

RSA NetWitness Platform

Event Source Log Configuration Guide



IBM Tivoli Access Manager WebSEAL

Last Modified: Thursday, August 9, 2018

Event Source Product Information:

Vendor: [IBM](#)

Event Source: Tivoli Access Manager WebSEAL

Version: 6.0, 7.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

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](#)

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	<i>InputFolderLocation/aznapi_servername-instancename.log</i> where: <ul style="list-style-type: none">• <i>InputFolderLocation</i> is the location of the input folder where you want to store the log files, for example, <code>C:\Program Files\Tivoli\PDWeb\log</code> You will need this location when you configure the IBM TAM WebSEAL script and when you set up the NIC SFTP agent. <ul style="list-style-type: none">• <i>servername</i> is the name of the IBM TAM WebSEAL server.• <i>instancename</i> is the instance of the server.
auditcfg	azn
auditcfg	authn
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 Files\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 <code>C:\Program Files\Tivoli\PDWeb\Custom_logs</code>
dir0.filespec	<code>*.xml</code>
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	<p><code>server_ip,nic_sshd,public.txt,IBMTAMWS_IPAddress</code> where:</p> <ul style="list-style-type: none"> • <i>server ip</i> is the IP address or hostname of your NetWitness Log Collector. • <i>IPAddress</i> is the IP address of the IBM TAM WebSEAL event source.

- Ensure that the **fileN** 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 <code>C:\Program Files\Tivoli\PDWeb\www-test\log\request.log</code>
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	<i>server_ip,nic_sshd,public.txt,IBMTAMWSWEB_IPAddress</i> where: <ul style="list-style-type: none">• <i>server ip</i> is the IP address or hostname of your NetWitness Log Collector.• <i>IPAddress</i> 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.

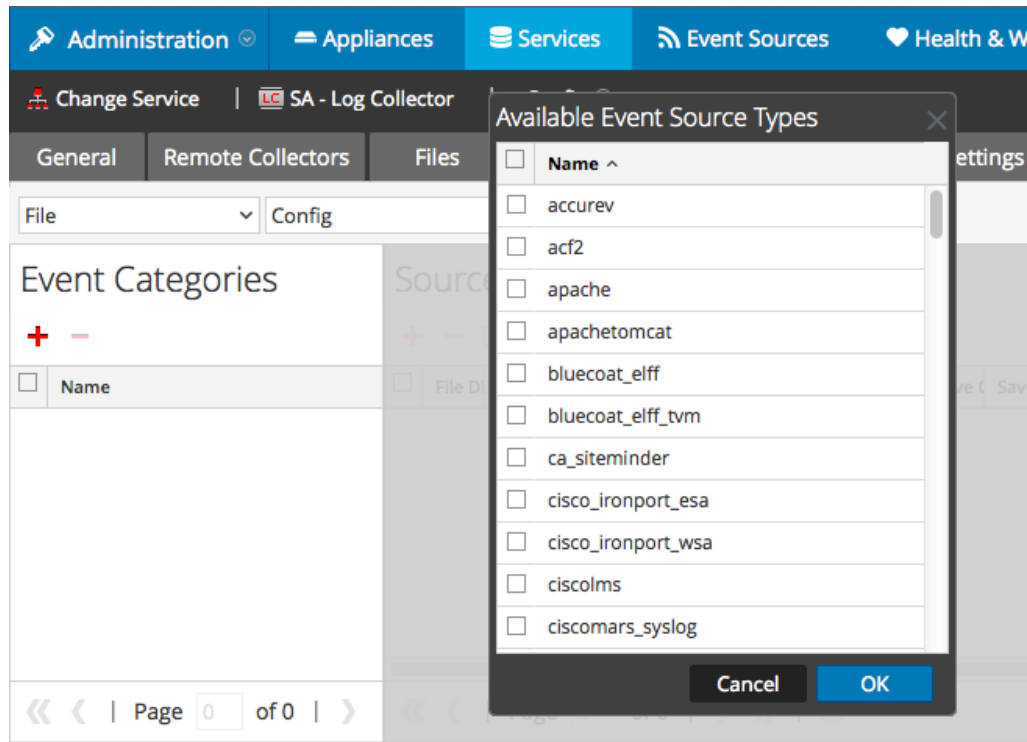
Configure the Log Collector for File Collection

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.

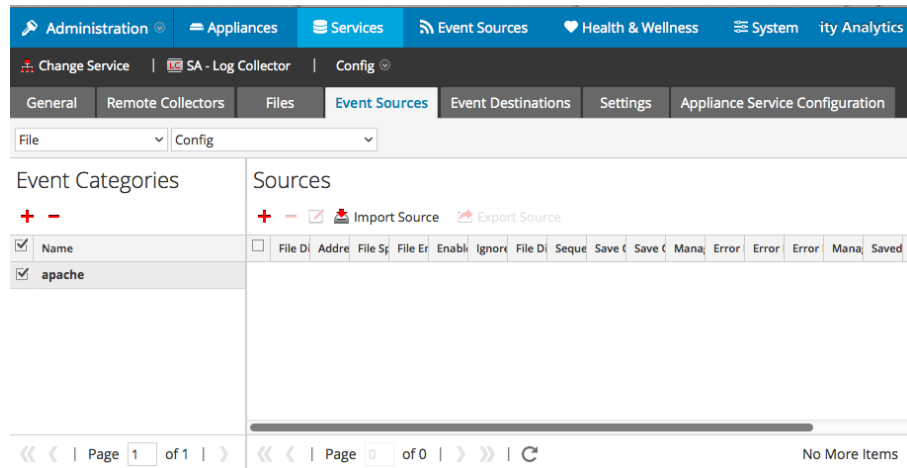


5. Select the correct type from the list, and click **OK**.

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

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

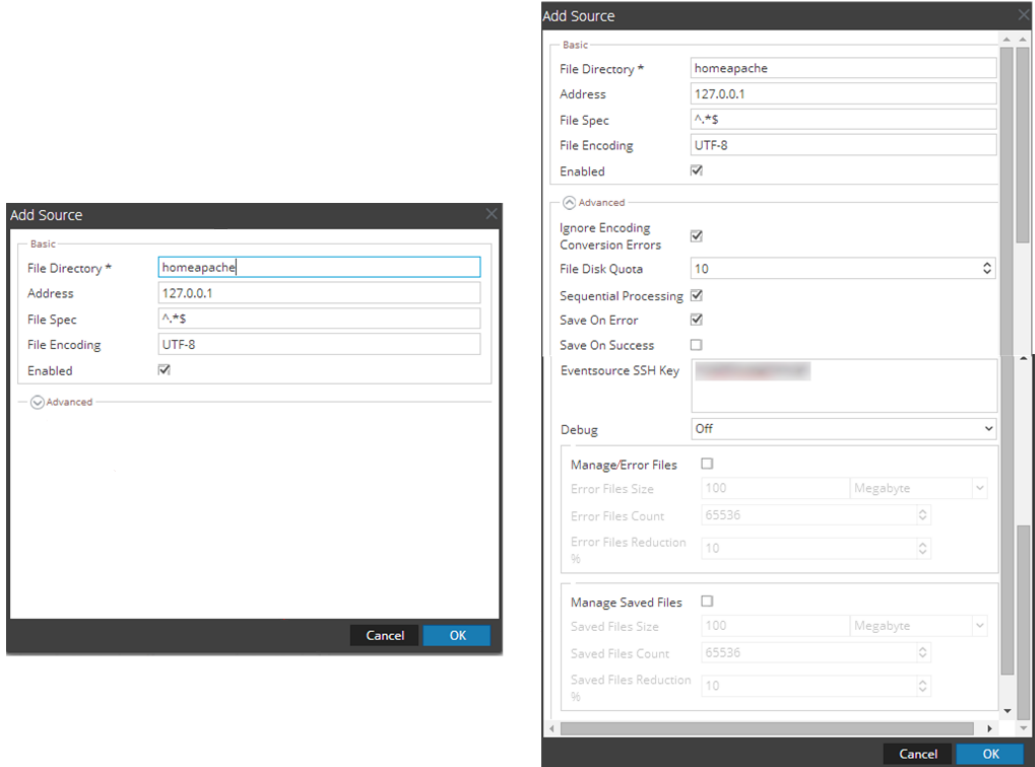
Note: The image below uses **Apache** as an example only. Your screen will look different, depending on which Event Source type you are configuring.



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.



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 © 2018 Dell Inc. or its subsidiaries. All Rights Reserved.

Trademarks

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