

RSA NetWitness Logs

Event Source Log Configuration Guide



Microsoft Forefront Unified Access Gateway

Last Modified: Thursday, June 08, 2017

Event Source Product Information:

Vendor: [Microsoft](#)

Event Source: Unified Access Gateway

Versions: 2010

Additional Download: [rsamsfuag.sql](#)

RSA Product Information:

Supported On: NetWitness Suite 10.0 and later

Event Source Log Parser: msfuag

Collection Method: Syslog, ODBC

Event Source Class.Subclass: Security.VPN

To configure Microsoft Forefront Unified Access Gateway to work with RSA NetWitness Suite, you must complete these tasks:

1. [Configure Microsoft Forefront Unified Access Gateway](#)
2. To configure the collection method, do one of the following:

Warning: To avoid duplicate data, you should configure Microsoft Forefront Unified Access Gateway for only one collection method.

- [Configure Syslog Collection](#)
- [Configure ODBC Collection](#)

Configure Microsoft Forefront Unified Access Gateway

To configure Microsoft Forefront Unified Access Gateway:

1. Log on to the Microsoft Forefront Unified Access Gateway Management console.
2. Click **Forefront Unified Access Gateway > HTTP Connections**.
3. For each trunk under **HTTP Connections**, do the following:
 - a. Click the trunk name.
 - b. In the **Trunk configuration** section, click **Configure**.
 - c. In the Advanced Trunk Configuration window, on the **General** tab, select **Enable web server logging** and **Include username in the log**.
 - d. Click **OK**.
4. Click **HTTPS Connections**, and repeat step 3 for each trunk listed.


Configure Syslog Collection

You need to configure the event source and RSA NetWitness Suite.

- [Configure Microsoft UAG for Syslog Collection](#)
- [Configure RSA NetWitness Suite for Syslog](#)

Configure Microsoft UAG for Syslog Collection

To configure Microsoft Unified Access Gateway for syslog collection:

1. Log on to the Microsoft Forefront Unified Access Gateway Management console.
2. Click **Admin > Event Log Settings**.
3. On the **Syslog** tab, follow these steps:
 - a. Select **Enable**.
 - b. In the **IP Address/host** field, enter the IP address of your RSA NetWitness Suite Log Decoder or Remote Log Collector.
 - c. Ensure that the **Port** field is set to **514**, the default value.
 - d. Click **OK**.
4. Click the **Activate Configuration** button. 
5. Click **Activate**.
6. Click **Finish**.

Configure RSA NetWitness Suite for Syslog

Perform the following steps in RSA NetWitness Suite:

- 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 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 **msfuag**.

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 **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 ODBC Collection

You need to configure the event source and RSA NetWitness Suite.

- [Configure Microsoft UAG for ODBC Collection](#)
- [Configure RSA NetWitness Suite for ODBC Collection](#)

Configure Microsoft UAG for ODBC Collection

Perform the following steps on the event source:

1. [Enable Logging of Events to the Threat Management Gateway Database](#)
2. [Create the Database That Will Host the Stored Procedures](#)
3. [Enable TCP Access to the Local Database on the Server](#)

Enable Logging of Events to the Threat Management Gateway Database

For instructions on enabling logging of UAG events into the TMG database, see the Microsoft Forefront Unified Access Gateway topic, [Logging to a SQL Server](#), on Microsoft TechNet.

Create the Database That Will Host the Stored Procedures

To create the database that will host the stored procedures:

1. Download [rsamsfuag.sql](#) from RSA Link.
2. On the system where Forefront UAG 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 **rsamsfuag.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 UAG 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. In 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 for TCP Dynamic Ports (delete the value **0** 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. To set the port on which to listen for ISARS protocols, follow these steps:
 - 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 for TCP Dynamic Ports (delete the value **0** 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 RSA NetWitness Suite for ODBC Collection

To configure ODBC collection in RSA NetWitness Suite, perform the following procedures:

- I. Ensure the required parser is enabled
- II. Configure a DSN
- 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 in 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 **msfuag**.

Configure a DSN

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**.


Field	Description
DSN Template (Security Analytics 10.4 and newer)	Choose the correct Oracle template from the available choices.
DSN Name	Enter a descriptive name for the DSN
Parameters section	
ServiceName	Enter the service name
PortNumber	The default port number is 1521
HostName	Specify the hostname or IP Address of the Oracle Identity Manager database
Edition Name	Enter the name of the Oracle edition

Field	Description
Driver	<p>If you choose one of the native templates, you can accept the default value, <code>/opt/netwitness/odbc/lib/R3sqls26.so</code>.</p> <p>If you choose one of the server templates, you need to point to the correct driver file on the Microsoft Forefront UAG server.</p>

Add the Event Source Type

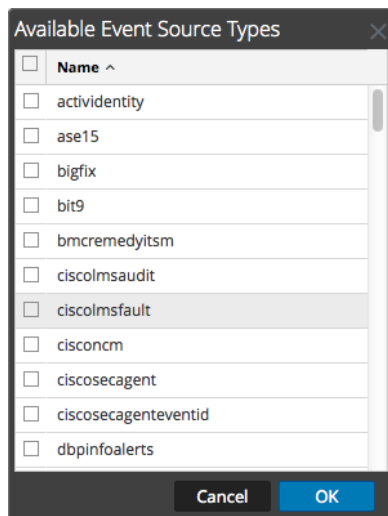
In step 6 below, select `ms_forefront_uag` from the **Available Event Source Types** dialog.

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.

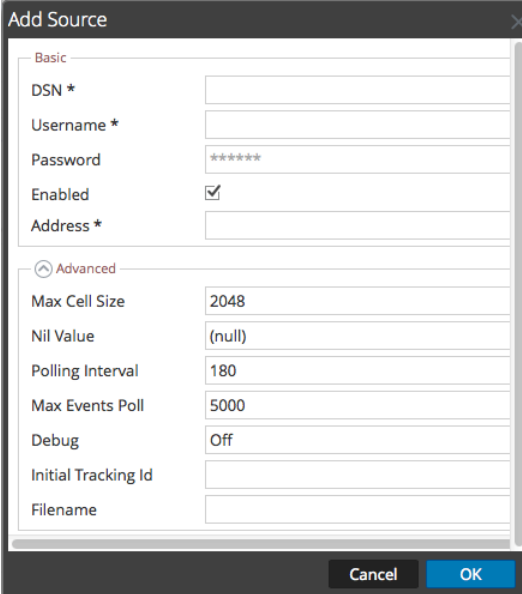
The Event Categories panel is displayed with the existing sources, if any.

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.




The screenshot shows the 'Add Source' dialog box with the following fields and values:

Section	Field	Value
Basic	DSN *	
	Username *	
	Password	*****
	Enabled	<input checked="" type="checkbox"/>
	Address *	
Advanced	Max Cell Size	2048
	Nil Value	(null)
	Polling Interval	180
	Max Events Poll	5000
	Debug	Off
	Initial Tracking Id	
	Filename	

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**.

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.