# NetWitness® Platform XDR

## Configure SFTP Shell Script

NETWITNESS
Platform XDR

## 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.



November, 2022

# Contents

# Configure SFTP Shell Script File Transfer

Use the **sasftpagent.sh** shell script to transfer text-based log data from Linux systems. This script takes data slices from active log files, but only transfers the new data each time the script runs.

Schedule the script in cron to run as often as you want log data sent to the NetWitness Log Collector. The script uses the SFTP or SCP protocol to transfer the data.

Note the following:

- All connections are initiated from the system to NetWitness Platform XDR.
- The script runs on all POSIX compliant Unix/Linux systems and shells.

  **Note:** You must use OpenSSH version 4.4p1 or later.

- NetWitness recommends that you set up a cron job to run the script at specified time intervals. However, if you do set up a cron job, make sure to run it as a user that has access to the logs that need to be sent to NetWitness Platform XDR.

This topic contains the following information:

- Enhancements for version 3 of the Agent
- Instructions for Upgrading the Agent: follow these steps if you are currently running version 2.7 of the agent
- Instructions for Installing the Agent: follow these steps if you are downloading the agent for the first time
- Details for the Shell Script Parameters
- Instructions to Configure the NetWitness Log Collector to Receive Log Files

You must perform the following steps to complete the installation and configuration of the agent:

I. Install or Upgrade the agent, depending on whether or not you are running it currently.

II. Configure the the NetWitness Log Collector to Receive Log Files.

# Enhancements for Version 3

- The script runs on all POSIX compliant Unix/Linux systems and shells.
- Expects configuration at `/etc/rsa/sasftpagent.conf`.
- Encourages the user to keep configuration separate from script source. Warning is logged if the user does not do so.
- Persistent state is written to `/var/lib/rsa` by default.
- Enhanced user interaction, such as:
  - Support for running the script without root privileges.
  - The agent has been made highly configurable so that it can be configured to run from anywhere, and create a persistent state directory anywhere. For example, non-root users can persist state information to their home directory, by specifying an alternate persistent state directory in the configuration file.
  - A configuration specified at a non-root user's home directory (e.g. `~/sasftpgent.conf`) is automatically picked up while running as a non-root user.
  - Command line options (`-C` or `--config`) have been added to point the agent to custom configuration.
- Logs are written to `/var/log/rsa/sasftpagent.log`. Logging levels have been introduced so that the logs may be filtered for WARN, ERROR and FATAL entries, to help troubleshoot issues. These log entries can now be used to perform troubleshooting after the fact.
- If the user forgets to edit the configuration, a FATAL log entry is generated. The entry contains a clear message that the user needs to edit the configuration before the script can be used.

# Upgrade the Agent

If you have used a version of **sasftpagent.sh** prior to version 3, then you should follow the instructions in this section to upgrade to the latest version.

The major steps are as follows:

I. Download the Agent from RSA NetWitness SFTP Agent Downloads on NetWitness Community link.

II. Move configuration information to `/etc/rsa/sasftpagent.conf`.

III. Download the **mvpersinfo.sh** script.

IV. Run the **mvpersinfo.sh** script to move persistent information to the location used by version 3.

V. Run version 3 of the agent.

## Move Configuration Information

In version 2.7, the user configuration was specified in one of the following two locations:

- The configuration may have been edited inline within `/usr/local/sa/sasftpapgent.sh` (or wherever you placed the script).
- The configuration may have been specified separately; wherever the **CONFIG_FILE** parameter in the sasftpagent.sh script is set.

For any parameters that you edited within the script or that you specified in the separate configuration file, you need to move them to a separate file in the following location: `/etc/rsa/sasftpagent.conf`.

The following parameters are the ones that users often change during configuration:

- SA
- DATA_DIRECTORY
- FILESPEC
- FLAG_REMOVE_AFTER_SEND (only set if you wanted to remove data files automatically after transferring them to the Log Collector).

## Download the Script

1. Navigate to RSA NetWitness SFTP Agent Downloads.

   **Note:** You need to log on with credentials supplied to you by NetWitness.

2. Click **mvpersinfo.sh** to download the script.

# Move Persistent Information

In version 2.7, the persistent state information is maintained in the `/usr/local/sa` directory by default. It can also be specified in the **PERSINFO_DIRECTORY** parameter.

The persistent information directory contains tracking files that contain the number of lines, for each data file, that have already been transferred to the Log Collector. The agent uses this information to figure out which lines in each file are new, since the last time it ran. It then transfers only the new data, and updates the tracking files accordingly.

It is important to move these files into the new location before you run version 3.0.1 of the agent. NetWitness provides a script, **mvpersinfo.sh**, for moving the persistent information.

## Run the Move Script

**To move the persistent information to its new location, perform the following steps:**

1. Copy **mvpersinfo.sh** to the system where you run version 2.7 of the agent.
2. Open **mvpersinfo.sh** with a text editor, and confirm that **OLD_PERSINFO_DIRECTORY** is set to the value set for **PERSINFO_DIRECTORY** in your 2.7 configuration.
3. Run the script using the following command:

   ```
   sh mvpersinfo.sh
   ```

If there are no errors, and the script runs successfully, it does not generate any output.

## Confirm the Files Were Moved

**After you run the script, you can confirm the successful movement by using the following procedure:**

1. Run the following command to get a list of the old tracking files:

   ```
   find /usr/local/sa -name "*-*last.line"
   ```

2. Run the following command to get a list of the new tracking files:

   ```
   find /var/lib/rsa/sasftpagent -name "*-*last.line"
   ```

3. Compare the output from the two commands. The output should be similar, with the only difference being the paths to the files. Here is a sample of the results of running these commands after moving the persistent files:

```
$ find /usr/local/sa -name "*-*last.line"

     /usr/local/sa/opt/log/bar.log-sa.last.line
     /usr/local/sa/opt/log/foo.log-sa.last.line
     usr/local/sa/var/log/foo.log-sa.last.line
     /usr/local/sa/var/log/fob.log-sa.last.line

$ find /var/lib/rsa/sasftpagent -name "*-*last.line"
```

```
/var/lib/rsa/sasftpagent/track/opt/log/bar.test-last.line
/var/lib/rsa/sasftpagent/track/opt/log/foo.test-last.line
/var/lib/rsa/sasftpagent/track/var/log/foo.test-last.line
/var/lib/rsa/sasftpagent/track/var/log/fob.test-last.line
```

# Install and Configure the Agent

If you are not upgrading from a previous version of the agent, follow the steps in this section to download, install, and configure the agent.

I. Download the Agent

II. Create or Configure a User Account to Run the Agent

III. Create and Update the Configuration File

IV. Schedule the Agent to Run Periodically: Configure cron or your OS scheduler to automate running the script at your desired interval.

## Download the Agent

Follow these steps to download the SA SFTP Agent (**sasftpagent.sh**) from NetWitness Community link.

1. Navigate directly to the NetWitness SFTP Agent Downloads URL on NetWitness Community link: RSA NetWitness SFTP Agent Downloads.

   **Note:** Log in with the credentials supplied to you by NetWitness.

2. Click **RSA NetWitness Unix SFTP Agent** and save the file anywhere on your file system.
3. Set execute permissions on the **sasftpagent.sh** file. For example, run the following command:

   ```
   chmod 755 /usr/local/sa/sasftpagent.sh
   ```

## Select a User Account to Run SFTP Agent Service

After you import the public key to the Log Collector (for details, see Generate the Public or Private Key Pair later in this document), you must set up the SFTP user.

1. Create the SFTP group, if it doesn't already exist. Run the following command:

   ```
   groupadd sftp_users
   ```

2. Create the SFTP user by running the following command, where USERNAME is the name of the user that you want to use:

   ```
   useradd -g sftp_users -d /upload -s /sbin/nologin USERNAME
   ```

3. Create a password for the SFTP user:

   ```
   passwd USERNAME
   ```

   where USERNAME matches the name you created in step 2.

## Create and Update the Configuration File

Create the configuration file here: `/etc/rsa/sasftpagent.conf`. If you do not have a configuration file, copy the script file (**sasftpagent.sh**) and remove everything but the configuration parameters. Update the configuration file with the information for your environment. For reference, see the Shell Script Parameters table below.

If you are running the script for the first time, run the following command, where ***collector-IP*** is the IP address of your NetWitness Log collector:

```
sftp collector-IP
```

**Caution:** It is important to run this command as the same user who will run it when it is automated.

# Shell Script Parameters

The following table describes the most important parameters that you need to set when configuring the script.

| Parameter | Values | Description |
|---|---|---|
| **SA** | Name or IP address | The name or IP address of your NetWitness Log Collector host. |
| **DATA_ DIRECTORY** | Directory path or paths, separated by colons (:) | The local source for the log data. For example:<br>`DATA_DIRECTORY=/var/log:/var/log/audit`<br>You can specify one or more folders.<br>**Note:** All folders that you specify are searched for the file names that you specify in the FILESPEC parameter. |
| **FILESPEC** | File name or names, separated by colons (:) | File mask that matches the log files to be processed by the script.<br>**Note:** The script supports line-by-line text data. Thus, .xml, .zip, .gz, .exe and other non-text formats are not supported.<br>For example, to process all files in the folder:<br>`FILESPEC=isi_webui.log:smb.log:/etc/logs/*.*`<br>**Note:** The files that you specify can reside in different folders. Make sure to list all of the necessary folders in the **DATA_DIRECTORY** parameter. |
| **SA_ DIRECTORY** | The directory name of your NetWitness Log Collector host | The destination folder name. For example:<br>`/upload/apache/muditapache` |
| **TRANSFER_ METHOD** | **SFTP**, or **SCP** | SFTP is the default (and recommended) transfer protocol. |
| **USEHEAD** | A non-negative integer, representing the number of header lines | The number of lines in each log file to be considered as a header that must be transferred to Log Collector in each transfer.<br>You can set this to 0 to indicate that there are no header lines. |
| **DEPTH** | A positive integer, representing number of folder levels | Governs how many levels deep the script searches to find logs under the configured DATA_DIRECTORY.<br>Defaults to **DEPTH=1**, which causes the script to search for data files directly under the directories configured in DATA_ DIRECTORY, but not in any sub-folders. |
| **SFTP and SCP Settings** | | |

| Parameter | Values | Description |
|---|---|---|
| **USERNAME** | **sftp** | Default setting for SSH daemon on the NetWitness Platform XDR platform. |
| **IDENTITY** | File path | Location of the private key used to connect to NetWitness Platform XDR. For instructions on generating keys, see Configure NetWitness Log Collector to Receive Log Files.<br>The default value is the following:<br>`$HOME/.ssh/id_rsa` |

# Configuration Script Information

All configuration settings can be loaded using a configuration file that is separate from the script. This file should contain one setting and one value per line (except for DATA_DIRECTORY and FILESPEC, which can contain multiple colon-separated entries).

The configuration file must be located in the directory assigned by SA_DIRECTORY in the shell script or in the path of the shell that calls the script. The SA_DIRECTORY can be overridden in the configuration file, although the shell script will try to use its own SA_DIRECTORY setting to open the configuration file.

For example, a configuration file could contain the following information:

```
SA=10.31.246.168
DATA_DIRECTORY=/var/log/httpd
SA_DIRECTORY=/upload/apache/muditapache
USERNAME=sftp
FILESPEC=*_log*
FLAG_REMOVE_FILE_AFTER_SEND=no
```

# Configure NetWitness Log Collector to Receive Log Files

For new event sources, there are two steps:

I. Run the `sftp` command

II. Generate the public or private key pair and copy it into the NetWitness Platform XDR.

## Run the `sftp` Command

Before you configure the Log Collector, remember to run the following command on any new event source, from which NetWitness Platform XDR has not previously collected logs using SFTP or SCP:

`sftp` ***`collector-IP`***

where ***collector-IP*** is the IP address of your NetWitness Log collector.

## Generate the Public or Private Key Pair

**To configure NetWitness Platform XDR to receive the log files:**

1. On the Linux or Unix event source, run the following command to generate the public or private key pair:

   ```
   ssh-keygen -b 1024 -t rsa
   ```

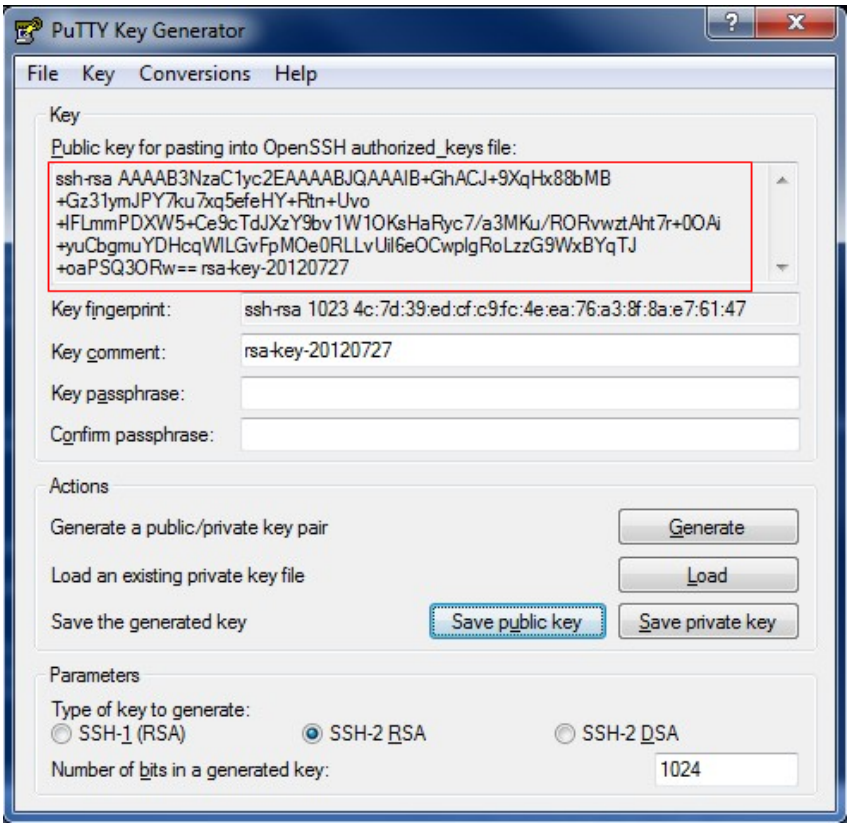
   This command creates id_rsa in OpenSSH format, which is used by NetWitness Platform XDR. If your Linux system creates IETF SECSH format by default, run the following command to convert it:

   ```
   ssh-keygen -f ~/.ssh/id_rsa.pub -i
   ```

   **Note:** If you are unable to generate the public or private key pair, see Troubleshooting.

2. Copy the public key into your buffer so that you can paste it into the parameter in NetWitness Platform XDR.

   In the following example, the public key is enclosed in a red box.




word-break: break-all; to all of the <td> tags for the second column i

3. You need to paste the key into the **Eventsource SSH Key** field in the File Event Sources configuration for the applicable event source.

   a. Go to **Admin > Services** from the NetWitness Platform XDR menu.

   b. Select a Log Collection service.

   c. Under **Actions**, select  **> View > Config** to display the Log Collection configuration parameter tabs.

   d. Click the **Event Sources** tab.

   e. In the **Event Sources** tab, select **File/Config** from the drop-down menu.

   f. In the **Event Categories** panel toolbar, do one of the following:

   - Select an existing event source to modify, or
   - Click  to add a new event source, then select a file event source type and click **OK**.

   g. Select the event source type in the **Event Categories** panel and click  in the **Sources** toolbar to add a new source, or  to edit an existing source.

   The **Add Source** dialog is displayed.

   h. Click **Advanced** to view the **Eventsource SSH Key** field.

i. Paste the public key that you copied in step 2 into the **Eventsource SSH Key** field, and click **OK**.

## Troubleshooting

This section provides information about the possible issue while generating public or private key pair.

| | |
|---|---|
| **Problem** | While generating **1024** bit public or private key pair for FIPS Compliant appliances, an error `key_generate failed` is displayed along with the message `rsa_generate_private_key: the key length might be unsupported by FIPS mode approved key generation method`. In some cases, only `key_generate failed` error is displayed. |
| **Cause** | **1024** bit public or private key pair cannot be generated for FIPS Compliant appliances, as the key size should be **2048** bits or higher. |
| **Solution** | To generate public or private key pair for FIPS Compliant appliances, run the command `ssh-keygen -b 2048 -t rsa`. |

# 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 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<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.