

RSA NetWitness Logs

Event Source Log Configuration Guide



Microdasys XML Security Gateway

Last Modified: Monday, May 22, 2017

Event Source Product Information:

Vendor: Microdasys

Event Source: XML Security Gateway

Versions: 1.1.0

Additional Downloads: sftpageant.conf.microdasys_xsg

RSA Product Information:

Supported On: NetWitness Suite 10.0 and later

Event Source Log Parser: microdasys_xsg

Collection Method: File

Event Source Class.Subclass: Security.Application Firewall

To configure Microdasys XML Security Gateway, complete the following tasks:

- I. Configure Microdasys XML Security Gateway
- II. Set Up the SFTP Agent and Configure the NetWitness Log Collector

Configure Microdasys XML Security Gateway

To configure Microdasys XML Security Gateway:

1. Log on to Microdasys XML Security Gateway with administrator credentials.
2. Click **Config > Logging**.
3. Ensure that **Edit all servers** is selected.
4. Ensure that the default log location is selected.

Note: If your default log location is different than **C:/Program Files (x86)/Microdasys/XSG/log/**, update the path in the **sftpagent.conf.microdasys_xsg** file to match the path displayed in the XML Security Gateway console.

5. Ensure that **Access Log** is selected and that the corresponding **File: xsg_access.log** checkbox is selected.
6. Click **Apply**.

Configure File Collection for RSA NetWitness Suite

To complete the File collection configuration, perform these tasks:

- I. Set up SFTP Agent
- II. Configure the RSA NetWitness Suite Log Collector for File Collection

Set Up the SFTP Agent

To set up the SFTP Agent Collector, download the appropriate PDF from RSA 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 SA SFTP Agent shell script](#)

Configure the Log Collector for File Collection

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

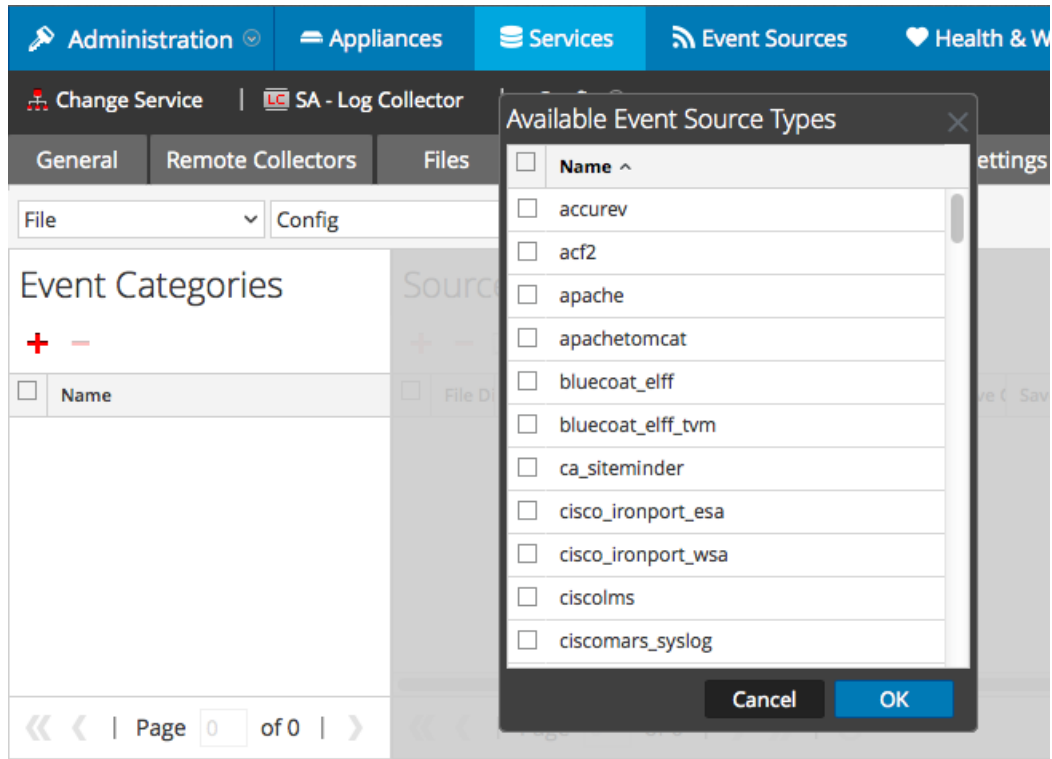
To configure the Log Collector for file collection:

1. In the **NetWitness** menu, select **Administration > 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 **+**.

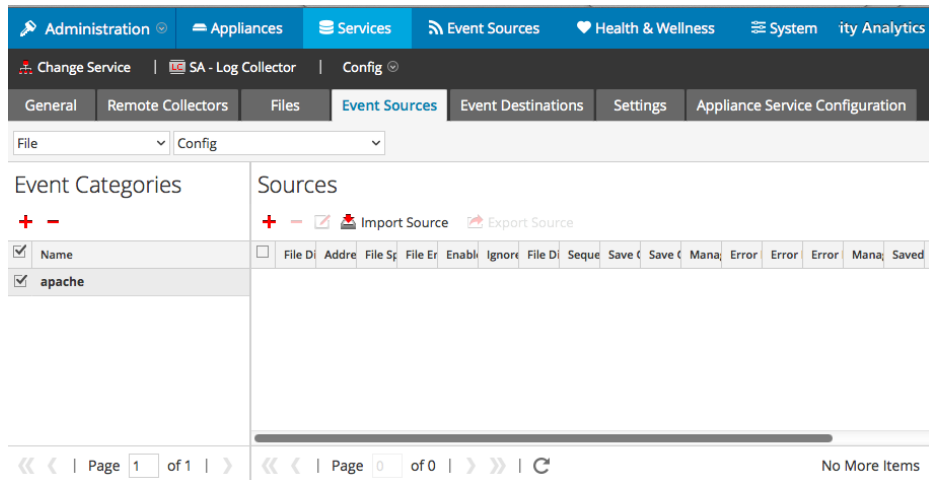
The Available Event Source Types dialog is displayed.



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

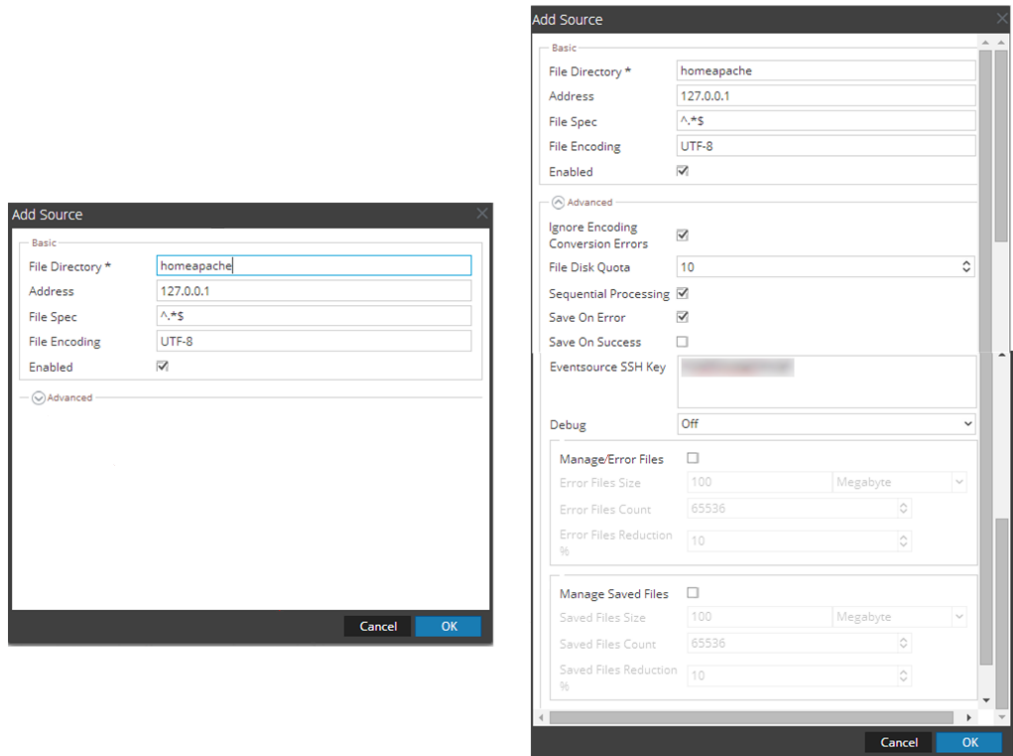
Select **microdasys_xsg** from the **Available Event Source Types** dialog.

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



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

The Add Source dialog is displayed.



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 © 2017 EMC Corporation. All Rights Reserved.

Trademarks

RSA, the RSA Logo and EMC are either registered trademarks or trademarks of EMC Corporation in the United States and/or other countries. All other trademarks used herein are the property of their respective owners.