

RSA NetWitness Platform

Event Source Log Configuration Guide



Microsoft SharePoint Server

Last Modified: Thursday, October 31, 2019

Event Source Product Information:

Vendor: [Microsoft](#)

Event Source: SharePoint Server

Versions: 2007, 2010 and 2013

Additional Downloads: LOGbinder SP (for SharePoint 2007); LOGbinder SP 2.0 (for SharePoint 2010); LOGbinder SP 3.1 (for SharePoint 2010); LOGbinder SP4.0 (for SharePoint 2013)

RSA Product Information:

Supported On: NetWitness Platform 10.0 and later

Event Source Log Parser: mssharepoint

Collection Method: Windows Eventing

Event Source Class.Subclass: Storage.Storage

Configure Microsoft SharePoint Server

To configure Microsoft SharePoint Server to work with RSA NetWitness Platform, you must complete these tasks:

- I. Configure LOGbinder SP
- II. Configure Microsoft SharePoint Server using Windows Collection

Configure LOGbinder SP

Note: To collect auditing events from Microsoft SharePoint Server into the Windows Event Viewer, you must download the third-party application LOGbinder SP from <http://www.logbinder.com>.

To configure LOGbinder SP:

1. Depending on your version of Microsoft SharePoint, download one of the following files from <http://www.logbinder.com>:
 - For Microsoft SharePoint 2007, download LOGbinder SP
 - For Microsoft SharePoint 2010, download LOGbinder SP 2.0 or LOGbinder SP 3.1.
 - For Microsoft SharePoint 2013, download LOGbinder SP 4.0.
2. To configure the input settings, follow these steps:
 - a. In the LOGbinder SP interface, click **Input**.
 - b. Double-click the site collector that you want to audit.
 - c. From the Site Collector window, select the type of event to audit.
 - d. Click **OK**.
3. To configure the output settings, follow these steps:
 - a. Click **Output**.
 - b. If you are using LOGbinder SP or LOGbinder SP 2.0, double-click **Windows Event Logs**. If you are using LOGbinder SP 3.1 or 4.0, click **LOGbinder SP Event Log**.
 - c. If you are using LOGbinder SP or LOGbinder SP 2.0, ensure that **Send Output to Windows Event Log** is selected. If you are using LOGbinder SP 3.1 or 4.0, ensure

that **Send output to LOGbinder SP Event Log** is selected.

d. Click **OK**.

4. To start the service, click **Service > Start**.

Configure Microsoft SharePoint Server using Windows Collection

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 need to specify the channel from which you wish to collect. Make sure to enter **LOGbndSP** for the channel value.

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.