RSA NetWitness Logs

Event Source Log Configuration Guide

BlackBerry Enterprise Server

Last Modified: Thursday, November 2, 2017

Event Source Product Information:

Vendors: Blackberry
Event Source: BlackBerry Enterprise Server
Versions: 5.x

Note: RSA is qualifying support for the major version. In case of any configuration changes or logs not parsing in a minor version, please open a case and we will add support for it.

Supported Platforms: Microsoft Exchange
Additional Downloads:

- sftpagent.conf.blackberryes
- blackberryes_logger.vbs
- BESlog.conf

RSA Product Information:

Supported On: NetWitness Suite 10.0 and later
Event Source Log Parser: blackberryes
Collection Method: File
Event Source Class.Subclass: Network.Messaging

To configure RIM BlackBerry Enterprise Server, you must complete these tasks:

I. Configure RIM BlackBerry Enterprise Server to generate logs

II. Set Up Windows Task Scheduler

III. Set Up the SFTP Agent

IV. Set up the File Service

Configure RIM BlackBerry Enterprise Server to Send Logs

Note: RSA currently collects logs from the following files: **PINLog.csv**, **PhoneCallLog.csv**, and **SMSLog.csv**.

To configure log collection in RIM BlackBerry Enterprise Server:

1. To set up RIM BlackBerry Enterprise Server to collect Phone Call, SMS, and PIN logs, follow these steps:
   a. Log on to the BlackBerry Administration Service console with your administrator credentials.
   b. Click **Policy** > **Manage IT Policies** > **Open a Policy** > **Edit IT Policy** > **PIM Synchronization**.
   c. Set the values in the following fields to **No**:
      - **Disable Phone Call Log Wireless Synchronization**
      - **Disable PIN Messages Wireless Synchronization**
      - **Disable SMS Messages Wireless Synchronization**
   d. Click **Save All**.
2. On the RIM BlackBerry Enterprise Server appliance, create a folder named **EnvisionScripts** on the C: drive.

   Note: The **EnvisionScripts** folder is case sensitive.
3. Download the following files from RSA Link (https://community.rsa.com/docs/DOC-58035), and paste them into the **C:\EnvisionScripts** folder:

- **blackberryes_logger.vbs**
- **BESlog.conf**

4. In the **BESlog.conf** file, specify the path where logs are created on your RIM BlackBerry Enterprise Server.

   The default path is **C:\Program Files\Research In Motion\BlackBerry Enterprise Server\Logs**.

Note: If you are using Windows Server 2008 R2, you **must** specify the path where the logs are created in the BESlog.conf file.

Warning: When the scripts run on your RIM BlackBerry Enterprise Server appliance, they create corresponding **.pos** files in the same directory as the log files. Do not delete the **.pos** files from this location.

Set Up Windows Task Scheduler

To set up Windows Task Scheduler, complete the following tasks depending on your environment:

- Set up Task Scheduler for Windows Server 2008 R2, or
- Set up Task Scheduler for Windows 2003

Set Up Windows Task Scheduler for Windows Server 2008 R2

To set up Windows Task Scheduler for Windows Server 2008 R2:

1. Log on to the RIM Blackberry Enterprise Server console.
2. Click **Start** > **Administrative Tools** > **Task Scheduler**.
3. From the **Task Scheduler Library**, click **Create Task**.
4. In the Create Task window, complete the following fields.
   - In the **General** tab, in the **Name** field, type **BESTask**.
   - In the **Security Options** section, RSA recommends using an administrator account when running the task.
   - Click **Run whether user is logged on or not**.
   - Click **Run with highest privileges**.
   - In the **Triggers** tab, click **New**.
   - From the New Trigger window, in the **Begin the task** field, select **On a schedule**.
   - In the **Settings** field, select **Daily**, and select the start date and start time. Ensure that the **Recur every** field displays **1 day**.
   - In the **Advanced Settings**, select **Repeat task every**.

     Note: RSA recommends every five minutes for a duration of one day.
   - Select **Enabled**.
   - Click **OK**.
   - From the **Actions** tab, click **New**.

- In the New Action window, in the **Action** field, select **Start a program**.
- In the **Settings** section, in the **Program/Script** field, type **C:\EnvisionScripts\blackberryes_logger.vbs**.
- In the **Start in** field, type **C:\EnvisionScripts**.
- Click **OK**.

5. Click **OK**.

Set Up Windows Task Scheduler for Windows 2003

Warning: In the following procedure, create only one scheduled task.

To schedule file conversion of RIM BlackBerry Enterprise Server logs:

1. On the RIM BlackBerry Enterprise Server host, to open the Scheduled Task Wizard, click **Start** > **Settings** > **Control Panel** > **Scheduled Tasks** > **Add Scheduled Task**.
2. To complete the Scheduled Task Wizard, follow these steps:
   a. Click **Next**.
   b. From the list, select **Command Prompt**, and click **Next**.
   c. In the task name field, type **BESTask**.
   d. Under **Perform this task**, select **Daily**, and click **Next**.
   e. Select the start time and start date, and click **Next**.
   f. Enter your server logon credentials, and click **Next**.
   g. Select **Open advanced properties for this task when I click finish**, and click **Finish**.
3. In the Advanced Properties dialog box, on the **Task** tab, follow these steps:
   a. In the **Run** field, type **C:\EnvisionScripts\blackberryes_logger.vbs**.
   b. In the **Start in** field, type **C:\EnvisionScripts**.
   c. Select **Enabled (scheduled task runs at specified time)**.
4. Click the **Schedule** tab, and click **Advanced**.
5. Select **Repeat task**, and complete the fields as follows.

Field	Action
Every	Select how frequently you want RSA NetWitness Suite to receive logs from RIM BlackBerry Enterprise Server. **Note:** RSA recommends that you schedule this task to run every five minutes.
Until	Select **Duration**. In the **Hours** field, type **24**.

6. Click **OK**.
7. Click **Apply**.
8. Click **OK**.

Set Up the SFTP Agent

To set up the SFTP agent on your Windows server:

1. Download **sftpagent.conf.blackberryes** from RSA Link (https://community.rsa.com/docs/DOC-58035).
2. To configure that file, see Install and Update SFTP Agent.

Configure the RSA NetWitness Log Collector

Configure the Log Collector for File Collection

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

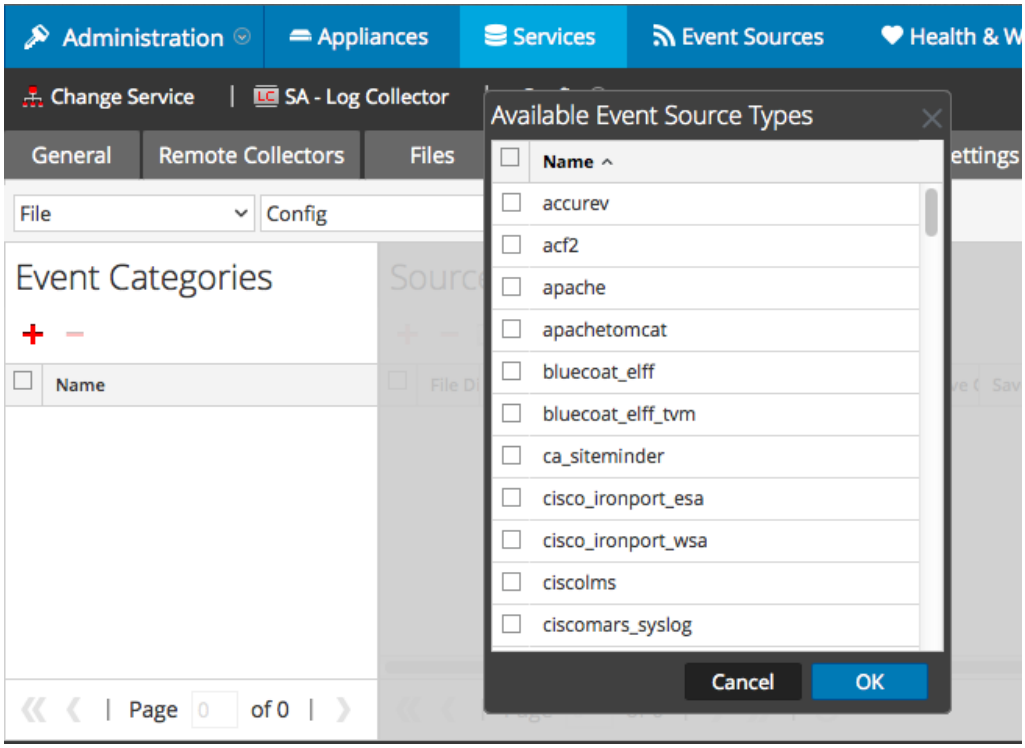
To configure the Log Collector for file collection:

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.

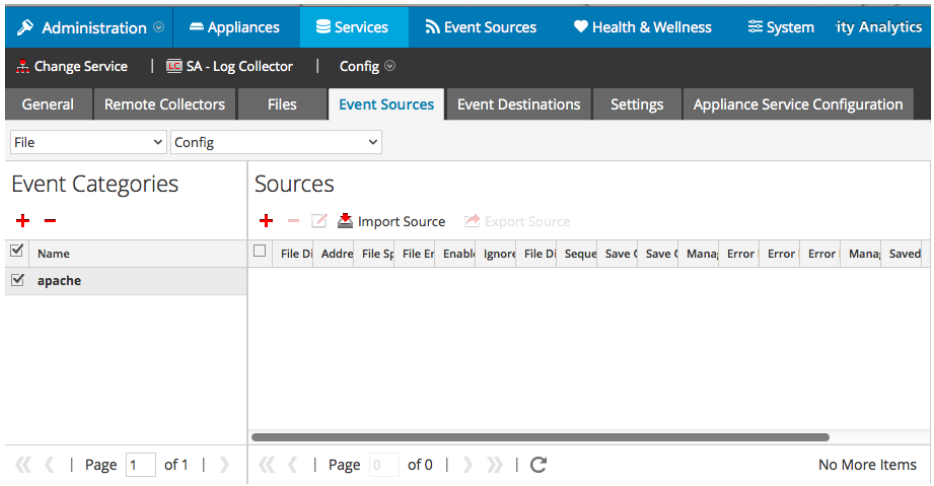


5. Select the correct type from the list, and click **OK**.

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

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

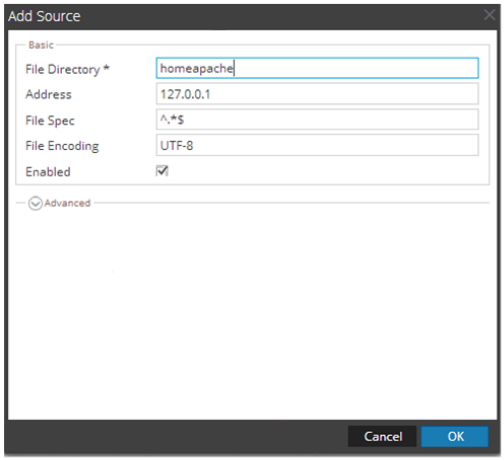
   Note: The image below uses **Apache** as an example only. Your screen will look different, depending on which Event Source type you are configuring.

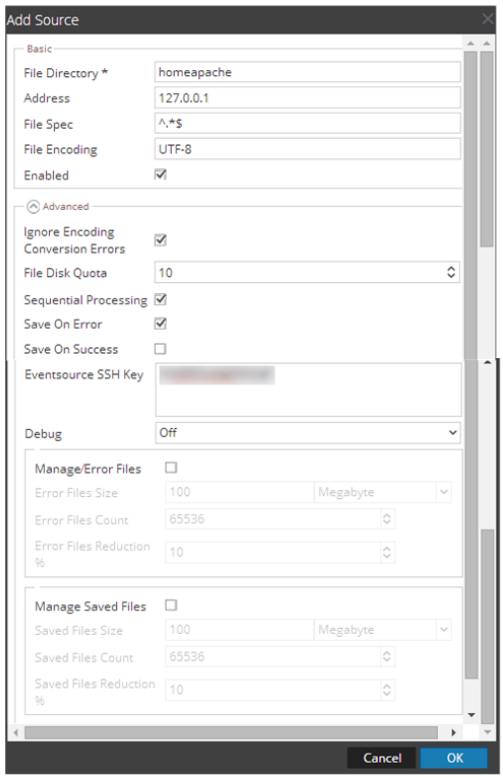


6. Select the new type in the Event Categories panel and click + in the Sources panel toolbar.

   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.

Trademarks