

# NetWitness<sup>®</sup> Platform

## Actiance Vantage Event Source Configuration Guide

# Actiance Vantage

Last Modified: Monday, December 2, 2024

## Event Source Product Information:

**Vendor:** [Actiance](#)

**Event Source:** Actiance Vantage

**Versions:** 12.2

## NetWitness Product Information:

**Supported On:** NetWitness Platform 12.3 and later

**Event Source Log Parser:** actiancevantage

**Collection Method:** ODBC

**Event Source Class.Subclass:** Security.Analysis

## 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 and 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.

## 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/>.

© 2024 RSA Security LLC or its affiliates. All Rights Reserved.

November 2024

# Contents

---

- Ensure the Required Parser is Enabled ..... 5
- Configure a DSN ..... 5
- Ensure the ODBC Collection Service is Running ..... 6
- Add the Event Source Type ..... 7
- ODBC Event Source Configuration Parameters ..... 9
  - Basic Parameters ..... 9
  - Advanced Parameters ..... 10
  - Advanced Parameters ..... 11
- Reference Tables and Typespec ..... 11
- Getting Help with NetWitness Platform ..... 12**
- Self-Help Resources ..... 12
- Contact NetWitness Support ..... 12
- Feedback on Product Documentation ..... 13

To configure ODBC collection in RSA NetWitness Platform, perform the following procedures:



- I. Ensure the required parser is enabled
- II. Configure a DSN
- III. Make Sure ODBC Collection is Running
- IV. Add the Event Source Type

For table reference, see [Reference Tables and Typespec](#) below.

## Ensure the Required Parser is Enabled

If you do not see your parser in the list while performing this procedure, you need to download it from RSA NetWitness Platform Live.



### Ensure that the parser for your event source is available:

1. In the **NetWitness** menu, select  (Admin) > **Services**.
2. In the **Services** grid, select a Log Decoder, and from the **Actions** () menu, choose **View > Config**.
3. In the **Service Parsers Configuration** panel, search for your event source, and ensure that the **Config Value** field for your event source is selected.

**Note:** The required parser is **actiancevantage**.

## Configure a DSN

### Configure a DSN (Data Source Name):

1. In the **NetWitness** menu, select  (Admin) > **Services**.
2. In the **Services** grid, select a Log Collector service and from the **Actions** () menu, choose **View > Config > Event Sources**.
3. In the Log Collector **Event Sources** tab, select **ODBC/DSNs** from the drop-down menu.
4. The **DSNs** panel is displayed with the existing DSNs, if any.
5. Click **+** to open the **Add DSN** dialog.

**Note:** To add a DSN template, see the **Configure a DSN** topic in the *Log Collection Configuration Guide*, available in [NetWitness Community](#).


6. Choose a **DSN Template** from the drop down menu and enter a name for the DSN. (Use this name when you set up the ODBC event source type.)
7. Fill in the parameters and click **Save**.

Field	Description
DSN Template	Choose the correct template from the available choices.
DSN Name	Enter a descriptive name for the DSN
<b>Parameters section</b>	
Database	Specify the database used by Actiance Vantage
PortNumber	Specify the Port Number. The default port number is <b>1433</b>
HostName	Specify the hostname or IP Address of Actiance Vantage
Driver	Depending on your NetWitness Log Collector version: <ul style="list-style-type: none"><li>• For 10.6.2 and newer, use /opt/netwitness/odbc/lib/R3sqls27.so</li><li>• For 10.6.1 and older, use /opt/netwitness/odbc/lib/R3sqls26.so</li></ul>

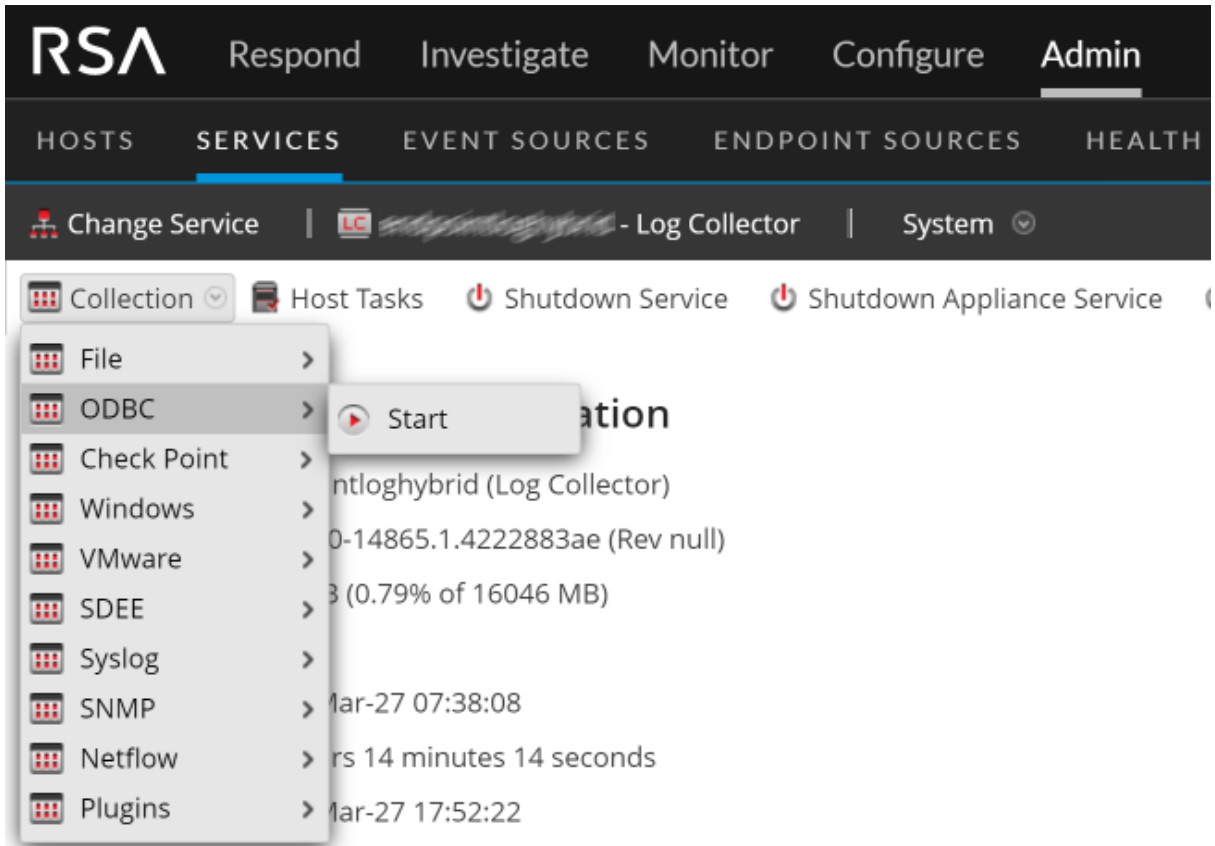
## Ensure the ODBC Collection Service is Running

The ODBC service needs to be running to collect data from ODBC event sources.

### Start the ODBC collection service:


1. In the NetWitness menu, select **Admin > Services**.
2. In the **Services** grid, select a **Log Collector** service.
3. Click  under **Actions** and select **View > System**.

- Click **Collection** > **ODBC**.

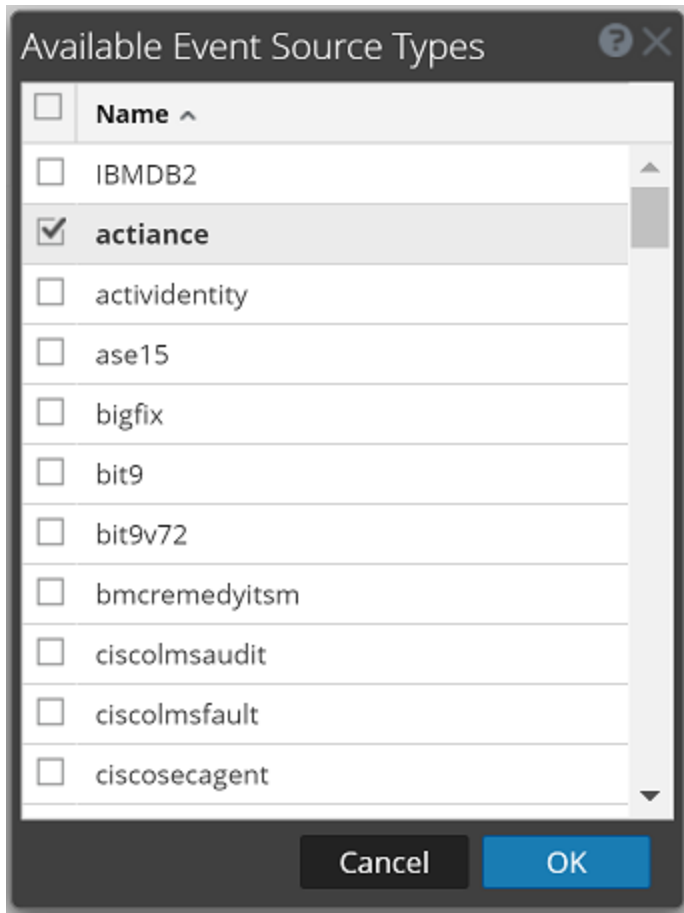


## Add the Event Source Type

### Add the ODBC Event Source Type:

- In the **NetWitness** menu, select **ADMIN** > **Services**.
- In the **Services** grid, select a **Log Collector** service.
- Click  under **Actions** and select **View** > **Config**.
- In the Log Collector **Event Sources** tab, select **ODBC/Config** from the drop-down menu.  
The Event Categories panel is displayed with the existing sources, if any.
- Click **+** to open the **Available Event Source Types** dialog.

Select **actiance** from the **Available Event Source Types** dialog.



7. In the **Event Categories** panel, select the event source type that you just added.
8. In the **Sources** panel, click **+** to open the **Add Source** dialog.

9. Enter the DSN you configured during the **Configure a DSN** procedure.
10. For the other parameters, see the **ODBC Event Source Configuration Parameters** topic in the *Log Collection Configuration Guide*, available in [NetWitness Community](#).

## ODBC Event Source Configuration Parameters

The following tables present the details for parameter used to configure ODBC event sources.

### Basic Parameters

(missing or bad snippet)

Name	Description
DSN*	The data source name (DSN) that defines the database from which to collect events. Select an existing DSN from the drop-down list. For details, see <a href="#">ODBC DSNs Event Source Configuration Parameters</a> .
Username*	User name that the data source name uses to connect to the database. You must specify a user name when you create the event source.
Password	Password that the data source name uses to connect to the database. <b>Caution:</b> The password is encrypted internally and is displayed in its encrypted form.
Enabled	Select the checkbox to enable the event source configuration to start collection. The checkbox is selected by default.
Address*	For ODBC, this field is not used. The Log Collector uses the address in the <b>ODBC.ini</b> file.

## Advanced Parameters

Name	Description
Max Cell Size	Maximum size in bytes of the data that the Log Collector can pull from one cell in the database. The default value is <b>2048</b> .
Nil Value	Character string that the Log Collector displays when NIL is returned for a cell in the database. Default value: "" (null).
Polling Interval	Interval (amount of time in seconds) between each poll. The default value is <b>180</b> . For example, if you specify 180, the collector schedules a polling of the event source every 180 seconds. If the previous polling cycle is still underway, the collector waits for that cycle to finish. If you have a large number of event sources that you are polling, it may take longer than 180 seconds for the polling to start because the threads are busy.
Max Events Poll	The maximum number of events per polling cycle (how many events collected per polling cycle).
Debug	<p><b>Caution:</b> Caution: Only enable debugging (set this parameter to On or Verbose) if you have a problem with an event source and you need to investigate this problem. Enabling debugging will adversely affect the performance of the Log Collector.</p> <p>Enables or disables debug logging for the event source. Valid values are:</p> <ul style="list-style-type: none"> <li>• <b>Off</b> = (default) disabled</li> <li>• <b>On</b> = enabled</li> <li>• <b>Verbose</b> = enabled in verbose mode - adds thread information and source context information to the messages.</li> </ul> <p>This parameter is designed to debug and monitor isolated event source collection issues. If you change this value, the change takes effect immediately (no restart required). The debug logging is verbose, so limit the number of event sources to minimize performance impact.</p>
Initial Tracking Id	Initial identification code that the Log Collector assigns to this event source if collection is not started. If there is no value for this parameter, the Log Collector starts at the end of the table and only pulls rows after the end of the table as they are added. The default value is "" (null).
Filename	For Microsoft SQL Server Event Sources only, the location of the trace files directory (for example, <b>C:\MyTraceFiles</b> ). Refer to the RSA Microsoft SQL Server Event Source Configuration Guide, located on RSA Link here: <a href="https://community.rsa.com/docs/DOC-40241">https://community.rsa.com/docs/DOC-40241</a> .
Test Connection	Checks the configuration parameters specified in this dialog to make sure they are correct.
Cancel	Closes the dialog without adding or modifying DSN parameters.
OK	Adds or modifies the parameters for the DSN.

## Advanced Parameters

### Reference Tables and Typespec

This event source collects data from the following tables:

- ActivityActions
- ActivityTypes
- AuditTrailEvent
- AuditTrailEventCategory
- AuditTrailEventSubCategory
- EventStats

The typespec file for this event source is **actiance.xml**.

## Getting Help with NetWitness Platform

---

### Self-Help Resources

There are several options that provide you with help as you need it for installing and using NetWitness:

- See the documentation for all aspects of NetWitness here: <https://community.netwitness.com/t5/netwitness-platform/ct-p/netwitness-documentation>.
- Use the **Search** and **Create a Post** fields in NetWitness Community portal to find specific information here: <https://community.netwitness.com/t5/netwitness-discussions/bd-p/netwitness-discussions>.
- See the NetWitness Knowledge Base: <https://community.netwitness.com/t5/netwitness-knowledge-base/tkb-p/netwitness-knowledge-base>.
- See the documentation for Logstash JDBC input plugin here: <https://www.elastic.co/guide/en/logstash/current/plugins-inputs-jdbc.html>.
- See Troubleshooting section in the guides.
- See also [NetWitness® Platform Blog Posts](#).
- If you need further assistance, [Contact NetWitness Support](#).

### Contact NetWitness Support

When you contact NetWitness Support, please provide the following information:

- The version number of the NetWitness Platform or application you are using.
- Logs information, even source version, and collection method.
- If you have problem with an event source, enable **Debug** parameter (set this parameter to **On** or **Verbose**) and collect the debug logs to share with the NetWitness Support team.

Use the following contact information if you have any questions or need assistance.

NetWitness Community Portal	<a href="https://community.netwitness.com">https://community.netwitness.com</a> In the main menu, click <b>Support</b> > <b>Case Portal</b> > <b>View My Cases</b> .
International Contacts (How to Contact NetWitness Support)	<a href="https://community.netwitness.com/t5/support/ct-p/support">https://community.netwitness.com/t5/support/ct-p/support</a>
Community	<a href="https://community.netwitness.com/t5/netwitness-discussions/bd-p/netwitness-discussions">https://community.netwitness.com/t5/netwitness-discussions/bd-p/netwitness-discussions</a>

## Feedback on Product Documentation

You can send an email to [feedbacknwdocs@netwitness.com](mailto:feedbacknwdocs@netwitness.com) to provide feedback on NetWitness Platform documentation.