

# RSA NetWitness Platform

## Event Source Log Configuration Guide



## Microsoft Dynamic Host Configuration Protocol Server

Last Modified: Wednesday, January 22, 2020

### Event Source Product Information:

**Vendor:** [Microsoft](#)

**Event Source:** Dynamic Host Configuration Protocol (DHCP) Server

**Versions:** Windows 2000, Windows 2003, Windows 2008, Windows 2012, Windows 2019

**Additional Downloads:** sftpagent\_conf\_msdhcpwin2000.txt, sftpagent\_conf\_msdhcpwin2003.txt sftpagent.conf.msdhcpwin2k8, sftpagent.conf.msdhcpwin2k12, sftpagent.conf.msdhcpwin2k19

Link to Additional Downloads on RSA Link: [Microsoft DHCP Additional Downloads](#)

### RSA Product Information:

**Supported On:** NetWitness Platform 10.0 and later

**Event Source Log Parser:** msdhcp

**Collection Method:** File

**Event Source Class.Subclass:** Host.Application Servers

You must complete these tasks to configure Microsoft DHCP Server to work with RSA NetWitness Platform:

- I. Configure Microsoft DHCP server.
- II. Set up the SFTP Agent
- III. Configure the RSA NetWitness Platform Log Collector for File Collection

## Configure Microsoft DHCP Server

---

Follow the appropriate instructions for your version of Microsoft DHCP Server.

### To configure Microsoft DHCP Server 2008, 2012, or 2019:

1. Open the Microsoft DHCP Service Manager.
2. In the left-hand pane, double-click the server name.
3. To configure IPv4 properties, double-click **IPv4**, and follow these steps:
  - a. Right-click **IPv4**, and select **Properties**.
  - b. On the **General** tab, make sure that **Enable DHCP audit logging** is selected.
  - c. Click the **Advanced** tab, and take note of the audit log file path.

**Note:** You will need to supply this path name when you set up the RSA SFTP Agent.

- d. Click **OK**.
4. To configure IPv6 properties, double-click **IPv6**, and follow these steps:
  - a. Right-click **IPv6**, and select **Properties**.
  - b. On the **General** tab, make sure that **Enable DHCP audit logging** is selected.
  - c. Click on **Advanced** tab, and take note of the audit log file path.

**Note:** You will need to supply this path name when you set up the RSA SFTP Agent.

- d. Click **OK**.

### To configure Microsoft DHCP Server 2000 or 2003:

1. Open the Microsoft DHCP Server administration console.
2. In the left-hand pane, right-click the server name, and select **Properties**.
3. On the **General** tab, make sure that **Enable DHCP audit logging** is selected.
4. Click the **Advanced** tab, and take note of the audit log file path.

**Note:** You will need to supply this path name when you set up the RSA SFTP Agent.

5. Click **OK**.

## Set Up SFTP Agent and File Collection

### Set Up the SFTP Agent

To set up the SFTP Agent Collector for Windows, see [Install and Update SFTP Agent](#).

### Configure the Log Collector for File Collection

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

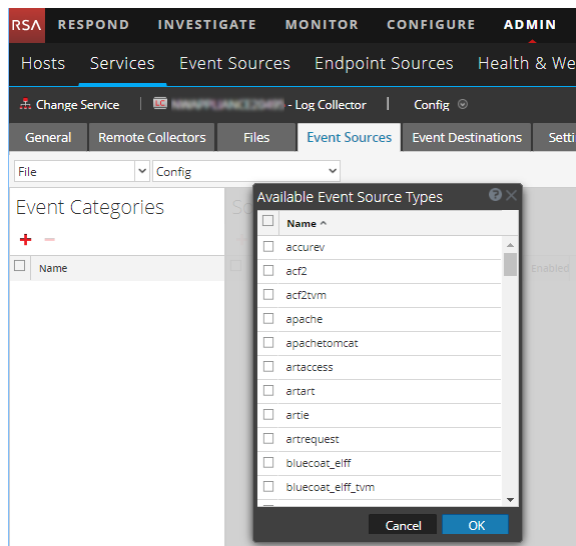
**To configure the Log Collector for file collection:**

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.



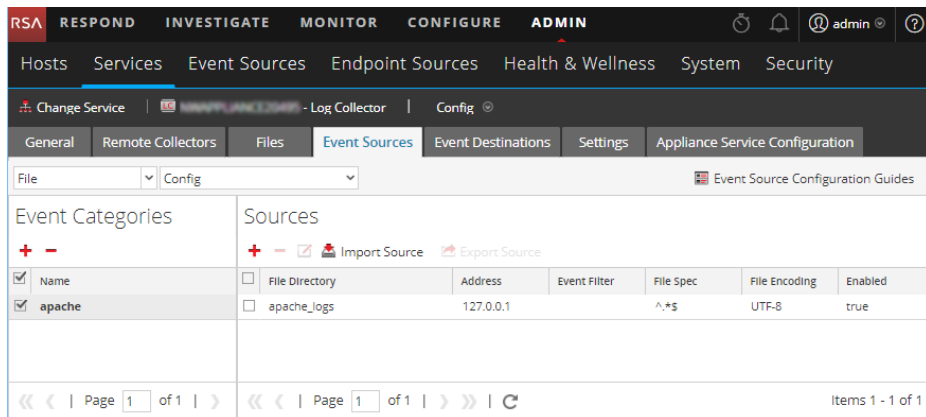
5. Select the correct type from the list, and click **OK**.

From the **Available Event Source Types** dialog, select the appropriate type, based on your version:

- If you are using Windows 2000, select **microsoft\_dhcp\_2000**
- If you are using Windows 2003, select **microsoft\_dhcp\_2003**
- If you are using Windows 2008, select **microsoft\_dhcp\_2008**
- If you are using Windows 2012, select **microsoft\_dhcp\_2012**
- If you are using Windows 2012, and DHCP for IPv6, select **microsoft\_dhcpv6\_2012**
- If you are using Windows 2019, select **microsoft\_dhcp\_2019**
- If you are using Windows 2019, and DHCP for IPv6, select **microsoft\_dhcpv6\_2019**

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

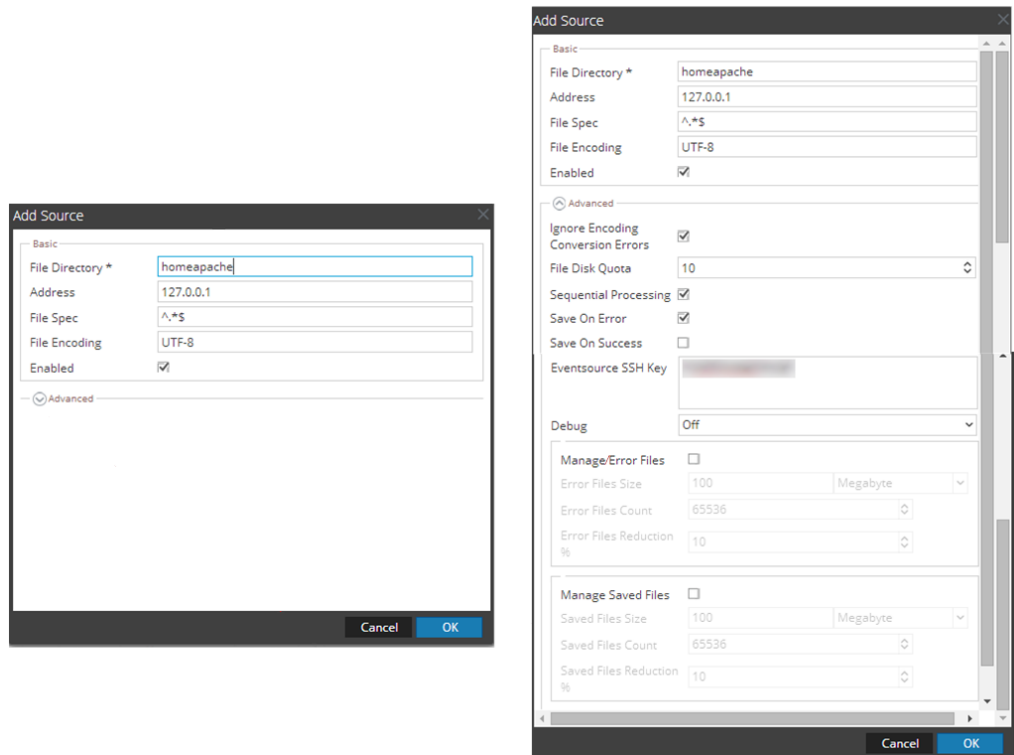
**Note:** The image below uses **Apache** as an example only. Your screen will look different, depending on which Event Source type you are configuring.



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.

Copyright © 2020 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](http://www.emc.com/legal/emc-corporation-trademarks.htm#rsa).