# NetWitness® Platform

# Accurev Event Source Configuration Guide

NETWITNESS
Platform

# Accurev

Last Modified: Monday, December 2, 2024

### Event Source Product Information:

**Vendor**: Accurev

**Event Source**: Accurev

**Versions**: 6.0.1

**Additional Downloads**:

- sftpagent.conf.accurev
- passwdConfig.pl
- passwdUtils.pl
- server_admin_trig.pl
- server_user_utilities.pl
- server_utilities triggers.pl
- server_auth_trig.pl

### RSA Product Information:

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

**Event Source Log Parser**: accurev

**Collection Method**: File

**Event Source Class.Subclass**: Storage.Content Management Systems

## 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.

## 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/.



November 2024

# Contents

# Configure Accurev

To configure Accurev, you must complete these tasks:

I. Configure Accurev to generate logs

II. Set Up the SFTP Agent

III. Set up the File Service

## Configure Accurev to generate logs

1. Create a **triggers** directory inside the `storage/site_slice` directory.
2. Use a browser to navigate to the Accurev Additional Downloads page in the NetWitness PlatformEvent Source Downloads space.
3. Download the following trigger PERL scripts and copy them into the **triggers** directory that you created in step 1.
   - server_auth_trig.pl
   - passwdConfig.pl
   - passwdUtils.pl
   - server_admin_trig.pl
   - server_user_utilities.pl
   - server_utilities triggers.pl
4. Change the extension for the files based on your OS. For example, rename **server_auth_trig.pl** as follows:
   - Linux/UNIX: leave as **server_auth_trig.pl**, or rename to **server_auth_trig**
   - Windows: rename to **server_auth_trig.bat**
5. In the same manner, change the extensions for the other files.

   For example on Windows, you might have the following path for **server_admin_trig.bat**:

   ```
   C:\Program Files\AccuRev\storage\site_slice\triggers\server_admin_trig.bat
   ```

## 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, seeInstall 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

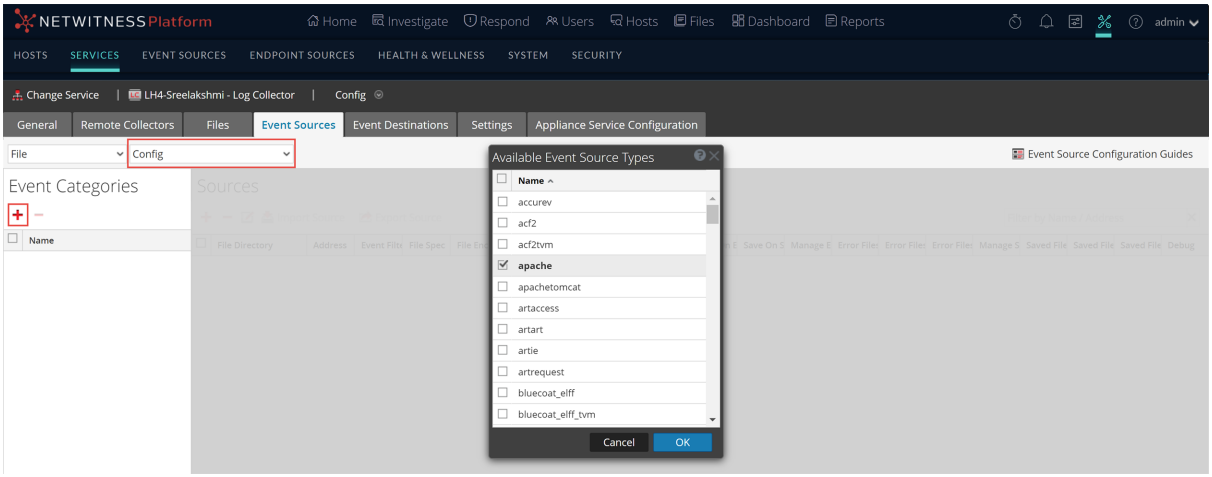
Perform the following steps to configure the Log Collector for File collection.

### 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.

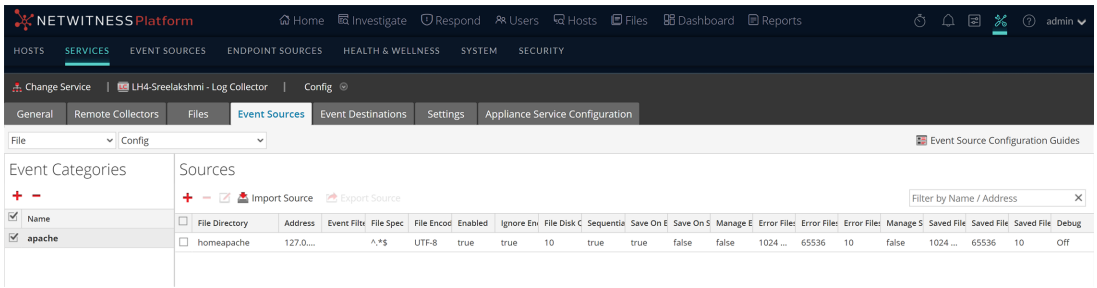



5. Select the correct type from the list and click **OK**.

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

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

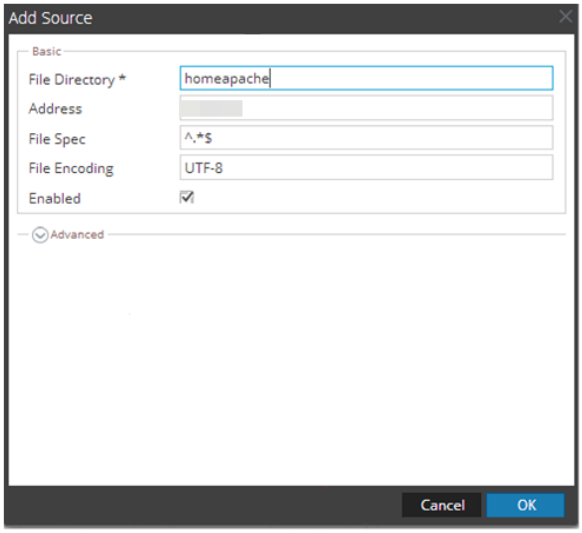
   **Note:** The image below uses **Apache** as an example only. Your screen will look different, depending on which Event Source type you are configuring.

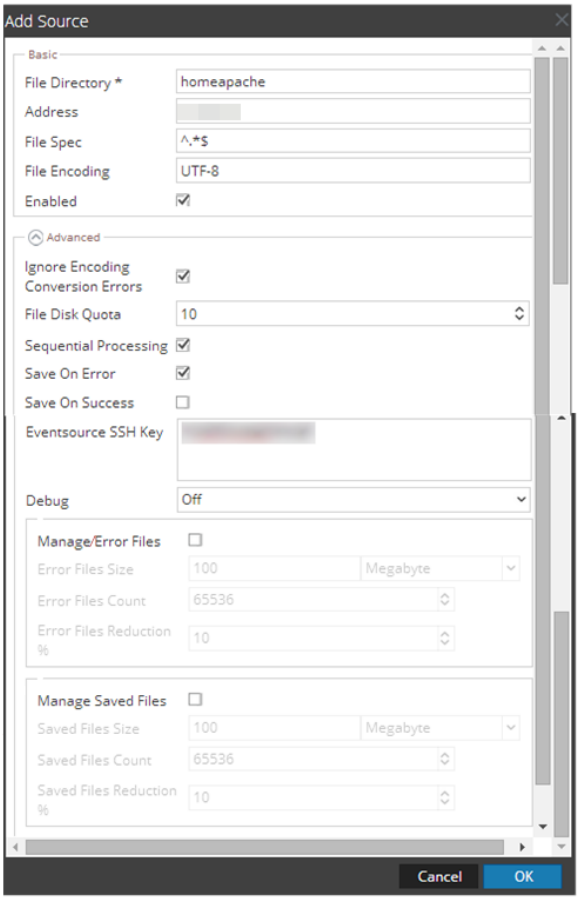


6. Select the new type in the Event Categories panel and click + in the Sources panel toolbar.

   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

## 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 | https://community.netwitness.com<br>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 feedbacknwdocs@netwitness.com to provide feedback on NetWitness Platform documentation.