

# RSA NetWitness Logs

## Event Source Log Configuration Guide



## RSA Access Manager

Last Modified: Friday, April 14, 2017

### Event Source Product Information:

**Vendor:** [RSA, The Security Division of EMC](#)

**Event Source:** Access Manager

**Versions:** 6.0, 6.2

### Additional Downloads:

- For Syslog collection: `aserver_logj4.conf`, `eserver_logj4.conf`, `dispatcher_logj4.conf`
- For File collection: `nicstftpage1.conf.rsaaccessmanager`, `nicstftpage2.conf.rsaaccessmanager`, `sftpage.conf.rsaaccessmanager`

### RSA Product Information:

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

**Event Source Log Parser:** `rsaaccessmgr`

**Collection Method:** File, Syslog

**Event Source Class.Subclass:** `Security.Access Control`

# Configure RSA Access Manager

---

To configure collection for the RSA Access Manager you can use either [Syslog](#) or [File](#) collection protocols.

## Syslog Collection

---

To configure Syslog collection for the RSA Access Manager you must:



- Configure RSA NetWitness Suite for Syslog Collection
- Configure Syslog Output on RSA Access Manager

### Configure RSA NetWitness Suite for Syslog Collection

**Note:** You only need to configure Syslog collection the first time that you set up an event source that uses Syslog to send its output to NetWitness.

You should configure either the Log Decoder or the Remote Log Collector for Syslog. You do not need to configure both.

#### To configure the Log Decoder for Syslog collection:

1. In the **NetWitness** menu, select **Administration > Services**.
2. In the Services grid, select a Log Decoder, and from the Actions menu, choose **View > System**.
3. Depending on the icon you see, do one of the following:
  - If you see  **Start Capture**, click the icon to start capturing Syslog.
  - If you see  **Stop Capture**, you do not need to do anything; this Log Decoder is already capturing Syslog.

#### To configure the Remote Log Collector for Syslog collection:

1. In the **NetWitness** menu, select **Administration > Services**.
2. In the Services grid, select a Remote Log Collector, and from the Actions menu, choose **View > Config > Event Sources**.
3. Select **Syslog/Config** from the drop-down menu.

The Event Categories panel displays the Syslog 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 either **syslog-tcp** or **syslog-udp**. You can set up either or both, depending on the needs of your organization.
6. Select the new type in the Event Categories panel and click **+** in the Sources panel toolbar.

The Add Source dialog is displayed.

7. Enter **514** for the port, and select **Enabled**. Optionally, configure any of the Advanced parameters as necessary.

Click **OK** to accept your changes and close the dialog box.

Once you configure one or both syslog types, the Log Decoder or Remote Log Collector collects those types of messages from all available event sources. So, you can continue to add Syslog event sources to your system without needing to do any further configuration in NetWitness.

## Configure Syslog Output on RSA Access Manager

**Note:** Centralized logging is not necessary if you are using syslog with RSA Access Manager.

### To configure RSA Access Manager:

1. Go to the **/conf** directory open the **aserver.conf** file, and add the following line:

```
cleartrust.aserver.log4j.config.file=aserver_
log4j.conf
```

2. Go to the **/conf** directory, open the **eserver.conf** file, and add the following line:

```
cleartrust.eserver.log4j.config.file=eserver_
log4j.conf
```

3. Go to the **/conf** directory, open the **dispatcher.conf** file, and add the following line:

```
cleartrust.dispatcher.log4j.config.file=dispatcher_
log4j.conf
```

4. Open a browser and log on to SecurCare Online. Follow these steps to edit the **logj4.conf** files:

- a. Download the **aserver\_logj4.conf** file to the **/conf** directory, and edit the parameters as follow:

- `log4j.appender.A1.SyslogHost=applianceIP`  
where *applianceIP* is the IP address of your RSA NetWitness Suite Log Collector.
  - `log4j.appender.file.File=logfilepath`  
where *logfilepath* is the path of the file where you archive all the logs.
  - `log4j.appender.A1.layout.ConversionPattern=%RSAAXM-4-  
ServerInstanceName: %m%n`  
where *ServerInstanceName* is the instance name of the server.
- b. Download the **eserver\_logj4.conf** file to the **/conf** directory, and edit the parameters as follow:
- `log4j.appender.A1.SyslogHost=applianceIP`  
where *applianceIP* is the IP address of your RSA NetWitness Suite Log Collector.
  - `log4j.appender.file.File=logfilepath`  
where *logfilepath* is the path of the file where you archive all the logs.
  - `log4j.appender.A1.layout.ConversionPattern=%RSAAXM-4-  
ServerInstanceName: %m%n`  
where *ServerInstanceName* is the instance name of the server.
- c. Download the **dispatcher\_logj4.conf** file to the **/conf** directory, and edit the parameters as follow:
- `log4j.appender.A1.SyslogHost=applianceIP`  
where *applianceIP* is the IP address of your RSA NetWitness Suite Log Collector.
  - `log4j.appender.file.File=logfilepath`  
where *logfilepath* is the path of the file where you archive all the logs.
  - `log4j.appender.A1.layout.ConversionPattern=%RSAAXM-4-  
ServerInstanceName: %m%n`  
where *ServerInstanceName* is the instance name of the server.
5. Save and close all the files that you modified.

## File Collection

---

To configure File collection for the RSA Access Manager you must:

- Set up the SFTP Agent
- Configure the RSA NetWitness Suite Log Collector for File Collection
- Configure RSA Access Manager for Centralized Logging

### 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.

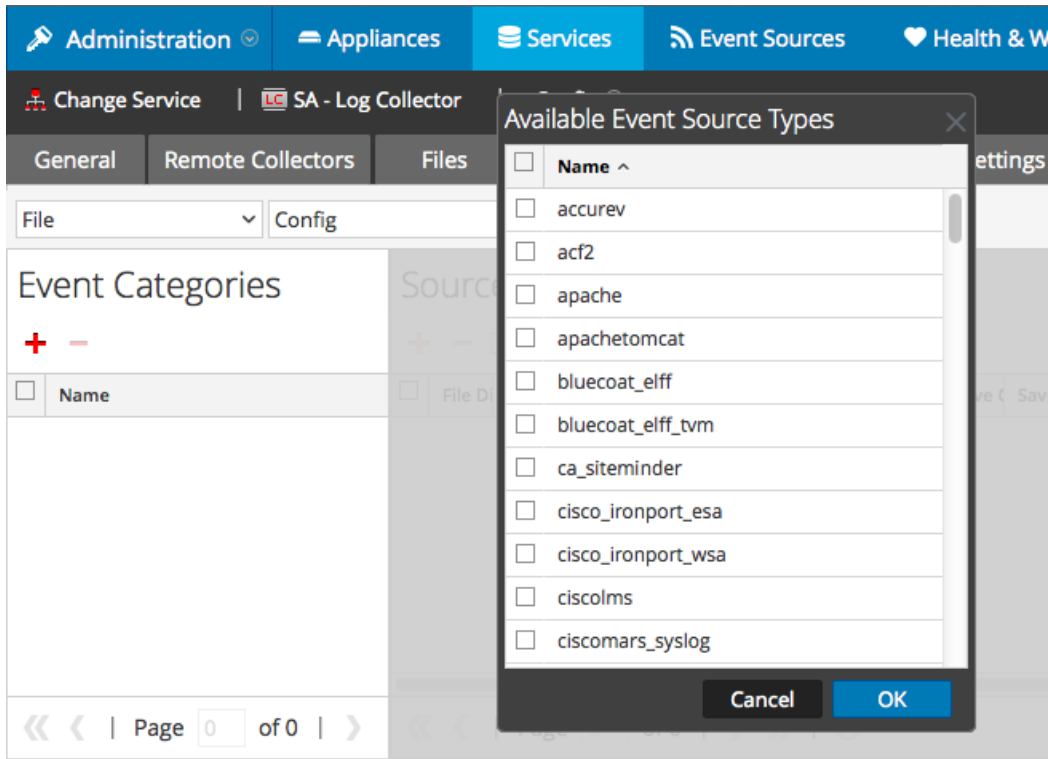
#### To configure the Log Collector for file collection:

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 **+**.

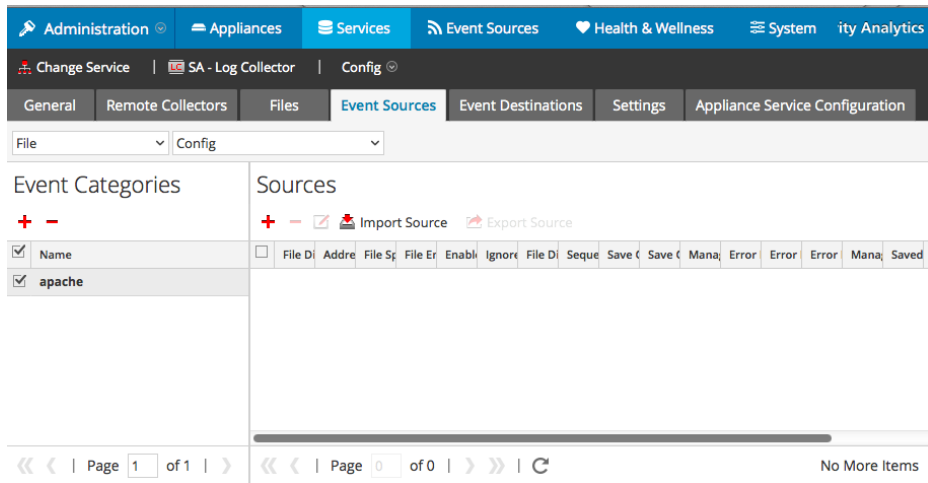
The Available Event Source Types dialog is displayed.



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

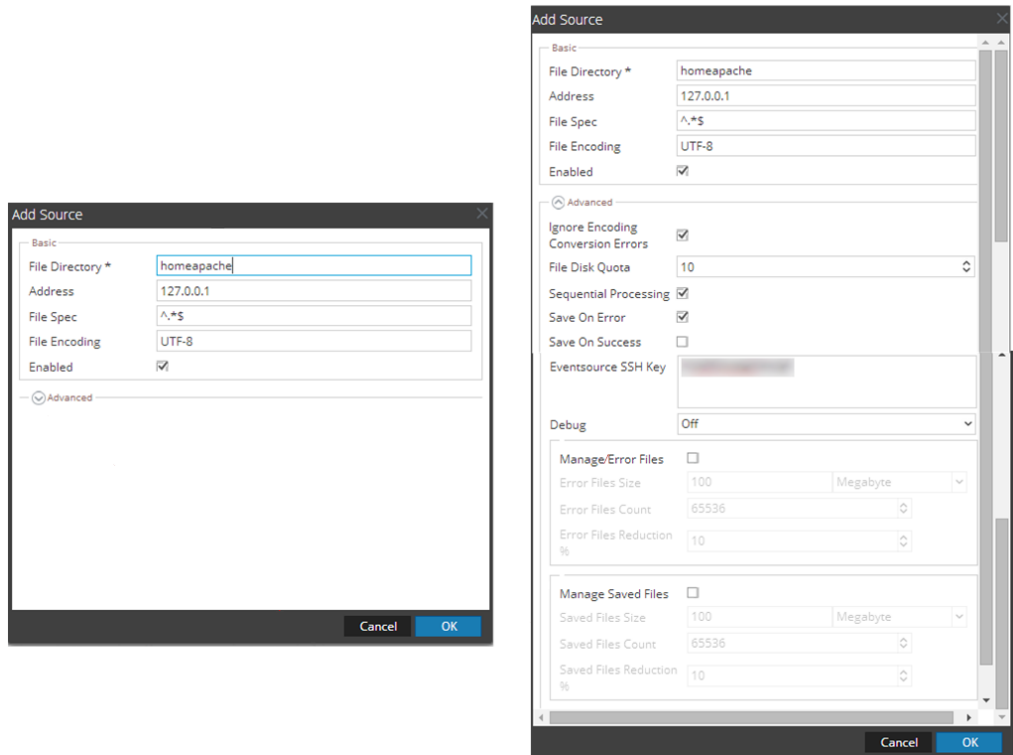
From the **Available Event Source Types** dialog, select **rsa\_access\_manager**.

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.

**Note:** Before proceeding, confirm that the RSA Access Manager Logging Server is installed and running.

## Configure RSA Access Manager for Centralized Logging

### To configure RSA Access Manager Log Server for centralized logging using File Reader:

1. Go to the *CT\_HOME/conf* directory on the host where your log server is installed and open the *lserver.conf* file. Accept the following default parameters or edit them



according to your system requirements.

- `cleartrust.lserver.log.listen_port=port`

where *port* is the port where the log server receives incoming messages from the servers. The default port is **5610**.

**Important:** Make sure that this value matches the **log.server\_port** parameter of each RSA Access Manager Server configuration file.

- `cleartrust.lserver.log=logfilename`

where *logfilename* is the name of the log file where the log server writes log messages. The default file name is **lserver.log**.

- `cleartrust.lserver.log.size=logsize`

where *logsize* is the maximum log size (in kilobytes) of the log server. The default value is **1000**.

- `cleartrust.lserver.log.backups=logbackups`

where *logbackups* is the number of log file backups to save. The default value is **10**.

- `cleartrust.lserver.log.backlog_size=backlogsize`

where *backlogsize* is the size of the backlog of incoming log messages. The default value is **1000**.

- `cleartrust.lserver.log.backlog_restart_size=restartsize`

where *restartsize* is the restart size for the Log Server to restart receiving requests. The default value is **500**.

2. Go to the **/conf** directory on the host where your Authorization Server is installed and open the **aserver.conf** file. Accept the following default parameters or edit them according to your system requirements.

- `cleartrust.aserver.log.level=loglevel`

where *loglevel* is the logging level of the Authorization server. The default level is **30**

- `log.server_host=hostname`

where *hostname* is the hostname of the Log Server. The default hostname is **localhost**.

- `log.server_port=port`

where *port* is the port where the log server receives incoming messages from the different servers. The default port is **5610**.

- `log.server_reconnect_delay=time`

where *time* is the number of milliseconds that the Authorization Server waits before attempting to reestablish the connection to the Log Server after the connection is lost. The default value is **3000**.

- `log.backlog_size=backlogsize`  
where *backlogsize* is the backlog size of the incoming log messages. The default value is **1000**.
- `log.restart_size=restartsize`  
where *restartsize* is the restart size for the Log Server to restart receiving requests. The default value is **1000**.
- `log.client_id=clientID`  
where *clientID* is the ID of the Authorization Server.

**Note:** By default, if you do not specify a value, the client ID is the IP address of the Authorization Server host. When several different Access Manager Servers send log messages to the Log Server, this parameter provides the client ID at the beginning of the log message to identify the origin of each message.

3. Go to the `/conf` directory on the host where your Entitlement Server is installed and open the `eserver.conf` file. Accept the following default parameters or edit them according to your system requirements.
  - `cleartrust.eserver.log.level=loglevel`  
where *loglevel* is the logging level of the Entitlement Server. The default level is **30**.
  - `log.server_host=hostname`  
where *hostname* is the hostname of the Log Server. The default hostname is **localhost**.
  - `log.server_port=port`  
where *port* is the port where the log server receives incoming messages from the servers. The default port is **5610**.
  - `log.server_reconnect_delay=time`  
where *time* is the number of milliseconds that the Entitlement Server waits before attempting to reestablish the connection to the Log Server after the connection is lost. The default value is **3000**.
  - `log.backlog_size=backlogsize`  
where *backlogsize* is the backlog size of the incoming log messages. The default value is **1000**.

- `log.restart_size=restartsize`  
where *restartsize* is the restart size for the Log Server to restart receiving requests. The default value is **1000**.
- `log.client_id=clientD`  
where *clientID* is the ID of the Entitlement Server.

**Note:** By default, if you do not specify a value, the client ID is the IP address of the Entitlement Server host. When several different Access Manager Servers send log messages to the Log Server, this parameter provides the client ID at the beginning of the log message to identify the origin of each message.

4. Go to the `/conf` directory on the host where your Dispatcher is installed and open the **dispatcher.conf** file. Accept the following default parameters or edit them according to your system requirements.
  - `cleartrust.eserver.log.level=loglevel`  
where *loglevel* is the logging level of the Dispatcher server. The default level is **30**.
  - `log.server_host=hostname`  
where *hostname* is the hostname of the Log Server. The default hostname is **localhost**.
  - `log.server_port=port`  
where *port* is the port where the log server receives incoming messages from the servers. The default port is **5610**.
  - `log.server_reconnect_delay=time`  
where *time* is the number of milliseconds that the Authorization Server waits before attempting to reestablish the connection to the Log Server after the connection is lost. The default value is **3000**.
  - `log.backlog_size=backlogsize`  
where *backlogsize* is the backlog size of the incoming log messages. The default value is **1000**.
  - `log.restart_size=restartsize`  
where *restartsize* is the restart size for the Log Server to restart receiving requests. The default value is **1000**.
  - `log.client_id=clientID`  
where *clientID* is the ID of the Dispatcher Server.

**Note:** By default, if you do not specify a value, the client ID is the IP address of the Dispatcher. When several different Access Manager Servers send log messages to the Log Server, this parameter provides the client ID at the beginning of the log message to identify the origin of each message

5. Save and close all the files that you modified.

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.