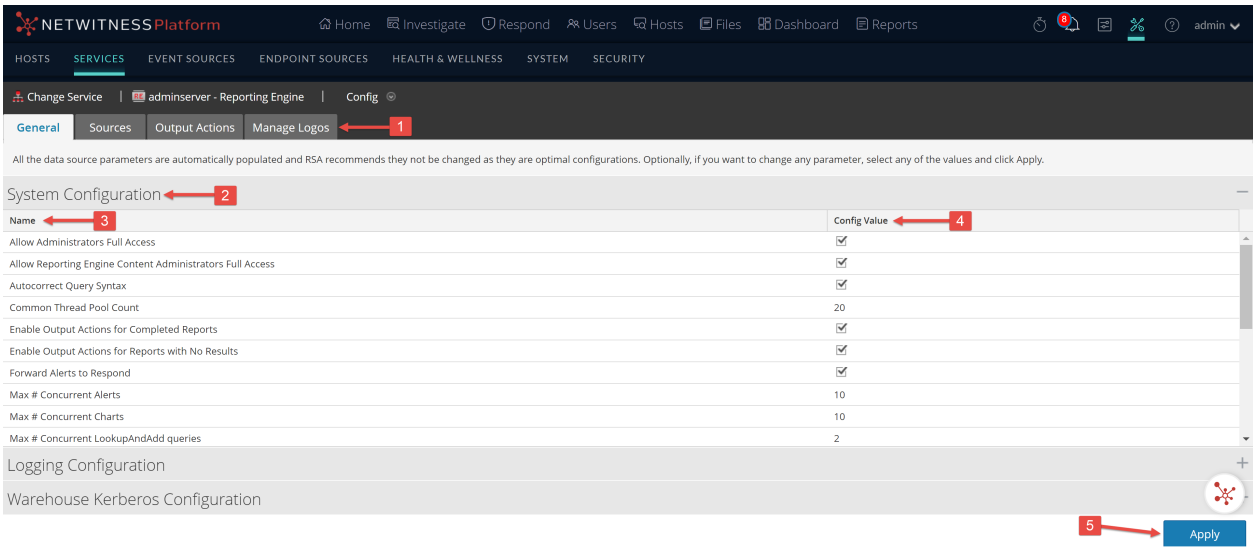
*You can complete these tasks here.

Related Topics

- How Reporting Engine Works

Quick Look

Here is example of the General tab where service configurations are displayed.

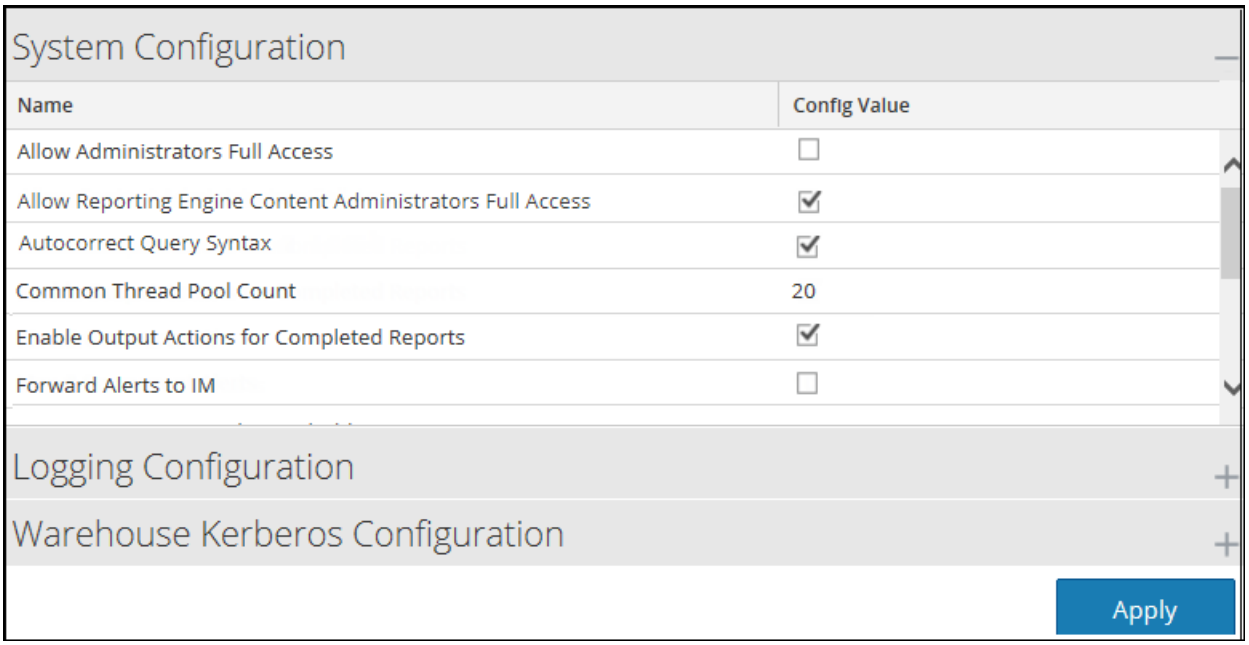


1 Displays all the available configurable tabs.
2 Displays the available configuration parameters for the system.
3 Displays the name of the parameter.
4 Displays the set values for each parameter.
5 Applies the changes.

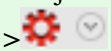
System Configuration

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. The default values are designed to accommodate most environments and recommends that you do not edit these values because it may adversely affect performance.

The following figure displays 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 Reporting Engine 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 Reporting Engine objects that were enabled by selecting 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.
Allow Reporting Engine Content Administrators Full Access	Select the checkbox if you want to access all the Reporting Engine objects (Reports, Rule, Charts, Schedule, and List) created by other users. By default, this is enabled. If disabled, you cannot access the Reporting Engine objects (Reports, Rule, Charts, Schedule, and List) created by other users.
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 Respond	Select the checkbox to forward all the alerts to Respond. By default, this is not enabled.

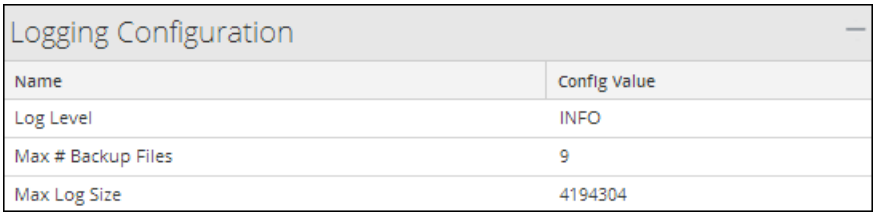
Name	Config Value
Max# of Concurrent Alerts	The maximum number of alerts that can be run simultaneously. This has a direct impact on the NetWitness service against which the alerts are run, as each alert consumes a query thread on the NetWitness service. A valid value is an integer (**10** default).
Max # of Concurrent Charts	The maximum number of charts that can be run simultaneously. A valid value is an integer (**10** default).
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).
Maximum disk space threshold	The maximum disk space threshold allotted (in GB) to execute reports, alerts and charts. The initial value is configured based on the available system space.
Minimum disk space threshold	The minimum disk space threshold allotted (in percentage) required to execute reports, charts, and alerts. By default, this is value is set to 5. **Note:** If the minimum threshold is reached, then the execution of reports, charts and alerts will stop even if the service is running.
NWDB Info Queries Time Out	The info queries time out in seconds for NWDB server. A valid value is an integer (**1800** 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. A valid value is an integer (**259200000** default).
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 of the Reporting Engine manages the logging configuration for a Reporting Engine service. When you add a Reporting Engine service, default values are in effect. NetWitness designed the default values to accommodate most environments and recommends that you do not edit these values because it may adversely affect performance of the Reporting Engine.

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



The following table describes the Logging Configuration panel features.

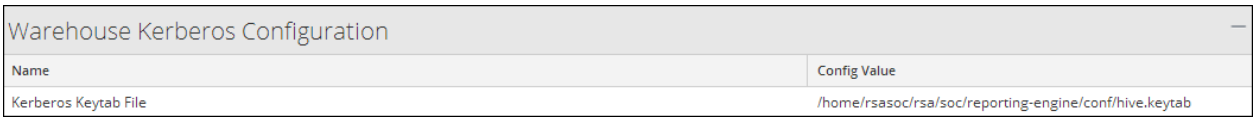
Name	Config Value
Log Level	The logging level that determines the scope of information included in log files. Possible values are: • `ERROR` • `WARN` • `INFO (default)` • `DEBUG` • `ALL`
Maximum # Backup Files	The maximum number of backup log files the system retains. A valid value is an integer (**9**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

Warehouse Kerberos Configuration

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

The following figure displays 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: `/var/netwitness/re-server/rsa/soc/reporting-engine/conf/hive.keytab`

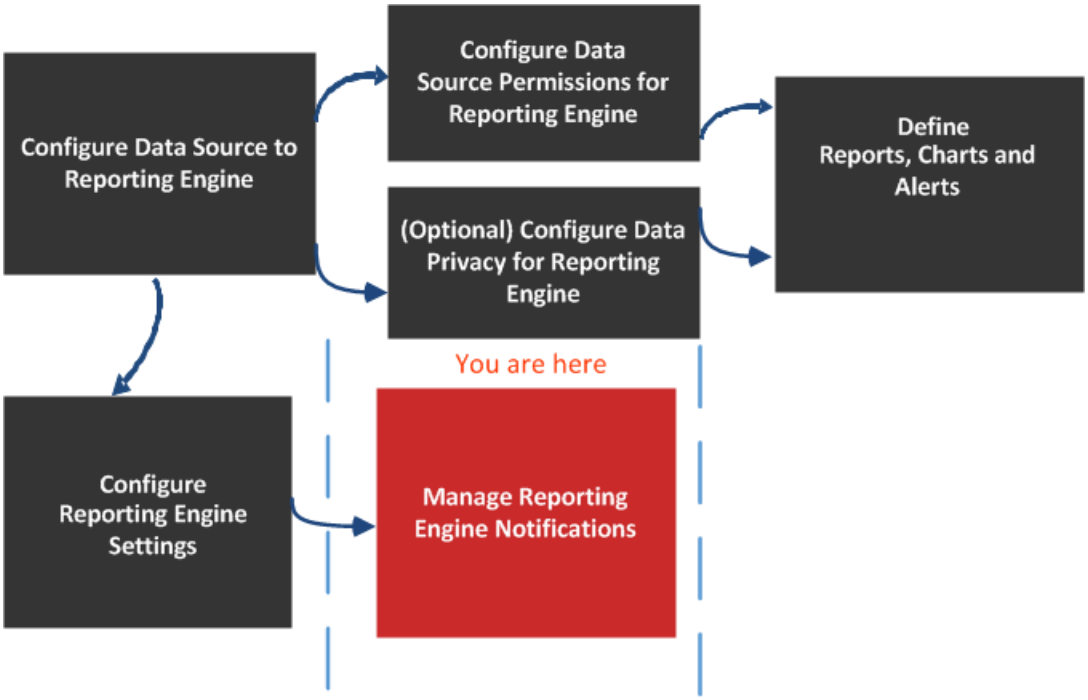
The default Kerberos configuration file is located at, `/etc/kbr5.conf` in the Reporting Engine. You can modify the configuration file to provide details for Kerberos realms and other parameters related to Kerberos.

Added the host name (or FQDN) and IP address of the Horton Works nodes and Warehouse Connector to the DNS server. If the DNS server is not configured, add the host name (or FQDN) and IP address of the Horton Works nodes and Warehouse Connector to the `/etc/hosts` file in the host on which the Warehouse Connector service is installed.

Reporting Engine Sources Tab

The services configuration parameters are 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.

Workflow



Role	I want to...	Refer to...
Administrator	Configure Data Source to Reporting Engine	Configure the Data Sources
Administrator	Configure Data Source Permissions for Reporting Engine	Configure Data Source Permissions
Administrator	Configure Data Privacy for Reporting Engine	Configure Data Privacy for the Reporting Engine
Administrator	Define Reports, Charts, and Alerts	Define Reports, Charts and Alerts
Administrator	Configure Reporting Engine Settings	Configure Reporting Engine Settings
Administrator	Add, delete or edit a new or available service*	Configure the Data Sources

Role	I want to...	Refer to...
Administrator	Set a data source as default*	Configure the Data Sources
Administrator	Configure data source permissions*	Configure Data Source Permissions

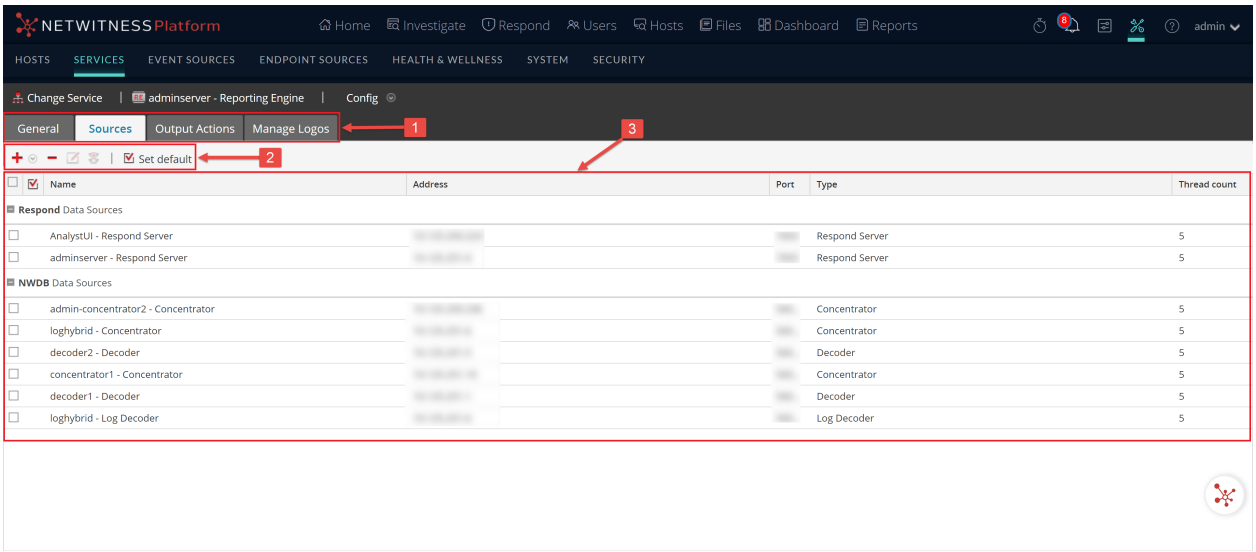
*You can complete these tasks here.

Related Topics

- How Reporting Engine Works

Quick Look

Here is example of the Sources tab where the available services are displayed.



1 Displays all the available configurable tabs.
2 Displays the available configuration parameters for the selected service .
3 Displays the field parameters for the selected service.

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

- **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 Configure Reporting Engine Settings.

IMPORTANT: If you change the admin password on a NetWitness service that is used as a Reporting Engine data source, you must remove and then re-add the service as a data source.

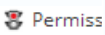
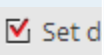
- **Warehouse Data Sources** - The Warehouse data sources are Horton Works and MapR.
- **Respond Data Sources** - Respond is used to generate reports on alerts and incidents. The Respond data sources are Reporting Engine, ESA, Malware, EndPoint, and Web Threat Detection. Respond is used to store the alerts and incidents reports.

If you set a source as the default data source, NetWitness 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 Configure Reporting Engine Settings.

Features

You can perform the following actions on the Sources tab:

Icon	Actions
	This option adds new services as data sources for Reporting Engine. Add existing services (Archiver, Workbench, and Collection) as data sources for Reporting Engine. For details, see the corresponding topic: • (Optional) Add Archiver as Data Source • (Optional) Add Collection as Data Source to Reporting Engine • (Optional) Add Workbench as Data Source
	This option removes data sources from a Reporting Engine.
	This option configures the Data Source Permissions. This is enabled only for NWDB and Warehouse Data Sources. For more information, see Configure Data Source Permissions.
	This option sets the default data sources for a Reporting Engine. This is the source to which NetWitness defaults in the **Data source** field of the following views: • Rule Definition view. • Create or Modify Alert view.

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

- NWDB Data Sources category displays the NetWitness data sources.
- Warehouse Data Sources category 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.

Column	Description
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.

Reporting Engine Output Actions Tab

You can configure output actions for a Reporting Engine to determine the format you want the data to be presented to you based on your requirements. The service configuration parameters are available in the Output Actions tab of the Services Config view configured for a report or an alert execution. This tab consists of the following panels:

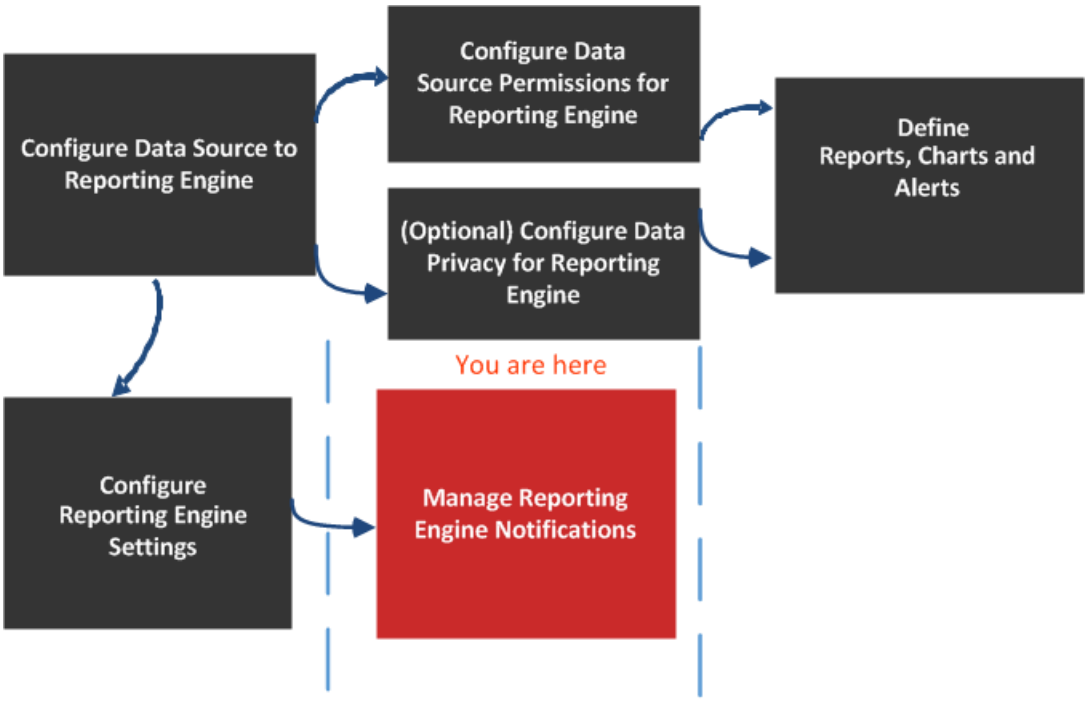
- NetWitness Configuration
- Simple Mail Transfer Protocol (SMTP)
- Simple Network Management Protocol (SNMP)
- Syslog
- Simple File Transfer Protocol (SFTP)
- Uniform Resource Locator (URL)
- Network Share

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.

You can configure the required permission to access this view in Manage Services.

You must ensure that the Reporting Engine is up and running and the data source from which you want to generate a report is configured in the NetWitness.

Workflow



What do you want to do?

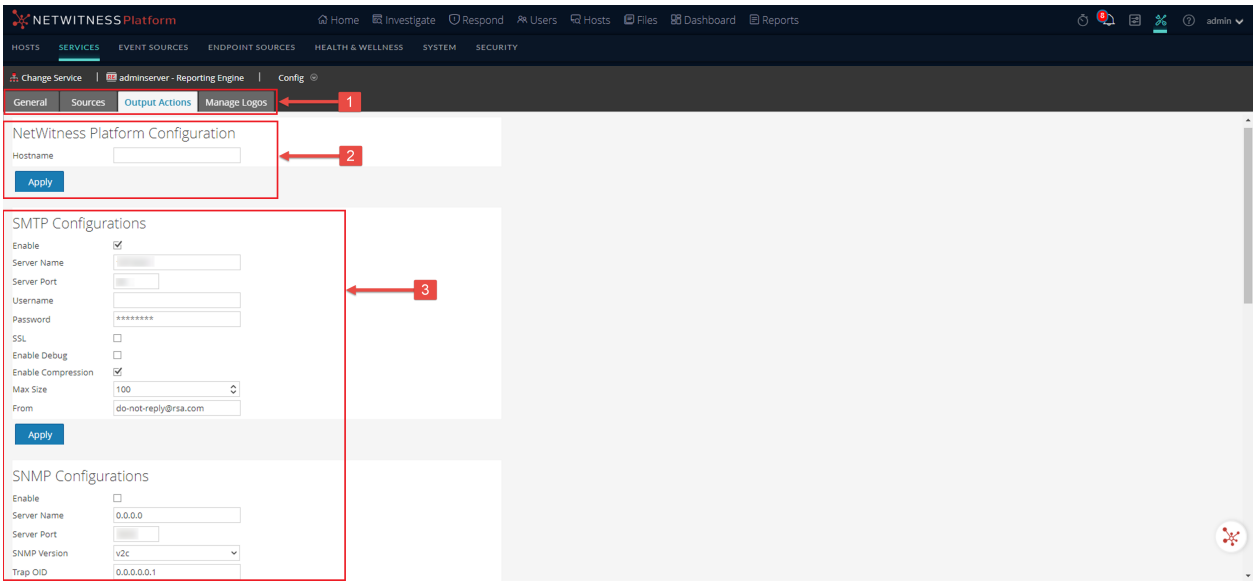
Role	I want to...	Refer to...
Administrator	Configure Data Source to Reporting Engine	Configure the Data Sources
Administrator	Configure Data Source Permissions for Reporting Engine	Configure Data Source Permissions
Administrator	Configure Data Privacy for Reporting Engine	Configure Data Privacy for the Reporting Engine
Administrator	Define Reports, Charts, and Alerts	Define Reports, Charts and Alerts
Administrator	Configure Reporting Engine Settings	Configure Reporting Engine Settings
Administrator	Configure NetWitness Configuration *	Configure Reporting Engine General Settings
Administrator	Configure SMTP Configuration*	Configure Reporting Engine General Settings
Administrator	Configure SNMP Configuration*	Configure Reporting Engine General Settings
Administrator	Configure Syslog Configuration*	Configure Reporting Engine General Settings
Administrator	Configure SFTP Configuration*	Configure Reporting Engine General Settings
Administrator	Configure URL Configuration*	Configure Reporting Engine General Settings
Administrator	Configure Network Share Configuration*	Configure Reporting Engine General Settings

*You can complete these tasks here.

Related Topics

- How Reporting Engine Works

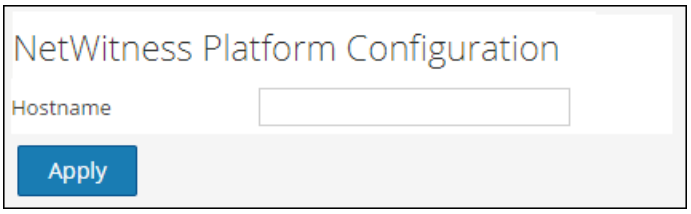
Quick Look



1	Displays all the available configurable tabs.
2	Displays the NetWitness configuration host.
3	Displays all the types of output action that can be configured.

NetWitness Configuration

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



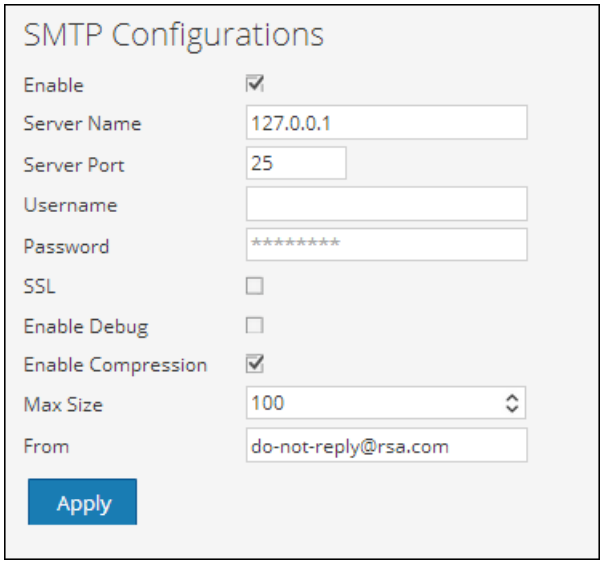
The following parameters identify the NetWitness host that is associated with the Reporting Engine.

Name	Config Value
Host Name	IP Address or Hostname of the NetWitness server. You must specify this parameter for all kind of deployments so that you can refer to this address to create investigation links to NetWitness from Reports, Alerts, and so on. The NetWitness 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

After 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.



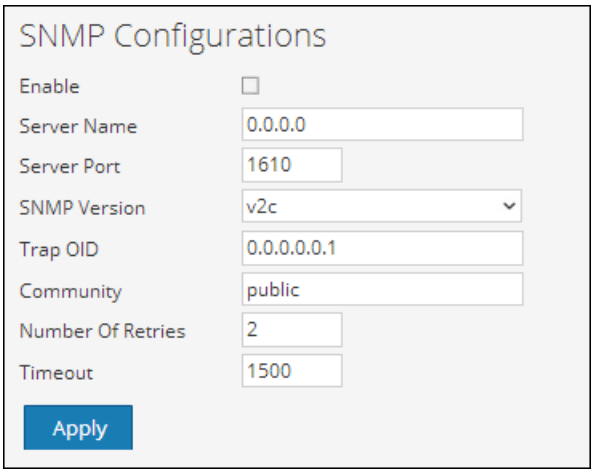
The following parameters manage SMTP (email) output action configuration for a Reporting Engine service. When you add a Reporting Engine service, default values are in effect. You must modify the **Config Values** of these parameters according to the requirements of your enterprise.

Name	Config Value
Enable	Check this box to enable SMTP as an output action for both alert and report from this Reporting Engine. By default, this value is enabled.
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
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

After 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.



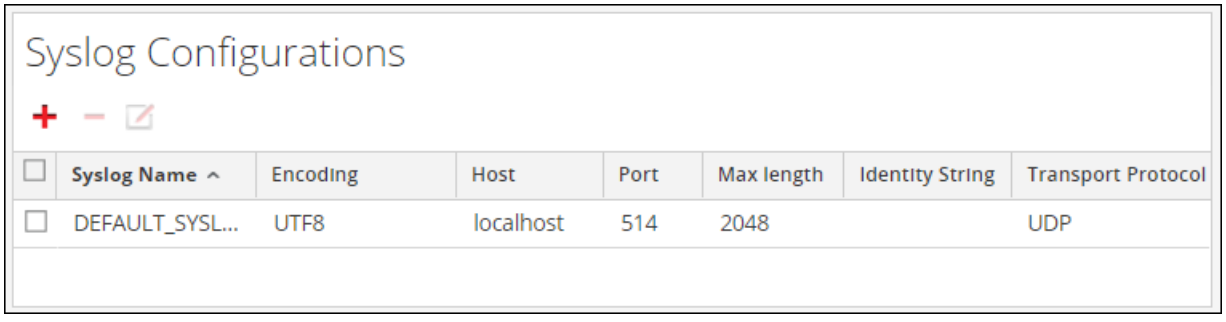
The following parameters manage SNMP (messages to network-attached services) output action configuration for a Reporting Engine service. When you add a Reporting Engine service, default values are in effect. You must modify the **Config Values** of these parameters according to the requirements of your 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 NetWitness 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 NetWitness belongs. The default value is **public**.
Number Of Retries	Specify the maximum number of times NetWitness tries to resend the alert message through SNMP. Default value is **2**.
Timeout	Specify the number of seconds after which NetWitness times out (stops trying to send SNMP alerts). Default value is **1500**.
Apply	Update the configuration.

Syslog

After 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.

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



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 NetWitness 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**.
Syslog Message Delimiter	Specify the delimiter for the Syslog message. There are three delimiters: CR, LF, and CRLF. By default the 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.

Name	Config Value
Apply	Save the configuration.

SFTP

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

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

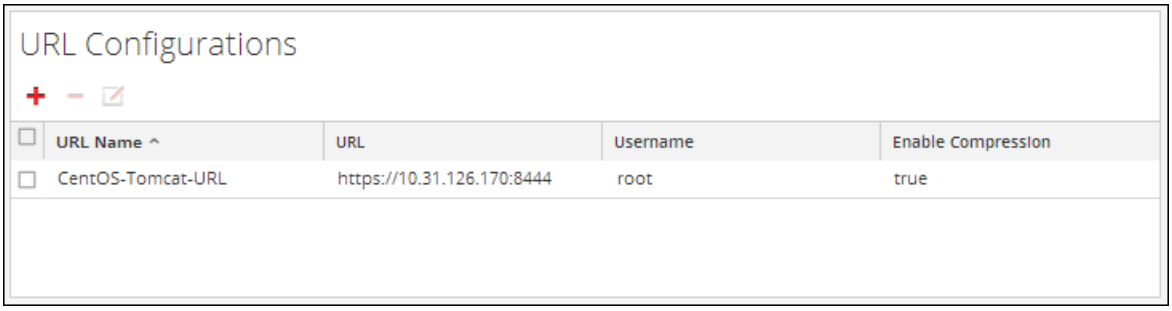
The following parameters manage SFTP (file transfer to a local drive) output action configuration for a Reporting Engine service. When you add a Reporting Engine service, you can define values for this output configuration, as no default values are available for this configuration. You must modify the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

After 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 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.
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.

Name	Config Value
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

After 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 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.
	Click to view how the mounted path is created. This pop-up notifies that you must manually create the mounted path.

Name	Config Value
Destination Directory	Name of the directory where the transferred file is stored in the shared location.
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.

The following table lists the common operations you can perform in the Syslog, SFTP, URL and Network Share sections.

Operation	Description
	Create a Syslog, SFTP, URL and Network Share configuration.
	Delete a Syslog, SFTP, URL and Network Share configuration.
	Edit a Syslog, SFTP, URL and Network Share configuration.

Reporting Engine Manage Logos Tab

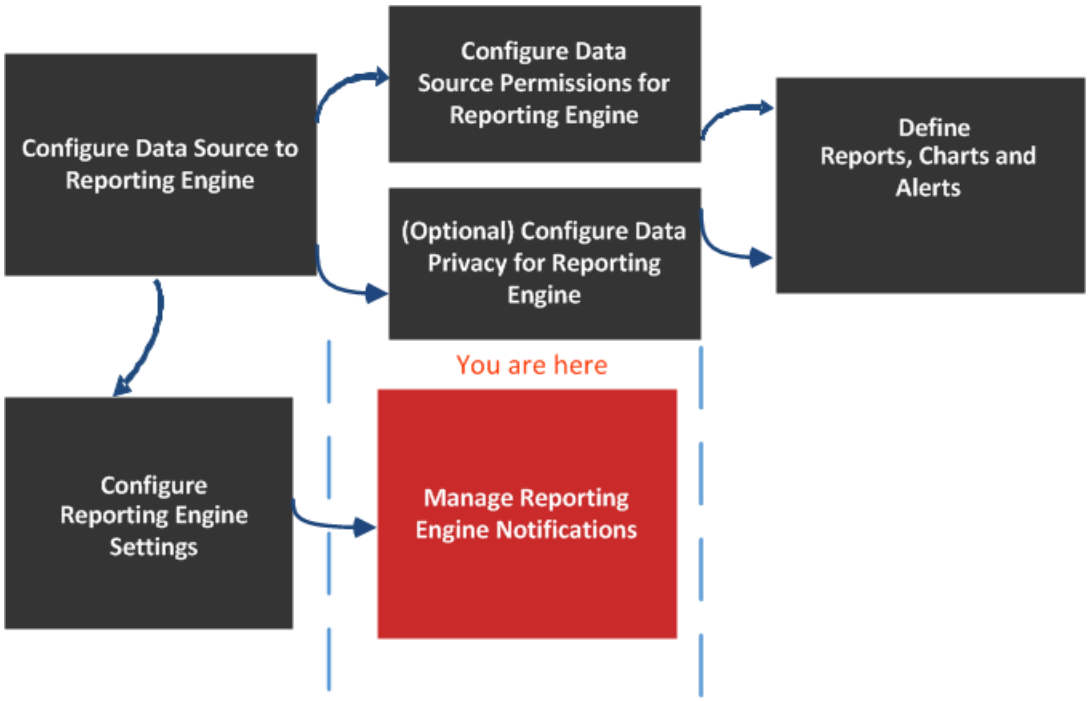
The Manage Logos option available in the **Services Config View** > **Manage Logos** tab, helps you to manage the logos associated with the Reporting Engine. The Manage Logos tab consists of a single panel with a toolbar and a grid that lists the logos.

You can upload the logos that you want to use in your report. After you upload the logo, you can set any logo as a default logo which will be automatically used in all the 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" topic in the *Reporting Guide*.

The supported image formats are:

- .jpg
- .png
- .gif

Workflow



What do you want to do?

Role	I want to...	Refer to...
Administrator	Configure Data Source to Reporting Engine	Configure the Data Sources

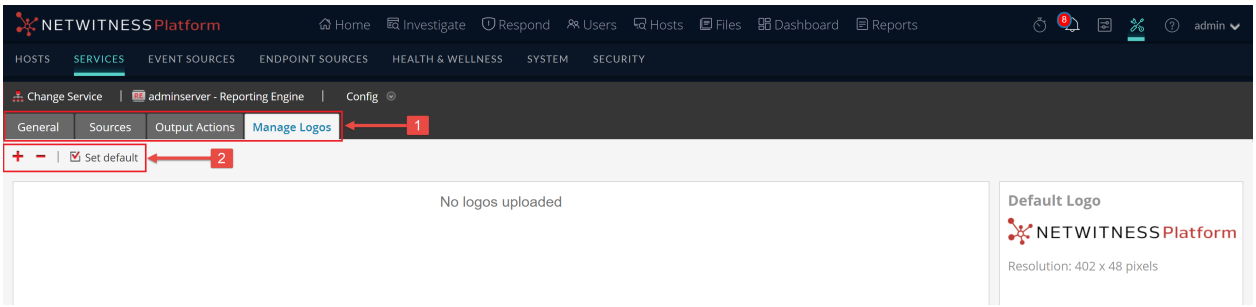
Role	I want to...	Refer to...
Administrator	Configure Data Source Permissions for Reporting Engine	Configure Data Source Permissions
Administrator	Configure Data Privacy for Reporting Engine	Configure Data Privacy for the Reporting Engine
Administrator	Define Reports, Charts, and Alerts	Define Reports, Charts and Alerts
Administrator	Configure Reporting Engine Settings	Configure Reporting Engine Settings
Administrator / SOC Manager	Add, or delete logos*	Configure Reporting Engine General Settings
Administrator / SOC Manager	View the list of logos*	Configure Reporting Engine General Settings
Administrator / SOC Manager	Set a logo as default*	Configure Reporting Engine General Settings

*You can complete these tasks here.

Related Topics

- How Reporting Engine Works

Quick Look



1 Displays all the available configurable tabs.
2 Displays edit actions.

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.
	Sets the default logo for a Reporting Engine. This is the logo NetWitness defaults to in the **Log** panel of the Schedule a Report view. **Note:** If no default logo is selected, the logo is displayed.