

RSA NetWitness Platform

Event Source Log Configuration Guide



Trustwave DbProtect

Last Modified: Tuesday, June 18, 2019

Event Source Product Information:

Vendor: [Trustwave](#)

Event Source: Trustwave DbProtect

Version: 6.0

RSA Product Information:

Supported On: NetWitness Platform 10.0 and later

Event Source Log Parser: appsecdbprotect

Collection Method: ODBC

Event Source Class.Subclass: Storage.Database

To configure the Trustwave DbProtect event source to work with RSA NetWitness Platform, perform the following tasks:

- Configure Trustwave DbProtect
- Configure ODBC collection for RSA NetWitness Platform

Configure Trustwave DbProtect

To configure Trustwave DbProtect, you must add and assign privileges to a user:

- I. [Create a New User](#)
- II. [Set Account Permissions](#)
- III. [Set Database Access Permissions](#)

Create a New User

To create a new user, follow these steps:

1. From the **Object Explorer** navigation menu, expand your database server, which is the top item in the navigation pane.
2. Expand **Security**.
3. Right-click **Logins** and select **New Login**.
4. From the **Select a page** navigation menu, select **General**.
5. From the **Login name** field, type **audit_reader**.
6. Select **SQL Server authentication**.
7. Create and confirm a password.
8. Ensure that **Enforce Password Expiration** is not selected, and click **OK**.
9. From the **Select a page** navigation menu, select **User Mapping**.
10. Select the **Map** column for the AppDetective database, and click **OK**.

Set Account Permissions

To set the account permissions, follow these steps:

1. From the **Object Explorer** navigation menu, right-click your database server, and select **Properties**.
2. From the **Select a page** navigation menu, select **Permissions**.

3. From the **Login or roles** section, select **audit_reader**.
4. From the **Explicit permissions** section, select the Grant column for **Alter trace** and **Connect SQL**.
5. Click **OK**.

Set Database Access Permissions

To set the database access permissions, follow these steps:

1. From the **Object Explorer** navigation menu, expand your database server.
2. Expand **Databases > AppDetective**. Right-click **AppDetective**, and select **Properties**.
3. From the **Select a page** navigation menu, select **Permissions**.
4. From the **Login or roles** section, select **audit_reader**.
5. From the **Explicit permissions** section, select the Grant column for **Connect** and **Execute**.
6. Click **OK**.

Configure NetWitness Platform for ODBC Collection

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

- I. Ensure the required parser is enabled
- II. Configure a DSN
- III. Add the Event Source Type

For table reference, see [Reference Tables](#) 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 enabled:

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 **appsecdbprotect**.

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.
3. Click  under **Actions** and select **View > Config**.
4. In the Log Collector **Event Sources** tab, select **ODBC/DSNs** from the drop-down

menu.

5. The DSNs panel is displayed with the existing DSNs, if any.
6. Click **+** to open the **Add DSN** dialog.


Note: If you need to add a DSN template, see the "Configure DSNs" topic in the *Log Collection Configuration Guide*, available in [RSA Link](#).

7. Choose a DSN Template from the drop down menu and enter a name for the DSN. (You use the name when you set up the ODBC event source type.)
8. 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
Parameters section	
Database	Specify the database used by Trustwave DbProtect
PortNumber	Specify the Port Number. The default port number is 1433
HostName	Specify the hostname or IP Address of Trustwave DbProtect
Driver	Depending on your NetWitness Log Collector version: <ul style="list-style-type: none"> • For 10.6.2 and newer, use /opt/netwitness/odbc/lib/R3sqls27.so • For 10.6.1 and older, use /opt/netwitness/odbc/lib/R3sqls26.so

Add the Event Source Type

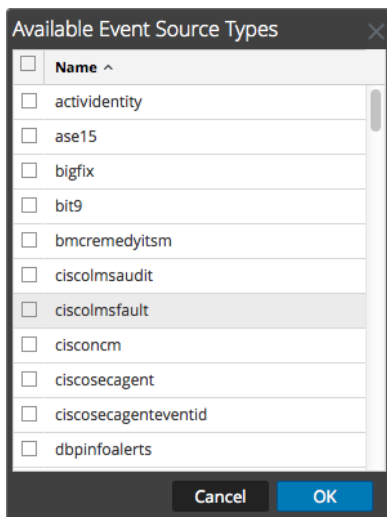
Add the ODBC Event Source Type:

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 > Config**.
4. 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.

5. Click **+** to open the **Available Event Source Types** dialog.



6. Choose the log collector configuration type for your event source type and click **OK**.

RSA NetWitness Platform collects several types of logs from the Trustwave DBProtect event source:

- To collect informational alerts, select **dbpinfoalerts** from the **Available Event Source Types** dialog.
- To collect security alerts, select **dbpsecalerts** from the **Available Event Source Types** dialog.
- To collect Penetration Test alerts, select **dbppenalerts** from the **Available Event Source Types** dialog.

To collect all these logs, repeat this procedure 3 times, each time selecting one of the available types.

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.

The screenshot shows the 'Add Source' dialog box with the following configuration:

Section	Parameter	Value
Basic	DSN *	
	Username *	
	Password	*****
	Enabled	<input checked="" type="checkbox"/>
	Address *	
Advanced	Max Cell Size	2048
	Nil Value	(null)
	Polling Interval	180
	Max Events Poll	5000
	Debug	Off
	Initial Tracking Id	
	Filename	

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 *RSA NetWitness Platform Log Collection Guide*.

Reference Tables

This event source collects data from the following tables, using the indicated typespec files.

- The following tables use the **dbpinfoalerts.xml** typespec file:
 - ins_alerts_info
 - ins_origins
 - ins_sql
 - history_sensors
 - history_rules_filters
 - risk_levels
 - app_types
- The following tables use the **dbppenalerts.xml** typespec file:

- MiscCodes
- PenTests
- hostnames
- Checks
- CheckMetaValue
- PenTestChecksStatus
- VulnerabilityDetails
- Organizations
- ScansServicesFound
- CheckLists
- The following tables use the **dbpsecalerts.xml** typespec file:
 - ins_alerts_security
 - ins_origins
 - ins_sql
 - history_sensors
 - history_rules_filters
 - risk_levels
 - app_types

Copyright © 2019 Dell Inc. or its subsidiaries. All Rights Reserved.

Trademarks

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