RSA NetWitness Logs

Event Source Log Configuration Guide

McAfee Endpoint Encryption

Last Modified: Friday, June 02, 2017

Event Source Product Information:

Vendor: McAfee
Event Source: Endpoint Encryption
Versions: 5.2.2 and 5.2.12
Additional Downloads: sftpagent.conf.mcafeeendpoint

RSA Product Information:

Supported On: NetWitness Suite 10.0 and later
Event Source Log Parser: mcafeeendpoint
Collection Method: File
Event Source Class.Subclass: Security.Access Control

Configure McAfee Endpoint Encryption

To configure McAfee Endpoint Encryption, you must complete these tasks:

I. Configure McAfee Endpoint Encryption

II. Set Up Windows Task Scheduler on Windows

III. Set Up the SFTP Agent

IV. Configure the RSA NetWitness Suite Log Collector for File Collection

Configure McAfee Endpoint Encryption

Warning: You must configure McAfee Endpoint Encryption Server at least 24 hours before proceeding on to the next tasks.

To configure McAfee Endpoint Encryption Server:

1. Set Up McAfee Endpoint Encryption according to vendor instructions.
2. In the McAfee Endpoint Encryption Server, create a folder named **MyScripts** on the C: drive.
3. Download the **main.bat** batch file and the **BatchLauncher.vbs** and **tologs.vbs** VBScript files from SecurCare Online, and paste them into the **MyScripts** folder.

   Note: These files are located below the McAfee Endpoint Encryption configuration document in the RSA NetWitness Suite Device Configuration page of SecurCare Online.
4. In the **tologs.vbs** file, edit the location of Endpoint Encryption Manager as follows:
   a. Open the **tologs.vbs** file.
   b. Replace **C:/Program Files/McAfee/Endpoint Encryption Manager/** with the location of the Endpoint Encryption Manager on your machine.
   c. Click **File** > **Save**.
5. In the **main.bat** file, edit the location of Endpoint Encryption Manager as follows:
   a. Open the **main.bat** file.
   b. Replace the following command with the administrator credentials:

      ```
      SbAdmCl.exe -adminuser:<EndpointEncryptionManager Administrator> -adminpwd:<EndpointEncryptionManager Password> -command:DumpUserAudit -group:"*" -File:1.txt -clear
      ```

      where:

      - *<EndpointEncryptionManager Administrator>* is the administrator's user name.
      - *<EndpointEncryptionManager Password>* is the administrator's password.

c. Replace **C:/Program Files/McAfee Endpoint Encryption Manager/** with the location of the Endpoint Encryption Manager on your machine.

d. Click **File** > **Save**.

6. In the Endpoint Encryption Manager folder, create two new folders with the following names:
   - logs
   - logerrors
7. Run the **main.bat** file twenty-four hours before setting up the Windows Tasks Scheduler.

Set Up Windows Task Scheduler on Windows

Warning: You must run the **main.bat** file twenty-four hours before proceeding to the following steps.

To set up Windows Task Scheduler on Windows:

Note: In the following procedure, create only one scheduled task. To set up Task Scheduler on other Windows operating systems, refer to Microsoft documentation.

1. On the McAfee Endpoint Encryption server, click **Start** > **Settings** > **Control Panel**.
2. Click **Scheduled Task** > **Add Scheduled Task**.
3. In the Scheduled Task Wizard, click **Next**.
4. Select any application from the list, and click **Next**.
5. In the **Type a name for this task** field, type **Endpoint**.
6. Under **Perform this task** field, select **Daily**, and click **Next**.
7. Select the start time and start date, and click **Next**.
8. In the username and password fields, enter the server logon credentials, and click **Next**.
9. Select **Open advanced properties for this task when I click Finish**, and click **Finish**.
10. On the **Task** tab of the advanced properties window, in the **Run** field, type **C:\WINDOWS\system32\wscript.exe "C:\MyScripts\BatchLauncher.vbs" "C:\MyScripts\main.bat"**
11. On the **Schedule** tab, click **Advanced**.
12. Select **Repeat task**, and complete the fields as follows.

Field	Action
Every	Select how frequently you want RSA NetWitness Suite to receive logs from Endpoint.
Until	Select **Duration**.

Field	Action
Hour(s)	Type **24**.

13. Click **Apply**.

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

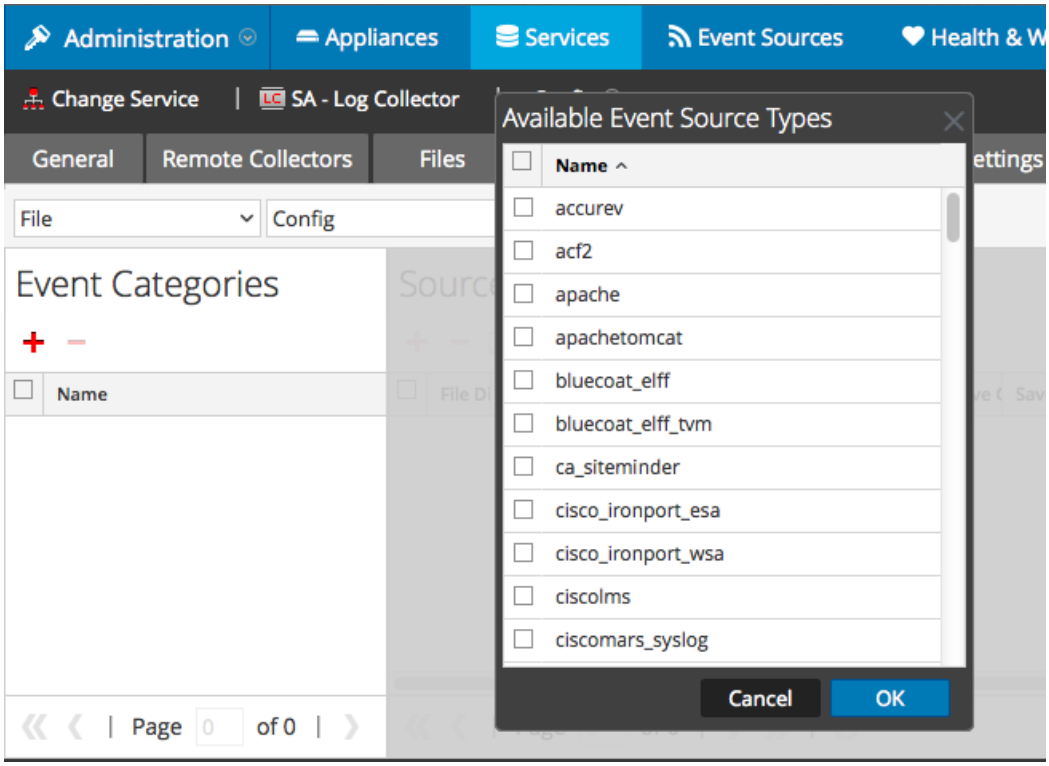
Perform the following steps to configure the Log Collector for File collection.

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 +.

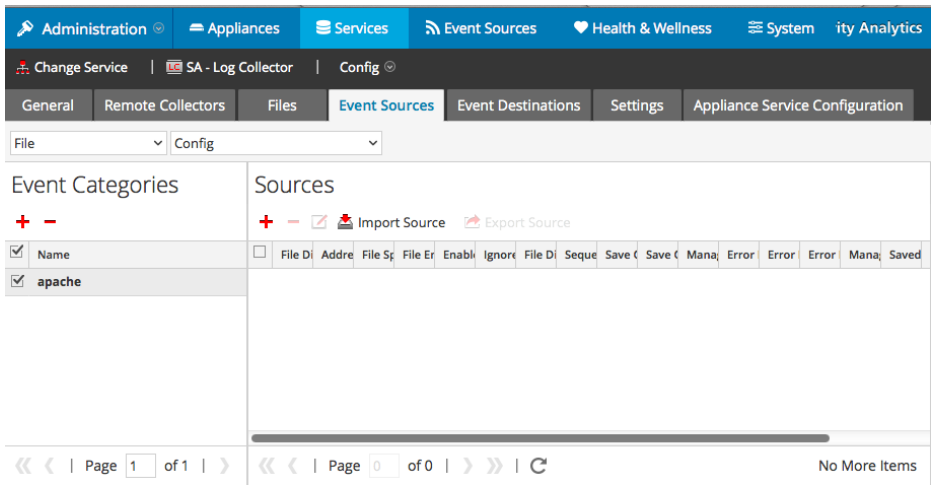
   The Available Event Source Types dialog is displayed.



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

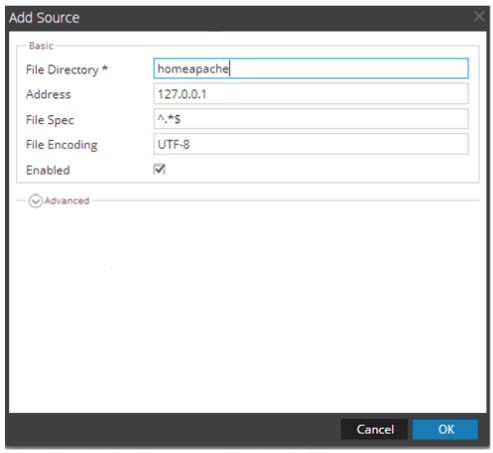
   Select **McAfeeEndpoint** from the **Available Event Source Types** dialog.

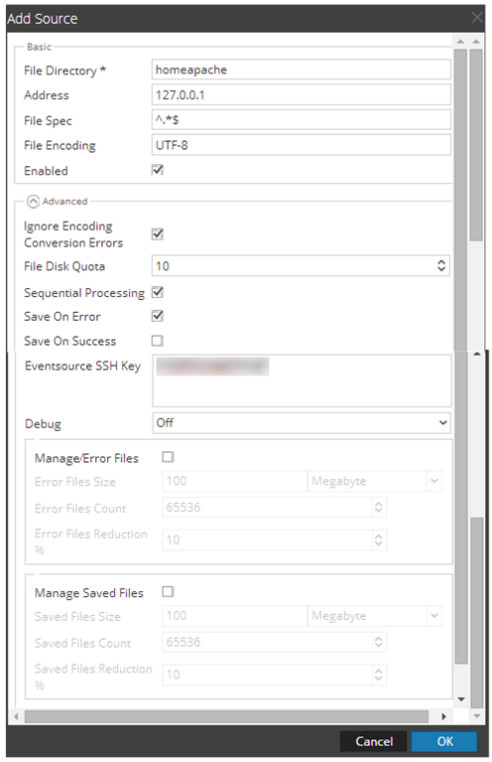
   The newly added event source type is displayed in the Event Categories panel.



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.

Trademarks