

RSA NetWitness Platform

Event Source Log Configuration Guide



Microsoft Forefront Endpoint Protection

Last Modified: Thursday, October 31, 2019

Event Source Product Information:

Vendor: [Microsoft](#)

Event Source:

- Forefront Endpoint Protection
- Forefront Client Security
- System Center Configuration Manager Endpoint Protection

Versions:

- Forefront Endpoint Protection 2010
- Forefront Client Security 1.x
- System Center 2012 Endpoint Protection

Platforms: Windows Server 2003, Windows Server 2003 R2, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, Windows 7, Windows 8

RSA Product Information:

Supported On: NetWitness Platform 10.0 and later

Event Source Log Parser: msforefrontcs

Collection Method:

- For **Forefront Client Security**: ODBC and Windows Event Logs
- For **Forefront Endpoint Protection** and **System Center Endpoint Protection**: Windows Event Logs

Event Source Class.Subclass: Security.Antivirus

Choose the appropriate procedure, based on which event source you are using:

- Forefront Endpoint Protection: [Configure NetWitness Platform for Windows Collection](#)
- System Center Endpoint Protection: [Configure NetWitness Platform for Windows Collection](#)
- Forefront Client Security, perform either, or both, of the following procedures:
 - [Configure NetWitness Platform for ODBC Collection](#)
 - [Configure NetWitness Platform for Windows Collection](#)

Configure NetWitness Platform for ODBC Collection

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

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

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 in 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 **msforefrontes**.

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 Forefront Client Security
PortNumber	Specify the Port Number. The default port number is 1433
HostName	Specify the hostname or IP Address of Forefront Client Security
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

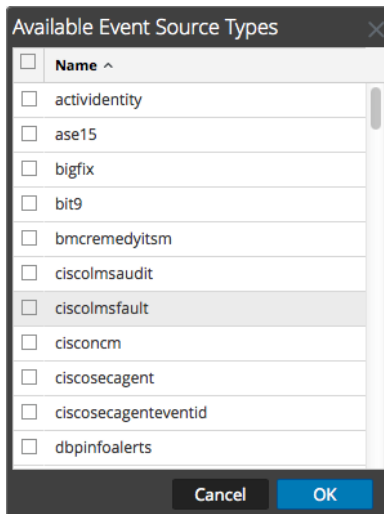
Add the Event Source Type

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.

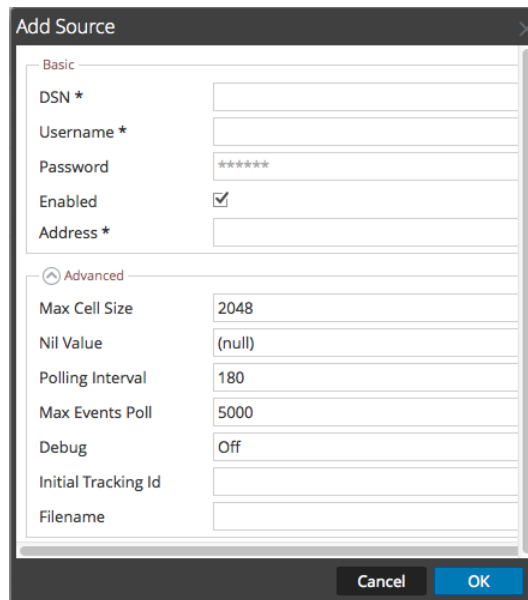
5. Click **+** to open the **Available Event Source Types** dialog.



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

Select **ms_forefront_client_security** 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.



The screenshot shows a dialog box titled "Add Source" with a close button (X) in the top right corner. The dialog is divided into two sections: "Basic" and "Advanced".

Basic Section:

- DSN *: [Empty text box]
- Username *: [Empty text box]
- Password: [Text box containing "*****"]
- Enabled:
- Address *: [Empty text box]

Advanced Section:

- Max Cell Size: [Text box containing "2048"]
- Nil Value: [Text box containing "(null)"]
- Polling Interval: [Text box containing "180"]
- Max Events Poll: [Text box containing "5000"]
- Debug: [Text box containing "Off"]
- Initial Tracking Id: [Empty text box]
- Filename: [Empty text box]

At the bottom of the dialog, there are two buttons: "Cancel" and "OK".

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*.

Configure NetWitness Platform for Windows Collection

For all supported version of this event source, you can configure Windows collection.

Note: For Forefront Client Security, you should collect from the **Forefront Endpoint Protection** channel. For System Center 2012 Endpoint Protection, use **System**. Choose the appropriate channel when you configure the Windows Event Type in the procedure below.

To configure WinRM, see the following document on RSA Link: [Microsoft WinRM Configuration and Troubleshooting](#). For more details about Windows Collection in the RSA NetWitness Platform, see the [Configure Windows Collection](#) topic on RSA Link.

Note: When you configure the Windows Event Type as described in the Microsoft WinRM Configuration Guide, you should collect from the **Forefront Endpoint Protection** channel. For System Center 2012 Endpoint Protection, use **System**.

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.