

NetWitness[®] Platform XDR

Kaspersky Anti-Virus Event Source Log Configuration Guide

Kaspersky Anti-Virus

Event Source Product Information:

Vendor: [Kaspersky](#)

Event Source: Kaspersky Anti-Virus

Versions:

- Kaspersky Security Center 9.0, 10.x, 11.x, 14.0
- Kaspersky Administration Kit 8.0
- Kaspersky Anti-Virus for Microsoft ISA Server 2004 Enterprise Edition and 2006 Enterprise Edition.

RSA Product Information:

Supported On: NetWitness Platform XDR 11.7 or later

Note: Kaspersky Anti-Virus is supported from NetWitness Platform XDR 11.5 or later. However, NetWitness recommends you to update NetWitness Platform XDR to the latest version.

Event Source Log Parser: kasperskyav

Collection Method: ODBC and File

Event Source Class.Subclass: Security.AntiVirus

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/>.

© 2023 RSA Security LLC or its affiliates. All Rights Reserved.

September, 2022

Contents

- Introduction to Kaspersky Anti-Virus 5**
- Configure NetWitness Platform XDR for ODBC Collection 6**
 - Ensure the Required Parser is Enabled 6
 - Configure a DSN 6
 - Add the Event Source Type 7
 - Reference Tables 9
- Configure File Collection for Kaspersky Anti-Virus 10**
 - Configure Kaspersky Anti-Virus for Microsoft ISA Server 10
 - Set Up the SFTP Agent 11
 - Configure the Log Collector for File Collection 11
- Getting Help with NetWitness Platform XDR 13**
 - Self-Help Resources 13
 - Contact NetWitness Support 13
 - Feedback on Product Documentation 14

Introduction to Kaspersky Anti-Virus

Kaspersky Endpoint Security for Business provides a tiered security approach based on a single integrated platform incorporating features including robust application, device and web control tools, data encryption, mobile endpoint security and MDM, and systems and patch management. Everything is managed from one central console — Kaspersky Security Center.

You can configure NetWitness Platform XDR to use ODBC or File collection for the Kaspersky Anti-Virus event source.

- If you use Kaspersky Security Center (previously Kaspersky Administration Kit), you must configure ODBC collection. For more information, see [Configure RSA NetWitness Platform XDR for ODBC Collection](#).
- If you use Kaspersky Anti-Virus for Microsoft ISA Server you must configure File collection. For more information, see [Configure File Collection for Kaspersky Anti-Virus](#).

Configure NetWitness Platform XDR for ODBC Collection

To configure ODBC collection in NetWitness Platform XDR, 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 XDR 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 **kasperskyav**.

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](#).

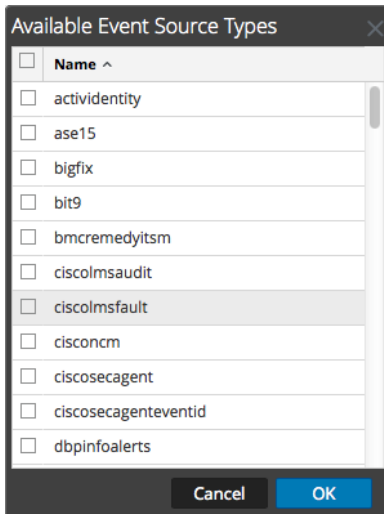
6. Choose a **DSN Template** from the drop down menu and enter a name for the DSN. (Use this name when you set up the ODBC event source type.)
7. Fill in the parameters and click **Save**.

Field	Description
DSN Name	Enter a descriptive name for the DSN
Parameters section	
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
Database	Enter the name of the database you are using with RSA NetWitness Platform XDR.
PortNumber	The default port is 1433 .
HostName	Enter the Kaspersky Anti-Virus IP address or host name. The default value is localhost .

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, and from the **Actions** () menu, choose **View > Config**.
3. 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.
4. Click **+** to open the **Available Event Source Types** dialog.

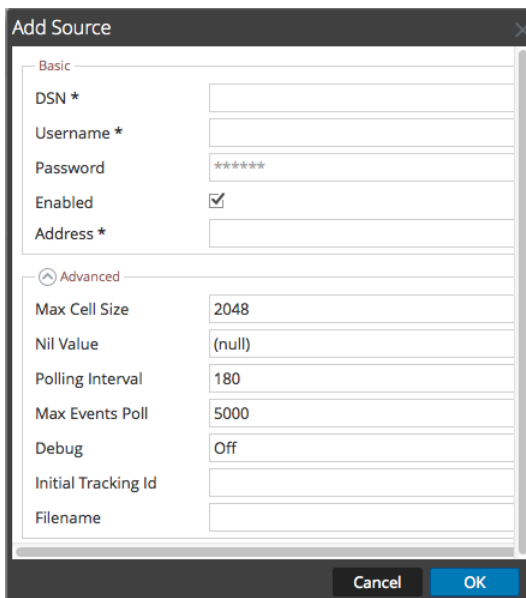


5. Choose the log collector configuration type for your event source type and click **OK**.

Select the appropriate value, based on your version, from the **Available Event Source Types** dialog:

- For Kaspersky Security Center 11.x, select **kasperskyav11**.
- For Kaspersky Security Center 9.0 or 10.x, select **kasperskyav9**.
- For Kaspersky Administration Kit 8.0, select **kasperskyav**.

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](#).

Reference Tables

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

- The **v_full_event** table use the **kasperskyav.xml** typespec file.
- The following tables use the **kasperskyav9.xml** typespec file:
 - v_akpub_ev_event
 - v_akpub_host

To export events in CEF format for Kaspersky Security Center version 14.0, see [About exporting events using CEF and LEEF formats](#).

Note: The required parser is *cef*.

Configure File Collection for Kaspersky Anti-Virus

You must complete these tasks to configure Kaspersky Anti-Virus for Microsoft ISA Server for File collection:

- I. Configure Kaspersky Anti-Virus for Microsoft ISA Server
- II. Set up the SFTP Agent
- III. Set Up the File Service

Configure Kaspersky Anti-Virus for Microsoft ISA Server

To configure Kaspersky Anti-Virus for Microsoft ISA Server:

1. Open the Administration Console.
2. In the Connect window, set the options appropriate to your server, and click **Next**.
3. In the Connect to array window, select your array, and click **Finish**.
4. In the directory panel, select your array.
5. Click **Edit Kaspersky Anti-Virus Settings**.
6. In the Properties of Kaspersky Anti-Virus for Microsoft ISA Server window, follow these steps:
 - a. On the **HTTP** tab, select **Disinfect HTTP traffic**.
 - b. On the **FTP** tab, click **Set default values**.
 - c. Click **OK**.
7. Click **Manage Servers**, and select the server you want to configure.
8. Click **Edit Server Settings**.
9. In the Properties of Kaspersky Anti-Virus for Microsoft ISA Server window, on the **Diagnostics** tab, follow these steps:

Warning: In the **Path to log files** field, do not alter the default path.

- a. From the list, select each product component, and use the drop-down list to set all diagnostic levels to **Debug**.

Note: You do not need to alter the diagnostic levels for the Licensing component.

- b. Click **Apply**.
- c. Click **OK**.

Set Up the SFTP Agent



To set up the SFTP Agent Collector, download the appropriate PDF from NetWitness Link:

- To set up the SFTP agent on Windows, see [Install and Update SFTP Agent](#)
- To set up the SFTP agent on Linux, see [Configure SFTP Shell Script File Transfer](#)

Configure the Log Collector for File Collection

Perform the following steps to configure the Log Collector for File collection.

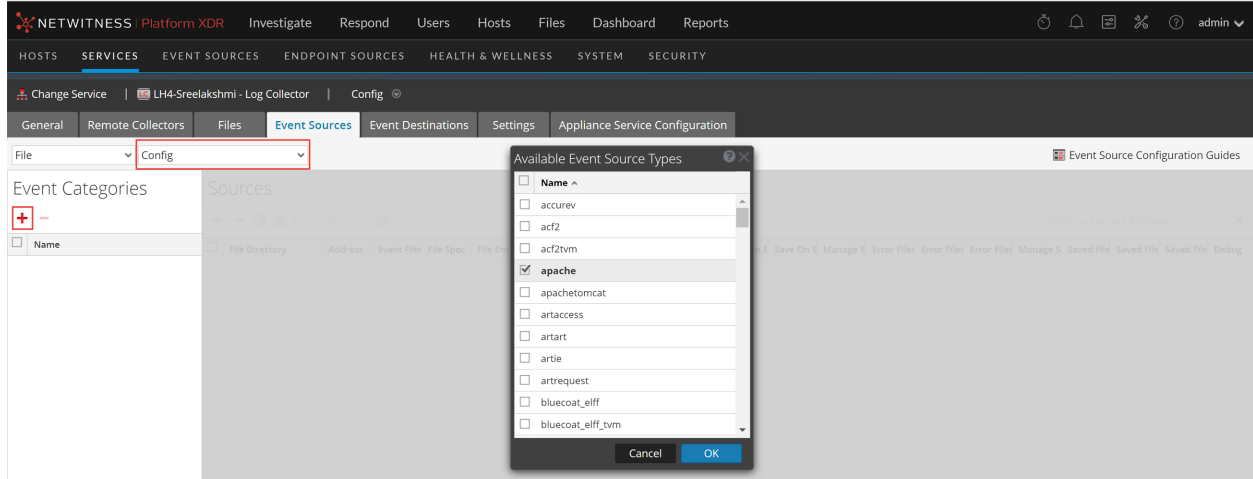
To configure the Log Collector for file collection:

1. In the **NetWitness** menu, select  (Admin) > **Services**.
2. In the **Services** grid, select a Log Collector, and from the **Actions** () menu, choose **View** > **Config** > **Event Sources**.
3. Select **File/Config** from the drop-down menu.

The Event Categories panel displays the File event sources that are configured, if any.

4. In the **Event Categories** panel toolbar, click **+**.

The **Available Event Source Types** dialog is displayed.

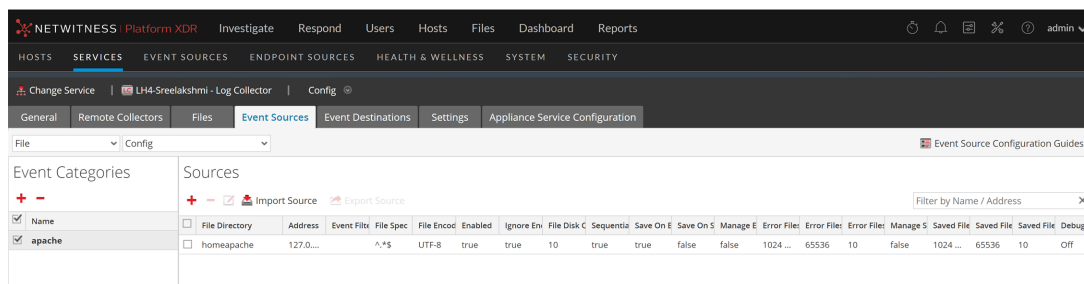


1. Select the correct type from the list and click **OK**.

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

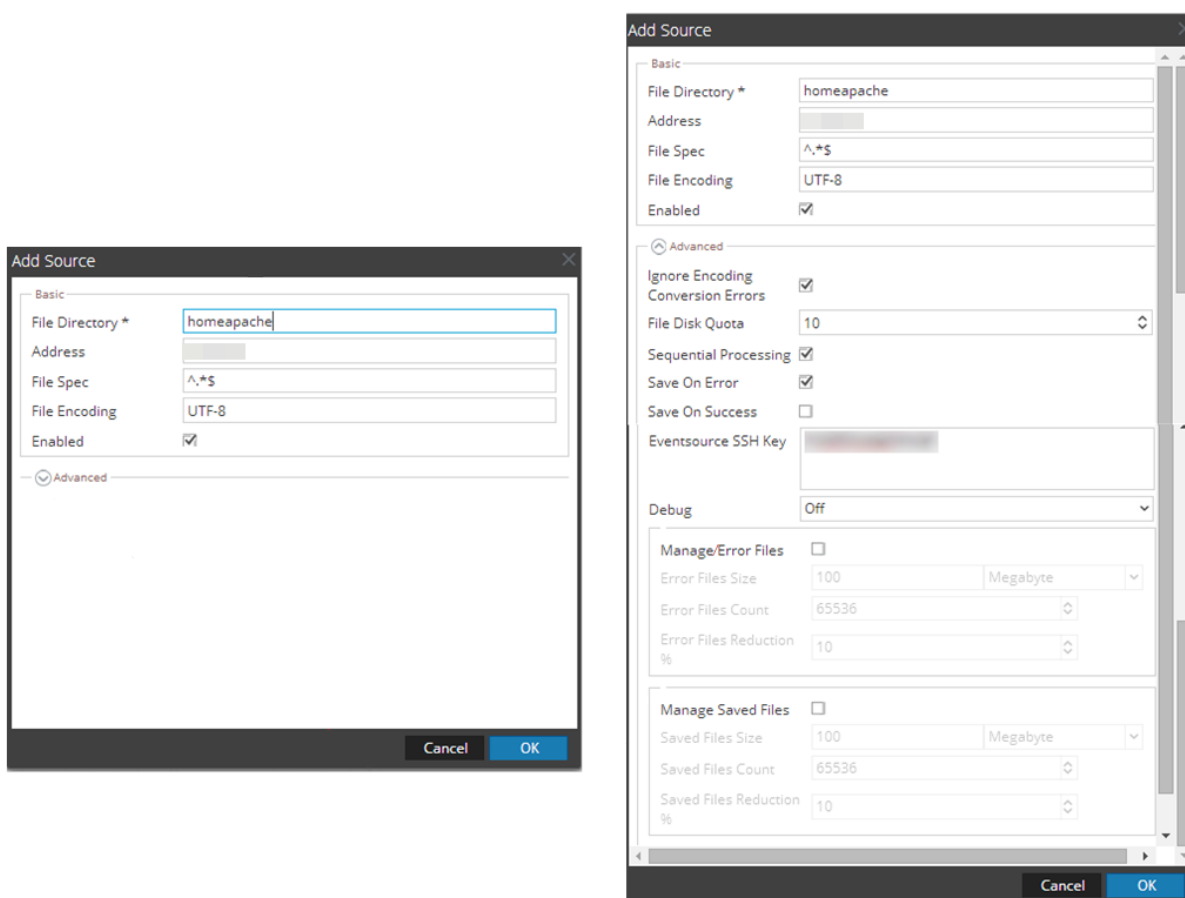
The newly added event source type is displayed in the Event Categories panel.

Note: The image below uses **Apache** as an example only. Your screen will look different, depending on which Event Source type you are configuring.



6. Select the new type in the Event Categories panel and click **+** in the Sources panel toolbar. The **Add Source** dialog is displayed.

Note: Again, the image below uses **Apache** as an example only. Your screen will look different, depending on which Event Source type you are configuring.



7. Add a File Directory name, modify any other parameters that require changes, and click **OK**.
8. Stop and Restart File Collection. After you add a new event source that uses file collection, you must stop and restart the NetWitness File Collection service. This is necessary to add the key to the new event source.

Getting Help with NetWitness Platform XDR

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

Feedback on Product Documentation

You can send an email to nwdocsfeedback@netwitness.com to provide feedback on NetWitness Platform documentation.