RSA NetWitness Platform

Event Source Log Configuration Guide

IBM Tivoli Access Manager WebSEAL

Last Modified: Tuesday, August 20, 2019

Event Source Product Information:

Vendor: IBM
Event Source: Tivoli Access Manager WebSEAL
Version: 6.0, 7.x, 9.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.

Platform: Windows
Additional Downloads:

- ibmtamws-addheader.vbs
- ibmtamws-addheader.conf
- sftpagent.conf.ibmtamws

RSA Product Information:

Supported On: NetWitness Platform 10.0 and later
Event Source Log Parser: ibmtamws
Collection Method: File, Syslog (9.x)
Event Source Class.Subclass: Security.Access Control

To configure IBM Tivoli Access Manager WebSEAL to work with RSA NetWitness Platform, you must perform the following tasks:

I. Configure IBM TAM WebSEAL

II. Configure the IBM TAM WebSEAL Script

III. Set Up the Windows Task Scheduler

IV. Set Up the SFTP Agent

V. Configure the Log Collector for File Collection

For version 9.x, you can send HTTP events to the RSA NetWitness Platform using Syslog. For details, see Configure Syslog for Tivoli Access Manager 9.x.

Configure IBM TAM WebSEAL

To configure IBM TAM WebSEAL:

1. On the IBM TAM WebSEAL server, locate the **\Tivoli\PDWeb\etc** directory.
2. Open any WebSEAL server instance .conf file, for example **webseald-default.conf** or **webseald-test.conf**.
3. Ensure that the following parameter values are set in the **aznapi-configuration** section of the WebSEAL server instance .conf file.

Parameter	Value
logaudit	yes
auditlog	*InputFolderLocation*/aznapi_*servername-instancename*.log where: • *InputFolderLocation* is the location of the input folder where you want to store the log files, for example, C:\Program Files\Tivoli\PDWeb\log You will need this location when you configure the IBM TAM WebSEAL script and when you set up the NIC SFTP agent. • *servername* is the name of the IBM TAM WebSEAL server. • *instancename* is the instance of the server.
auditcfg	azn
auditcfg	authn

Parameter	Value
auditcfg	http
logsize	Default size (in bytes) or **5000000**

4. Ensure that the following parameter values are set in the **logging** section of the WebSEAL server instance .conf file.

Parameter	Value
max-size	Default size (in bytes) or **2000000**
requests	yes
requests-file	The location where you want to store the request log file, for example, `C:\Tivoli\PDWeb\www-default\logs\request.log` **Note:** You will need this location when you set up the SFTP agent.
gmt-time	no
absolute-uri-in-request-log	yes
host-header-in-request-log	no

5. Repeat steps 3 and 4 for each of the WebSEAL server instance .conf files.

6. Restart the Access Manager services for the changes to take effect.

Configure the IBM TAM WebSEAL Script

To configure the IBM TAM WebSEAL script:

1. On the IBM TAM WebSEAL server, create an **NetWitnessScripts** folder on the C: drive.

2. Download the **ibmtamws-addheader.vbs** script file and the **ibmtamws-addheader.conf** file, and paste the files into the **NetWitnessScripts** folder. These files are available on the RSA Link Additional Downloads space here: https://community.rsa.com/docs/DOC-53584

3. In any directory, create the output folder and the staging folder, which the IBM TAM WebSEAL script will use. For example, create `C:\Program Files\Tivoli\PDWeb\Custom_logs` and `C:\Program Files\Tivoli\PDWeb\Staging`. An input folder was created when you configured IBM TAM WebSEAL.

4. Edit the **ibmtamws-addheader.conf** file to specify the location of the input, output, and staging folders. Open the **ibmtamws-addheader.conf** file and set the following parameters:

   - Input_Folder=*InputFolderLocation*

     where *InputFolderLocation* is the location of the input folder where the logs are stored, for example, `C:\Program Files\Tivoli\PDWeb\log`.

   - Output_Folder=*OutputFolderLocation*

     where *OutputFolderLocation* is the location of the output folder to which the script writes logs, for example, C:\Program F`iles\Tivoli\PDWeb\Custom_logs`. This is also the location from which the SFTP agent gathers logs to send to RSA NetWitness Platform.

     Note: You will need this output folder location when you set up the SFTP Agent.

   - Staging_Folder=*StagingFolderLocation*

     where *StagingFolderLocation* is the location of the staging folder where the temporary files used by the script are stored, for example, `C:\Program Files\Tivoli\PDWeb\Staging`.

Warning: When the scripts run on your IBM TAM WebSEAL server, they create two text files, **Positionfile_(*Instance*).txt** and **sizeFile_(*Instance*).txt**, for each instance of the WebSEAL server. The files are stored in the staging folder and must not be deleted. You will need these files for the script to run, which collects logs from IBM TAM WebSEAL and stores it in the output folder location.

5. Save and close the file.

Set Up the Windows Task Scheduler

To set up the Windows Task Scheduler:

1. On the IBM TAM WebSEAL server, click **Start** > **Control Panel** > **Scheduled Task** > **Add Scheduled Task**.
2. In the Scheduled Task Wizard, click **Next**.
3. Select any application from the list, and click **Next**.
4. In the **Type a name for this task** field, type **IBMTAMWS_Audit**.
5. Under the **Perform this task** field, select **Daily**, and click **Next**.
6. Select the start time and start date, and click **Next**.
7. In the user name and password fields, enter the server logon credentials, and click **Next**.
8. Select **Open advanced properties for this task when I click Finish**, and click **Finish**.
9. On the **Task** tab of the advanced properties window, complete the fields as follows.

Field	Value
Run	C:\WINDOWS\system32\wscript.exe
Start	C:\NetWitnessScripts\ibmtamws-addheader.vbs.

10. On the **Schedule** tab, click **Advanced**.
11. Select **Repeat task**, and complete the fields as follows.

Field	Action
Every	Select **5 minutes** as the frequency of time RSA NetWitness Platform uses to collect logs from IBM TAM WebSEAL.
Until	Select **Duration**.
Hour (s)	Type **24**.

12. Click **OK**, and click **Apply**.

Set Up the SFTP Agent

On the GlobalSCAPE event source, configure the SFTP Agent.

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 SFTP Shell Script File Transfer

The steps to set up the SFTP agent are described in the previous links. Note the following details:

- Ensure that the **dir0** parameters are set as follows:

Parameter	Value
dir0	The path of the output folder you created when you configured the IBM TAM WebSEAL script, for example `C:\Program Files\Tivoli\PDWeb\Custom_logs`
dir0.filespec	*.xml
dir0.interval	The number of seconds to wait between file checks. The recommended value is **300**.
dir0.compression	false
dir0.enabled	true
dir0.delete_after_read	true
dir0.ftp	`server_ip,nic_sshd,public.txt,IBMTAMWS_IPAddress` where: • *server ip* is the IP address or hostname of your NetWitness Log Collector. • *IPAddress* is the IP address of the IBM TAM WebSEAL event source.

- Ensure that the **file*N*** parameters are set as follows, where *N* denotes each instance

Note: Repeat this step for the request log file of each IBM TAM WebSEAL server instance.

Field	Action
fileN	The location of the request log file, for example `C:\Program Files\Tivoli\PDWeb\www-test\log\request.log`
fileN.interval	The number of seconds to wait between file checks. The recommended value is **300**.
fileN.compression	false
fileN.enabled	true

Field	Action
fileN.ftp	*server_ip*,nic_sshd,public.txt,IBMTAMWSWEB_*IPAddress* where: - *server ip* is the IP address or hostname of your NetWitness Log Collector. - *IPAddress* is the IP address of the IBM TAM WebSEAL event source.
fileN.delete_after_read	false

Configure the Log Collector for File Collection

This section describes steps you need to perform on RSA NetWitness Platform.

Configure the Log Collector for File Collection

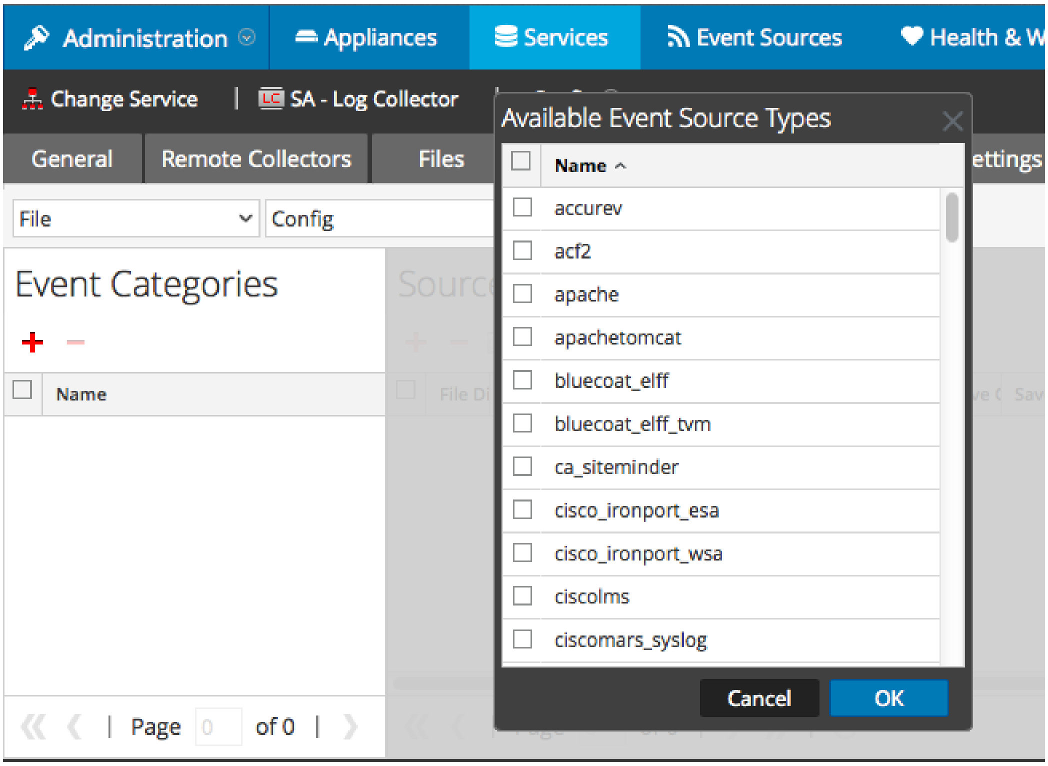
Perform the following steps to configure the Log Collector for File collection.

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.

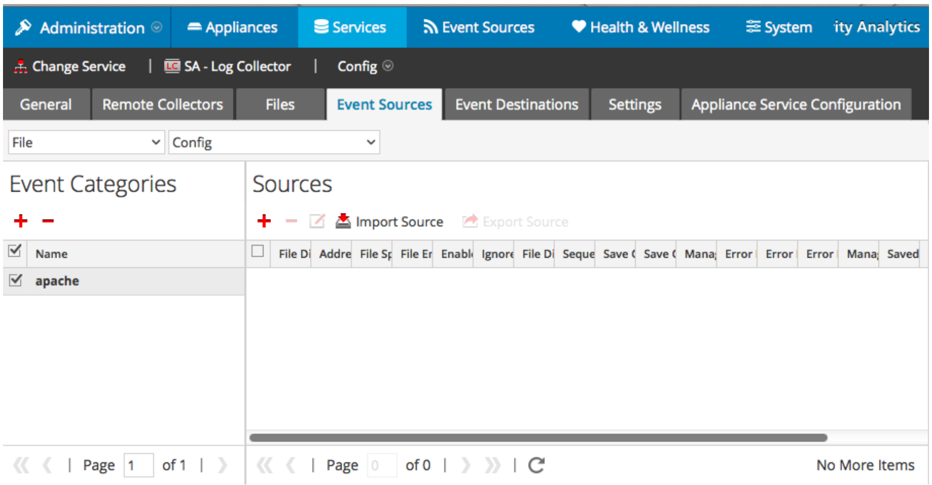


5. Select the correct type from the list, and click **OK**.

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

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

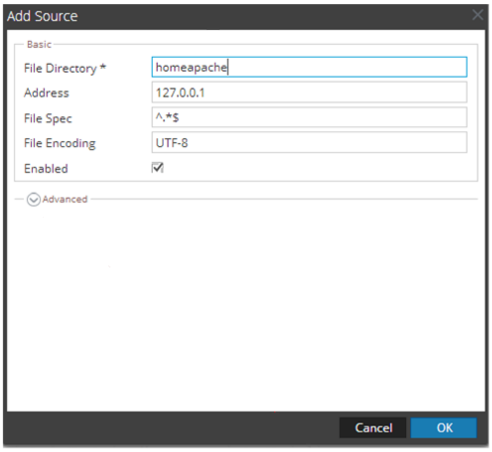
   Note: The image below uses **Apache** as an example only. Your screen will look different, depending on which Event Source type you are configuring.



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.



Basic

File Directory * homeapache

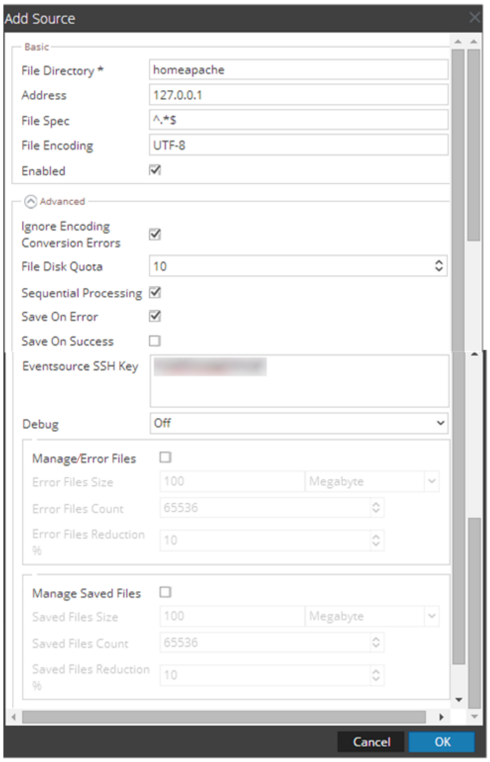
Address 127.0.0.1

File Spec ^.*$

File Encoding UTF-8

Enabled ☑

Advanced



Basic

File Directory * homeapache

Address 127.0.0.1

File Spec ^.*$

File Encoding UTF-8

Enabled ☑

Advanced

Ignore Encoding Conversion Errors ☑

File Disk Quota 10

Sequential Processing ☑

Save On Error ☑

Save On Success □

Eventsource SSH Key [redacted]

Debug Off

Manage/Error Files □

Error Files Size 100 Megabyte

Error Files Count 65536

Error Files Reduction % 10

Manage Saved Files □

Saved Files Size 100 Megabyte

Saved Files Count 65536

Saved Files Reduction % 10

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.

Configure Syslog for Tivoli Access Manager 9.x

To configure syslog for the event source, you first set up the event source, and then configure RSA NetWitness.

Configure Syslog Output on Tivoli Access Manager 9.x

For version 9.x, you can send HTTP events to the RSA NetWitness Platform using Syslog.

To configure Tivoli Access Manager:

1. Log onto Tivoli Access Manager's IBM Security Web Gateway.
2. From the navigation menu, select **Secure Reverse Proxy Settings** > **Manage** > **Reverse Proxy**.

   The Reverse Proxy pane is displayed.
3. From the **Instance** column, select an instance.
4. Click the **Manage** list and select **Configuration** > **Advanced**.

   The text of the WebSEAL configuration file is displayed.
5. Locate the Authorization API Logging configuration.

   The remote syslog configuration begins with `logcfg`.
6. Edit the remote syslog configuration as follows:

   ```
   logcfg = http:rsyslog server=IP_address,port=514,log_id=log_name
   ```

   where:

   - ***IP_address*** is the IP address of the RSA NetWitness Log Decoder or Remote Log Collector
   - ***Log_name*** is the name assigned to the log. For example, `log_id=WebSEAL-log`.
7. Customize the `request.log` file. For example:

   ```
   request-log-format = isam-http-request-log|client-ip=%a|
   server-ip=%A|client-logname=%l|remote-user=%u|time=%t|port=%p|
   protocol=%H|request-method=%m|response-status=%s|url=%U|
   bytes=%b|remote-host=%h|request=%r
   ```

   Where:

- ***client-ip*** is the Remote IP address
- ***server-ip*** is the Local IP address

8. Click **Submit**.
9. From the navigation menu, click **Deploy**.
10. From the **Instance** column, select your instance configuration.
11. Click the **Manage** list and select **Control > Restart**.

A status message is displayed after the restart completes.

> **Note:** RSA currently supports only HTTP events, in the request-log-format customized format described in the procedure.

Configure RSA NetWitness Platform

Perform the following steps in RSA NetWitness Platform:

- Ensure the required parser is enabled
- Configure Syslog Collection

Ensure the Required Parser is Enabled

If you do not see your parser in the list while performing this procedure, you need to download it in RSA NetWitness Platform Live.

Ensure that the parser for your event source is enabled:

1. In the **NetWitness** menu, select **ADMIN** > **Services**.
2. In the Services grid, select a Log Decoder, and from the Actions menu, choose **View** > **Config**.
3. In the Service Parsers Configuration panel, search for your event source, and ensure that the **Config Value** field for your event source is selected.

> **Note:** The required parser is **ibmtamws**.

Configure 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 **ADMIN** > **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 **ADMIN** > **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.

Trademarks

For a list of RSA trademarks, go to www.emc.com/legal/emc-corporation-trademarks.htm#rsa.