RSA NetWitness Logs

Event Source Log Configuration Guide

Microsoft Forefront Threat Management Gateway

Last Modified: Thursday, June 08, 2017

Event Source Product Information:

Vendor: Microsoft
Event Source: Forefront Threat Management Gateway
Versions: 2010
Additional Downloads:

- MS_Forefront_TMG_Scripts.sql
- sftpagent.conf.msisa
- sftpagent.conf.tmg

RSA Product Information:

Supported On: NetWitness Suite 10.0 and later
Event Source Log Parser: msisa
Collection Method: ODBC, File
Event Source Class.Subclass: Security.Firewall

You must complete these tasks to configure Microsoft Forefront TMG to work with RSA NetWitness Suite:

I. Configure the Microsoft Forefront TMG Event Source
    i. Set Up Logging to a Local Database.
    ii. Create the Database That Will Host the Stored Procedures.
    iii. Enable TCP Access to the Local Database on the Server.
II. In NetWitness Suite, configure File collection
III. In NetWitness Suite, configure ODBC Collection

Configure Microsoft Forefront TMG

Set Up Logging to a Local Database

To set up logging to a local database:

1. On the system where Forefront TMG is installed, click **Start** > **Programs** > **Microsoft Forefront TMG** > **Forefront TMG Management**.
2. In the Navigation pane, expand ***server_name***, where *server_name* is the name of the RSA NetWitness Suite Log Decoder or RSA NetWitness Suite Remote Log Collector, and click **Logs & Reports**.
3. In the right-hand pane, in the **Tasks** tab, ensure that the defaults are selected for Firewall and Web Proxy Logging:
   - Click **Configure Firewall Logging**, ensure that **SQL Server Express Database (on local server)** is selected, and click **OK**.
   - Click **Configure Web Proxy Logging**, ensure that **SQL Server Express Database (on local server)** is selected, and click **OK**.

Create the Database That Will Host the Stored Procedures

To create the database that will host the stored procedures:

1. Download **MS_Forefront_TMG_Scripts.sql** from RSA SecurCare online:
2. On the system where Forefront TMG is installed, open **Microsoft SQL Server 2008 Management Studio**.
3. Right-click **Databases**, and select **New**.
4. In the **Database Name** field, type **MS_Forefront_TMG**.
5. To create the database, click **OK**. Do not click **Add**.
6. Select **MS_Forefront_TMG** > **Programmability** > **Stored Procedures**.
7. Right-click **Stored Procedures**, and select **New Stored Procedure**.

8. Copy all contents from the **MS_Forefront_TMG_Scripts.sql** file to the new text file.
9. Click **Execute**.

Enable TCP Access to the Local Database on the Server

To enable TCP access to the local database on the server:

1. Log on to your Forefront TMG server using administrator credentials.
2. Click **Start** > **All Programs** > **Microsoft SQL Server 2008** > **Configuration Tools** > **SQL Server Configuration Manager**.
3. To enable MSFW protocols, follow these steps:
   a. Expand **SQL Server Network Configuration**, and select **Protocols for MSFW**.
   b. Right-click **TCP/IP**, and select **Enable**.
   c. On the Warning dialog box, click **OK**.
4. To set the port on which to listen for MSFW protocols, follow these steps:
   a. Expand **SQL Server Network Configuration**, and select **Protocols for MSFW**.
   b. Right-click **TCP/IP**, and select **Properties**.
   c. On the **IP Addresses** tab, in the **IPAll** section, change the TCP Port to **1433**, and ensure that nothing is entered in TCP Dynamic Ports (delete the **0** value if present).
   d. Click **OK**, and , in the Warning dialog box, click **OK**.
5. To enable ISARS protocols, follow these steps:
   a. Expand **SQL Server Network Configuration**, and select **Protocols for ISARS**.
   b. Right-click **TCP/IP**, and select **Enable**.
   c. In the Warning dialog box, click **OK**.
6. For ISARS protocols, set the port to listen on:
   a. Expand **SQL Server Network Configuration**, and select **Protocols for ISARS**.
   b. Right-click **TCP/IP**, and select **Properties**.
   c. On the **IP Addresses** tab, in the **IPAll** section, change the TCP Port to **1434**, and ensure that nothing is entered in TCP Dynamic Ports (delete the **0** value if present).
   d. Click **OK**, and, in the Warning dialog box, click **OK**.

7. To restart the MSFW and ISARS services, follow these steps:
   a. Click **Start** > **Administrative Tools** > **Services**.
   b. Right-click the **SQL Server (ISARS)** service, and select **Restart**.
   c. Right-click the **SQL Server (MSFW)** service, and select **Restart**.

Configure File Collection in NetWitness Suite

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

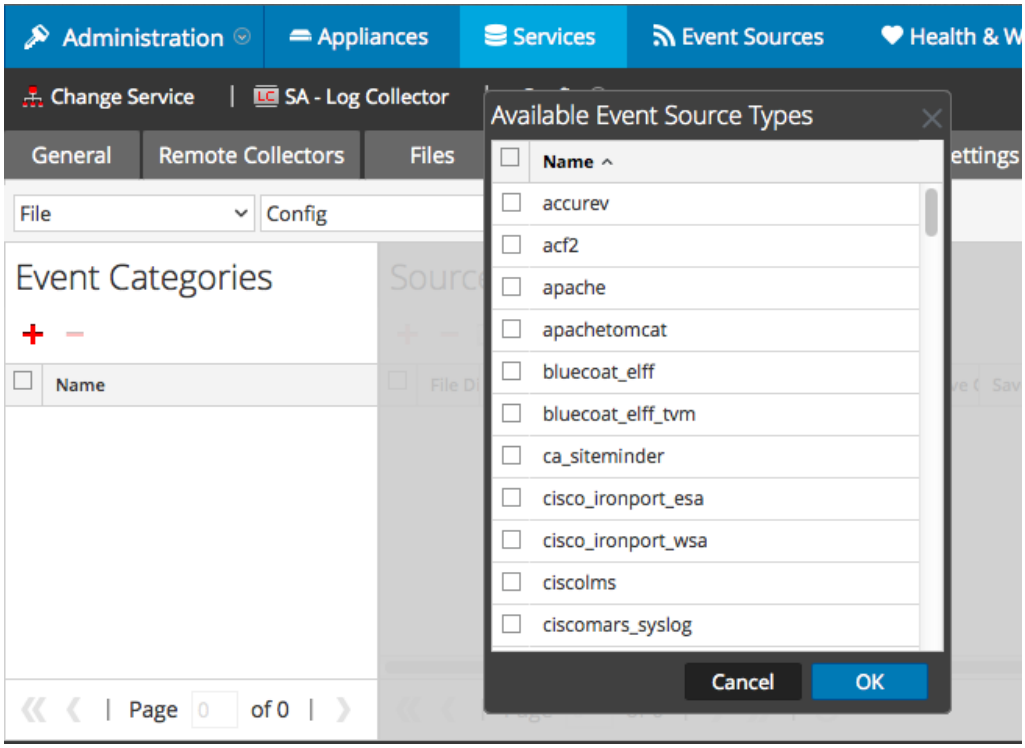
Perform the following steps to configure the Log Collector for File collection.

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 +.

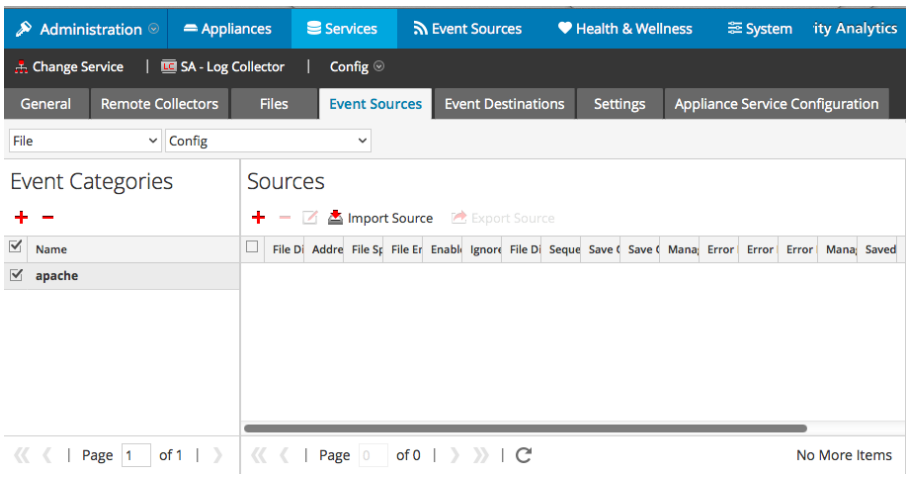
   The Available Event Source Types dialog is displayed.



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

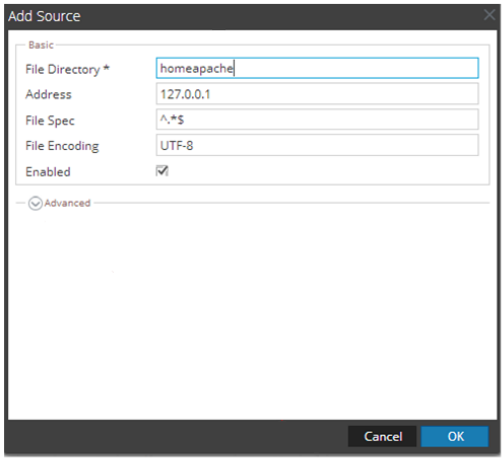
   From the **Available Event Source Types**, select **msftmg**.

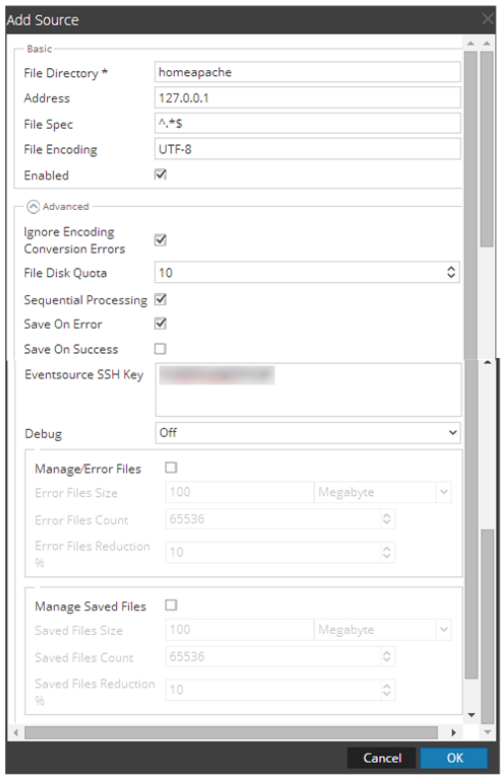
   The newly added event source type is displayed in the Event Categories panel.



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.

Configure ODBC Collection in NetWitness Suite

i. Ensure the Required Parser is enabled

ii. Configure DSNs

iii. Add the Event Source Type

iv. Restart the ODBC Collection Service

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 from RSA NetWitness Suite Live.

Ensure that the parser for your event source is enabled:

1. In the **NetWitness** menu, select **Administration** > **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 **msisa**.

Configure Two DSNs

For RSA NetWitness Suite, you need to configure two ODBC services, one for Firewall logging and a separate one for Web Proxy logging.

Configure a DSN (Data Source Name):

1. In the **NetWitness** menu, select **Administration** > **Services**.
2. In the **Services** grid, select a **Log Collector** service.
3. Click  under **Actions** and select **View** > **Config**.
4. In the Log Collector **Event Sources** tab, select **ODBC/DSNs** from the drop-down

menu.

5. The DSNs panel is displayed with the existing DSNs, if any.
6. Click + to open the **Add DSN** dialog.

   Note: If you need to add a DSN template, see Configure DSNs in the NetWitness User Guide.

7. Choose a DSN Template from the drop down menu and enter a name for the DSN. (You use the name when you set up the ODBC event source type.)
8. Fill in the parameters and click **Save**.

   ```
   Database=<Specify the database used by MS Forefront TMG>
   PortNumber=<Specify the Port Number, default is 1433>
   HostName=<Specify the hostname or IP Address of your
   TMG server>
   Driver=/opt/netwitness/odbc/lib/R3sqls26.so
   ```

   Note: The Driver field refers to the complete path to your ODBC driver.

Repeat the above procedure and create a second DSN. All the information should be the same, except for the names. For example, you might name the two DSNs as follows:

- **MS_Forefront_TMG** for Firewall logging, and
- **MS_Forefront_TMG_WP** for Web Proxy logging

Add the ODBC Event Source Type

You need to add two event source types, one to correspond to each of the DSNs that you created.

Run through the following procedure twice:

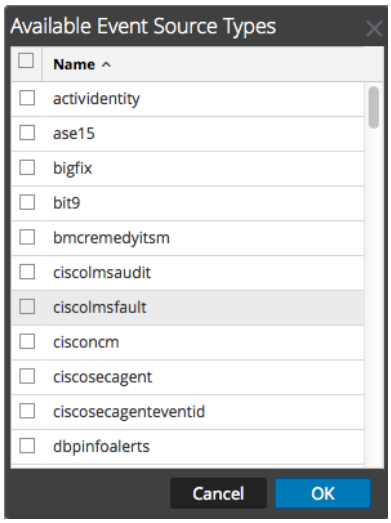
- In step 6:
  - First time through, select **ms_forefront_tmg** from the **Available Event Source Types** dialog.
  - Second time through, select **ms_forefront_tmg_wp** from the **Available Event Source Types** dialog.
- In step 10:

- First time through, select the DSN you created for Firewall logging.
- Second time through, select the DSN you created for Web Proxy logging.

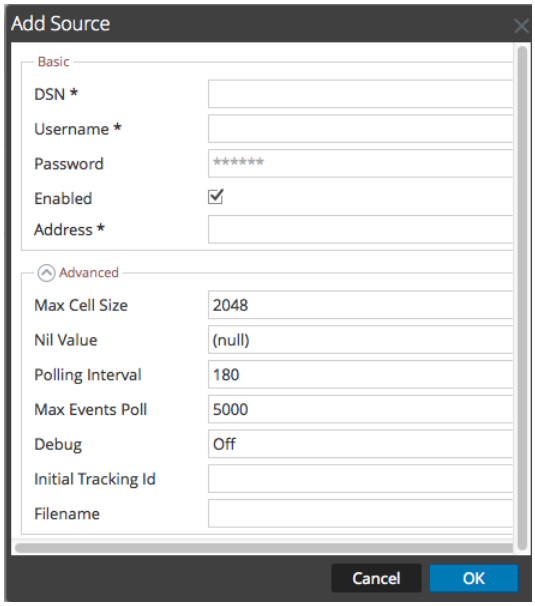
Add the ODBC Event Source Type:

1. In the **NetWitness** menu, select **Administration** > **Services**.
2. In the **Services** grid, select a **Log Collector** service.
3. Click  under **Actions** and select **View** > **Config**.
4. In the Log Collector **Event Sources** tab, select **ODBC/Config** from the drop-down menu.

   The Event Categories panel is displayed with the existing sources, if any.
5. Click + to open the **Available Event Source Types** dialog.



6. Choose the log collector configuration type for your event source type and click **OK**.
7. Fill in the parameters and click **Save**.
8. In the **Event Categories** panel, select the event source type that you just added.
9. In the **Sources** panel, click + to open the **Add Source** dialog.



10. Enter the DSN you configured during the **Configure a DSN** procedure.
11. For the other parameters, see ODBC Event Source Configuration Parameters in the SA User Guide.

Restart the ODBC Collection Service

Restart the ODBC collection service:

1. In the **Security Analytics** menu, select **Administration** > **Services**.
2. In the **Services** grid, select a **Log Collector** service.
3. Click  under **Actions** and select **View** > **System**.
4. Click **Collection** > **ODBC**.
   - If the available choice is **Start**, click **Start** to start ODBC collection.
   - If the available choices are **Stop** and **Pause**, click **Stop**, wait a few moments, and then click **Start**.

Trademarks