RSA NetWitness Platform

Event Source Log Configuration Guide

Microsoft Exchange Server

Last Modified: Friday, May 3, 2019

Event Source Product Information:

Vendor: Microsoft
Event Source: Exchange Server
Versions: 2003, 2007, 2010, 2013, 2016
Additional Downloads: sftpagent.conf.msexchange, sftpagent.conf.msexchange2k7, sftpagent.conf.msexchange2010, sftpagent.conf.msexchange2013, sftpagent.conf.msexchange2016, LOGbinder EX (for Exchange Server 2010, 2013 and 2016)

Note: Additional downloads are available in RSA Link at this URL: https://community.rsa.com/docs/DOC-47139

RSA Product Information:

Supported On: NetWitness Platform 10.0 and later
Event Source Log Parser: msexchange
Collection Method: File and Windows Event Logs
Event Source Class.Subclass: Host.Mail Servers

Depending on your version of Microsoft Exchange Server, do one of the following:

- Configure Collection from Microsoft Exchange Server 2003
- Configure Collection from Microsoft Exchange Server 2007
- Configure SMTP Protocol logging on Microsoft Exchange Server 2007, 2010, 2013 and 2016
- Configure Collection from Microsoft Exchange Server 2007 Service Pack 2 and later
- Configure Microsoft Exchange Server 2010, 2013 and 2016 for Administrator Audit and Mailbox Audit
- Configure User Mailbox to enable or disable MAPI on Microsoft Exchange Server 2010, 2013 and 2016
- Configure Collection from Microsoft Exchange Server 2010
- Configure Collection from Exchange Server 2013 and 2016

To configure File collection, see Configure SFTP and File Collection

Configure Collection from Microsoft Exchange Server 2003

To configure Microsoft Exchange Server 2003:

I. Set Up Your Windows Legacy Event Source Domain

II. Configure the Windows Legacy Event Source in RSA NetWitness Platform

III. Configure Microsoft Exchange Server 2003

IV. Configure SFTP and File Collection

Set Up Your Windows Legacy Event Source Domain

Important: You only need to perform this task if this the first time you are configuring Windows Legacy event collection for RSA NetWitness Platform and have not set up your event source domain for NetWitness Windows Legacy collection.

To set up your event source domain for Windows Legacy event source collection:

1. Download the **RSA Security Analytics Legacy Windows Collection Update and Installation Instructions** guide from RSA Link here: https://community.rsa.com/docs/DOC-41196
2. Follow the instructions in this document to set up your event source domain so that the RSA NetWitness Log Collector can collect events from Windows Legacy event sources.

Configure the Windows Legacy Event Source in RSA NetWitness Platform:

To configure the Windows Legacy Event Source in RSA NetWitness Platform:

1. Visit RSA Link for NetWitness and search for the help topic **Configure Windows Legacy and NetApp Event Sources**.
2. Complete the steps in this topic using the following value for the **Event Log Name**:

   Application

Configure Microsoft Exchange Server 2003

To configure Microsoft Exchange Server 2003:

1. To set Up Windows Application Event Logging and Collect Windows Application event log messages in Microsoft Exchange Server 2003, follow these steps:
   a. Open the Exchange System Manager.
   b. Click **Administrative Group** or **Organization** > **Servers**.
   c. Right-click the name of the server, and select **Properties**.
   d. On the **Diagnostics Logging** tab, enable logging at the levels shown in the following table.

      Note: Hardware platforms and server loads influence how much degradation your system will experience if you enable logging.

Service	Category	Logging Level
IMAPSvc4	Connections	Maximum
	Authentication	Maximum
	General	Maximum
POPSvc4	Connections	Maximum
	Authentication	Maximum
	General	Maximum
MSExchangeDSAccess	General	Maximum
MSExchangeIS - System	Connections	Maximum
	General	Maximum
MSExchange - Public Folders	Logons	Maximum

   e. Click **OK**.
2. To collect message tracking log messages, follow these steps:
   a. Open the Exchange System Manager.
   b. Click **Administrative Group** or **Organization** > **Servers**.

c. In the Servers window, right-click the name of the server, and select **Properties**.

d. Click the **General** tab.

e. Select **Enable subject logging and display** and **Enable message tracking**.

f. Click **OK**.

Configure Collection from Microsoft Exchange Server 2007

To configure Microsoft Exchange Server 2007:

I. Set Up Your Windows Systems for RSA NetWitness Platform

II. Configure RSA NetWitness Platform for this Event Source

III. Configure Microsoft Exchange Server 2007

IV. Configure SFTP and File Collection

To configure Windows Collection:

1. To set up your event source domain for Windows event source collection, see the Configure Windows Collection topic on RSA Link. Follow the instructions in this document.

   Important: You only need to perform this task if this the first time you are configuring Windows event collection for the RSA NetWitness Platform and have not configured your Windows systems for RSA NetWitness Platform.

2. Download the Microsoft WinRM Configuration Guide from RSA Link, and follow the directions in this guide.

3. When configuring Windows Collection on the RSA NetWitness Platform Log Collector, enter the following values for **Channel**:

   Application, **Exchange Auditing**

Configure Microsoft Exchange Server 2007

To configure Microsoft Exchange Server 2007:

1. To collect Windows event log messages, using the Exchange Management Shell, configure the logging services at the levels shown in the following table.

Service	Category	Logging Level
MSExchange ADAccess	General	Expert
MSExchangeIS\9002 System	Connections	Expert
	General	Expert

Service	Category	Logging Level
MSExchangeIS\9001 Public	Logons	Expert
	General	Expert
	Access Control	Expert
MSExchangeIS\9000 Private	Logons	Expert
	General	Expert
	Access Control	Expert

For more information, see the following articles on Microsoft TechNet:

- Diagnostic Logging of Exchange Processes
- Processes with Configurable Event Logging Levels
- Change Logging Levels for Exchange Processes

2. To confirm that message tracking logging is enabled, follow these steps:
   a. Open the Exchange Management Console.
   b. From the **Server Configuration** section, right-click the name of the server, and select **Properties**.
   c. Click the **Log Settings** tab.
   d. Ensure that **Enable message tracking logging** is selected.
   e. Click **OK**.

Configure SMTP Protocol logging on Microsoft Exchange Server 2007, 2010, 2013 and 2016

To configure SMTP Protocol Logging on Microsoft Exchange Server 2007 and 2010:

1. To enable protocol logging on a Receiver Connector from Exchange Management Console (EMC):
   a. Expand the **Server Configuration | Hub Transport** node.
   b. Select the Hub Transport server you want to configure, then select the **Receive Connector** > **Properties** tab.
   c. On the **General** tab, change the **Protocol Logging Level** to **Verbose**.
2. To enable protocol logging on a Send Connector from Exchange Management Console (EMC):
   a. Expand the **Organization Configuration | Hub Transport** node.
   b. On the **Send Connectors** tab, select the **Send Connector** > **Properties** tab.
   c. On the **General** tab, change the **Protocol Logging Level** to **Verbose**.

> **Note:** The default location of the SMTP protocol logs:
> Receive Connector logs are located in:
> **Exchange 2010**: \Exchange Server\V14\TransportRoles\Logs\ProtocolLog\SmtpReceive
> **Exchange 2007**: \Exchange Server\TransportRoles\Logs\ProtocolLog\SmtpReceive
>
> Send Connector logs are located in:
> **Exchange 2010**: \Exchange Server\V14\TransportRoles\Logs\ProtocolLog\SmtpSend
> **Exchange 2007**: \Exchange Server\TransportRoles\Logs\ProtocolLog\SmtpSend
>
> This location is used during Configuration of File Reader Collection of Exchange Server 2007 and 2010. Please refer to the additional download 'sftpagent.conf.MSExchangeSMTP'.

To configure SMTP Protocol Logging on Microsoft Exchange Server 2013 and 2016:

1. To enable protocol logging on a Receiver Connector and Send Connector connector in the Transport service on a Mailbox server, or on a Receive connector in the Front End Transport service on a Client Access server from Exchange Administration Console (EAC):
   a. In the EAC, navigate to **Mail flow** > **Send connectors** or **Mail flow** > **Receive connectors**.
   b. Select the connector you want to configure, and then click **Edit**.
   c. On the **General** tab in the **Protocol logging level** section, select **Verbose** Protocol logging is enabled on the connector.
   d. Click **Save**.
2. To configure the protocol log paths for the Send connectors and Receive connectors in the Transport service on a Mailbox server from Exchange Administration Console (EAC):
   a. In the EAC, navigate to **Servers** > **Servers**.
   b. Select the Mailbox server you want to configure, and then click **Edit** .
   c. On the server properties page, click **Transport logs**.
   d. In the Protocol log section, change any of the following settings:
      - **Send protocol log path** The value you specify must be on the local Exchange server. If the folder doesn't exist, it will be created for you when you click **Save**.
      - **Receive protocol log path** The value you specify must be on the local Exchange server. If the folder doesn't exist, it will be created for you when you click **Save**.
   e. Click **Save**.

   Note: This location is used in “Send protocol log path” and “Receive protocol log path” should be used during Configuration of File Reader Collection of Exchange Server 2013 and 2016. Please refer to the additional download ‘sftpagent.conf.MSExchangeSMTP’.

Configure Collection from Microsoft Exchange Server 2007 Service Pack 2 and Later

To configure Microsoft Exchange Server 2007 SP2:

I. Set Up Your Windows Systems and configure RSA NetWitness Platform for this Event Source

II. Configure Microsoft Exchange Server 2007 SP2

III. Configure SFTP and File Collection

Set Up Windows and Configure RSA NetWitness Platform

To configure Windows Collection:

1. To set up your event source domain for Windows event source collection, see the Configure Windows Collection topic on RSA Link. Follow the instructions in this document.

   Important: You only need to perform this task if this the first time you are configuring Windows event collection for the RSA NetWitness Platform and have not configured your Windows systems for RSA NetWitness Platform.

2. Download the Microsoft WinRM Configuration Guide from RSA Link, and follow the directions in this guide.

3. When configuring Windows Collection on the RSA NetWitness Platform Log Collector, enter the following values for **Channel**:

   Using a comma as the delimiter between channel names, enter any of the following event channels to which you want to subscribe:

   - Application
   - Exchange Auditing
   - Microsoft-Exchange-MailboxDatabaseFailureItems/Operational
   - Microsoft-Exchange-HighAvailability/Operational

- Microsoft-Exchange-HighAvailability/Debug

Note: You must enter the names as they appear in the preceding list. If you misspell any channel name, events from that channel will not be collected.

Configure Microsoft Exchange Server 2007 SP2

To configure Microsoft Exchange Server 2007 SP2:

1. To set up Windows Application event logging and collect Windows Application event log messages, follow these steps:
   a. Open the Exchange Management Console.
   b. From the navigation menu, click **Microsoft Exchange On-Premises** > **Server Configuration**.
   c. In the Actions pane, click **Manage Diagnostic Logging Properties**.
   d. Select **Update logging levels for services**.
   e. From the **Configure Server Diagnostic Logging Properties** list, enable logging of services at the levels shown in the following table.

Service	Category	Logging Level
MSExchange ADAccess	General	Expert
MSExchangeIS\9002 System	Connections	Expert
	General	Expert
MSExchangeIS\9001 Public	Logons	Expert
	General	Expert
	Access Control	Expert
MSExchangeIS\9000 Private	Logons	Expert
	General	Expert
	Access Control	Expert

   f. Click **Configure**.
   g. In the **Completion** window, check the status of the configuration.

If the configuration fails, use the **Back** button to make the necessary changes.

h. Click **Finish**.

2. In Microsoft Exchange Server 2007, to confirm that message tracking logging is enabled, follow these steps:

   a. Open the Exchange Management Console.

   b. From the **Server Configuration** section, right-click your server, and select **Properties**.

   c. On the **Log Settings** tab, ensure that **Enable message tracking logging** is selected.

   d. Click **OK**.

   In Microsoft Exchange Server 2010, to confirm that message tracking logging is enabled, follow these steps:

   a. Open the Exchange Management Console.

   b. From the navigation menu, click **Microsoft Exchange On-Premises** > **Server Configuration**.

   c. From the **Server Configuration** section, right-click your server, and select **Properties**.

   d. On the **Log Settings** tab, ensure that **Enable message tracking log** is selected.

   e. Click **OK**.

3. To enable Microsoft Exchange Server 2007 Exchange Auditing, follow these steps:

   a. Open the Exchange Management Console.

   b. Click **Server Configuration** > **Mailbox**.

   c. In the **Create Filter** section, right-click the name of your server, and select **Manage Diagnostic Logging Properties**.

   d. Click ***ServerName*** > **MSExchangeIS** > **9000 Private**.

   e. Select **Folder Access**, **Message Access**, **Extended Send As**, and **Extended Send On Behalf Of**, and set their logging levels to **Expert**.

   f. Click **Configure**, then click **Finish**.

Configure Microsoft Exchange Server 2010, 2013 and 2016 for Administrator Audit and Mailbox Audit

To configure Microsoft Exchange Server 2010, 2013 and 2016 for Administrator Audit and Mailbox Audit:

1. To configure Microsoft Exchange Server 2010, 2013 and 2016 for Administrator Audit and Mailbox Audit:
   a. Log on to the Microsoft Exchange Server 2010, 2013 and 2016 using Domain Privileges.
   b. Configure Exchange Mailbox Auditing using the link:

      http://www.ultimatewindowssecurity.com/exchange/mailboxaudit/configure.aspx

      Please refer to the example command:

      ```
      Set-Mailbox -Identity "John Smith" -AuditDelegate
      SendAs,SendOnBehalf,MessageBind,FolderBind -AuditEnabled $true
      ```

      in the link to Configure Mailbox Auditing for each of the users and their respective parameters for each user as per company requirements. Run this command using the “Exchange Management Shell” with administrator privileges.
   c. Configure Exchange Administrator Auditing using the link:

      http://www.ultimatewindowssecurity.com/exchange/adminaudit/configure.aspx

      Please refer to the sample command:

      ```
      Set-AdminAuditLogConfig -AdminAuditLogEnabled $true -
      AdminAuditLogCmdlets * -AdminAuditLogParameters * -
      AdminAuditLogExcludedCmdlets *Mailbox*, *TransportRule*
      ```

      in the link to Configure Administrator Auditing for each of the users and their respective parameters for each user as per company requirements . Run this command using the “Exchange Management Shell” with administrator privileges.
   d. Configure Microsoft Exchange for changing the Exchange audit search poll interval:

      The value that controls the search poll interval timing is stored in an XML configuration file under the *%ExchangeInstallPath%* folder. The file is in the *Bin* folder, and called *Microsoft.Exchange.Servicehost.exe.config*. Look for the following line inside the<appSettings> tag:

```
<add key="AuditLogSearchPollIntervalInMilliseconds" value="…" />
```

This value determines (in milliseconds) the search poll interval. Set the value to an appropriate number for the task.

2. To configure LOGbinder EX to send Administrator Audit and Mailbox Audit to RSA NetWitness Platform:

> **Note:** To collect auditing events from Microsoft Exchange Server into the Windows Event Viewer, you must download the third-party application LOGbinder EX from http://www.logbinder.com. When configuring Exchange Server 2010 and 2013, you must download LOGbinder EX 2.0. For Microsoft Exchange Server 2016, download LOGbinder EX 3.4.28.0 from http://www.logbinder.com.

   a. For Microsoft Exchange Server 2010, 2013 and 2016, download LOGbinder as described in the previous Note.

   b. To configure the input settings, follow these steps:

      i. In the LOGbinder EX interface, click **New Input**.

      ii. Refer to the LOGbinder EX documentation to enter the fields "Powershell URL", "Exchange URL", and "Recipient" correctly.

      iii. Click **OK**.

   c. To configure the output settings, follow these steps:

      i. Click **Output**.

      ii. Using LOGbinder EX, double-click **LOGbinder EX Event Log** and ensure that **Send output to LOGbinder EX Event Log** is selected.

      iii. Deselect **Include noise events** and **Include XML data**.

      iv. Click **OK**.

   d. To start the service, follow these steps:

      i. Click **Service**.

      ii. Click **Start**.

Configure User Mailbox to enable or disable MAPI on Microsoft Exchange Server 2010, 2013 and 2016

To enable or disable MAPI for a User Mailbox on Microsoft Exchange Server 2010, 2013 and 2016, see the following procedures.

Enable or Disable MAPI for Exchange Server 2010

To enable or disable MAPI for a User Mailbox on Microsoft Exchange Server 2010:

1. In the console tree, navigate to **Recipient Configuration** > **Mailbox**.
2. In the Result pane, select the user mailbox for which you want to enable or disable MAPI.
3. In the Action pane, under the mailbox name, click **Properties**.
4. In **< User Mailbox** > **Properties**, on the **Mailbox Features** tab, click **MAPI**, then click either **Enable** or **Disable**.
5. Click **OK**.

Enable or Disable MAPI for Exchange Server 2013

To enable or disable MAPI for a User Mailbox on Microsoft Exchange Server 2013:

1. In the EAC, navigate to **Recipients** > **Mailboxes**.
2. In the list of user mailboxes, click the mailbox that you want to enable or disable MAPI, and then click **Edit** .
3. On the mailbox properties page, click **Mailbox Features**.
4. Under **Email Connectivity**, do one of the following:
   a. To disable MAPI, under **MAPI: Enabled** click **Disable**.

      A warning appears asking if you're sure you want to disable MAPI. Click **Yes**.

b. To enable MAPI, under **MAPI: Disabled** click **Enable**.

5. Click **Save**.

Enable or Disable MAPI for Exchange Server 2016

To enable or disable MAPI for a User Mailbox on Microsoft Exchange Server 2016:

1. In the EAC, navigate to **Recipients** > **Mailboxes**.
2. In the list of mailboxes, find the mailbox that you want to modify by doing any of the following actions:
   - Scroll through the list of mailboxes, or
   - Click **Search** and enter part of the user's name, email address, or alias, or
   - Click **More options > Advanced search** to search for a specific mailbox.
3. After you find the mailbox that you want to modify, select it and then click **Edit**.

   The Mailbox Properties page is displayed.
4. On the mailbox properties page, click **Mailbox Features**.
5. In the **Email Connectivity** section, do one of the following:
   - If you see **MAPI: Enabled**, click **Disable** to disable it, and then click **Yes** in the warning message that appears.
   - If you see **MAPI: Disabled** click **Enable** to enable it.
6. Click **Save**.

Default Locations for Connectivity Logs

Note the following default locations for the SMTP and MAPI Connectivity logs:

- **Exchange 2010:**

  C:\Program Files\Microsoft\Exchange Server\V14\TransportRoles\Logs\Connectivity
- **Exchange 2013:**
  - **Transport service**: C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Logs\Hub\Connectivity

- **Front End Transport service**: C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Logs\FrontEnd\Connectivity
- **Mailbox Transport Delivery service**: C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Logs\Mailbox\Connectivity\Delivery
- **Mailbox Transport Submission service**: C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Logs\Mailbox\Connectivity\Submission

- **Exchange 2016:**
  - **Transport service**: C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Logs\Hub\Connectivity
  - **Front End Transport service**: C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Logs\FrontEnd\Connectivity
  - **Mailbox Transport Delivery service**: C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Logs\Mailbox\Connectivity\Delivery
  - **Mailbox Transport Submission service**: C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Logs\Mailbox\Connectivity\Submission

These locations are used during Configuration of File Collection of Exchange Server 2010, 2013 and 2016. Please refer to the additional downloads **sftpagent.conf.msexchange2010**, **sftpagent.conf.msexchange2013** and **sftpagent.conf.msexchange2016**

Configure Collection from Exchange Server 2010

To configure Windows Collection:

1. To set up your event source domain for Windows event source collection, see the Configure Windows Collection topic on RSA Link. Follow the instructions in this document.
2. Download the Microsoft WinRM Configuration Guide from RSA Link, and follow the directions in this guide.
3. When configuring Windows Collection on the RSA NetWitness Platform Log Collector, enter the following values for **Channel**:

   Application, **LOGbndEX**, **Exchange Auditing**

Configure Collection from Exchange Server 2013 and 2016

To configure Windows Collection:

1. To set up your event source domain for Windows event source collection, see the Configure Windows Collection topic on RSA Link. Follow the instructions in this document.
2. Download the Microsoft WinRM Configuration Guide from RSA Link, and follow the directions in this guide.
3. When configuring Windows Collection on the RSA NetWitness Platform Log Collector, enter the following values for **Channel**:

   Application, **LOGbndEX**

Configure SFTP and File Collection

You must complete these tasks to configure File Collection for RSA NetWitness Platform:

I. Set up the SFTP Agent

II. Configure the Log Collector for File Collection

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

Configure the Log Collector for File Collection

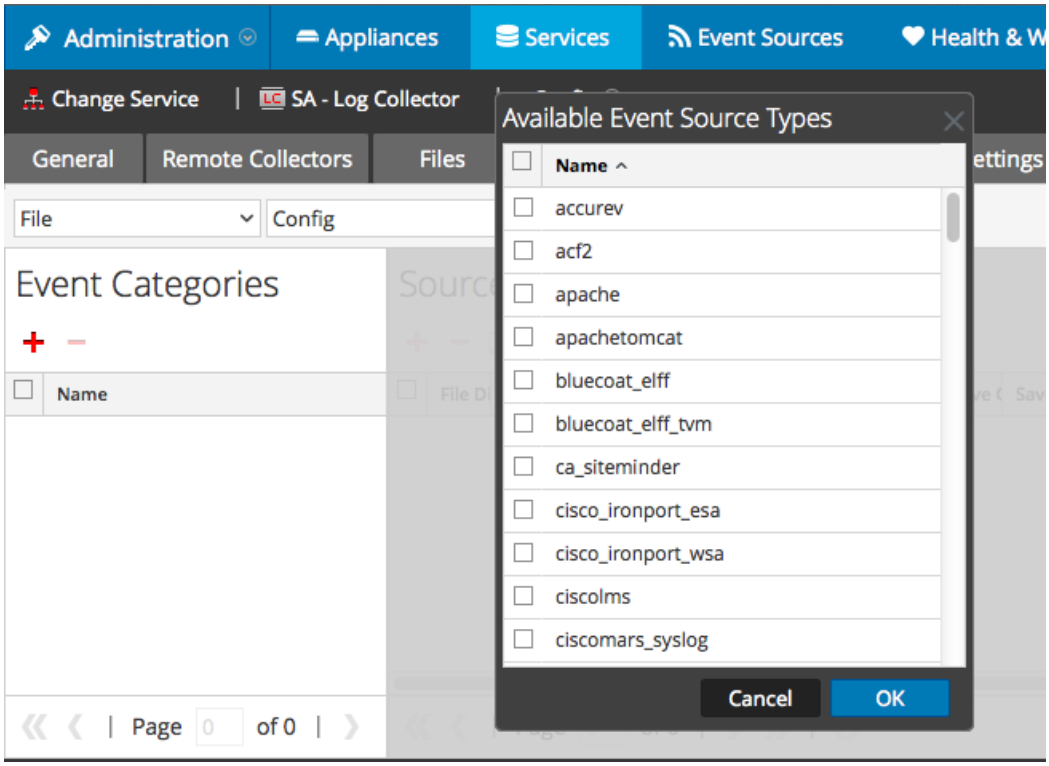
Perform the following steps to configure the Log Collector for File collection.

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.



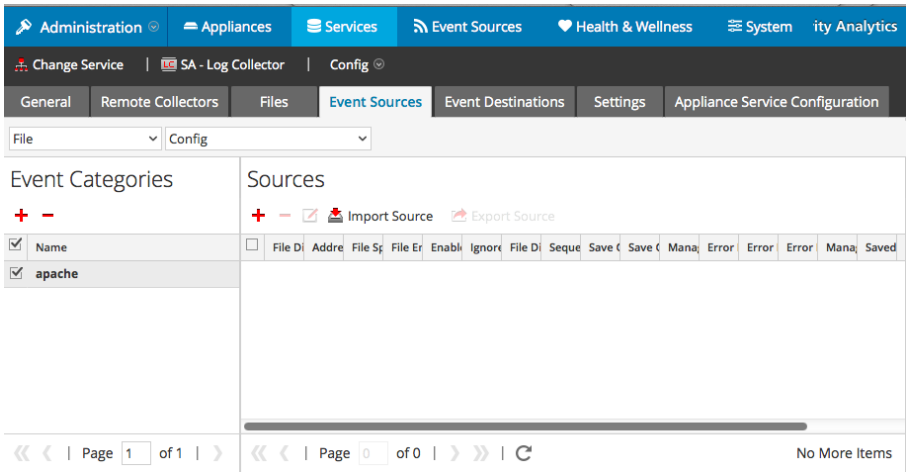
5. Select the correct type from the list, and click **OK**.

   Depending on your Microsoft Exchange Server version, select one of the following from the **Available Event Source Types** dialog:

   - For MS Exchange Server 2003, select **exchange**
   - For MS Exchange Server 2007 (and 2007 SP2), select **exchange2007**
   - For MS Exchange Server 2010, select **exchange2010**
   - For MS Exchange Server 2013, select **exchange2013**
   - For MS Exchange Server 2016, select **exchange2016**

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

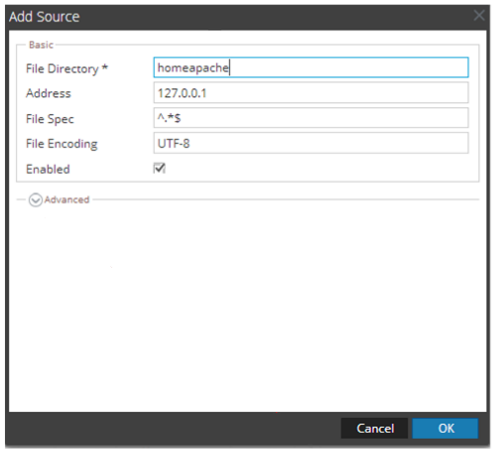
   Note: The image below uses **Apache** as an example only. Your screen will look different, depending on which Event Source type you are configuring.

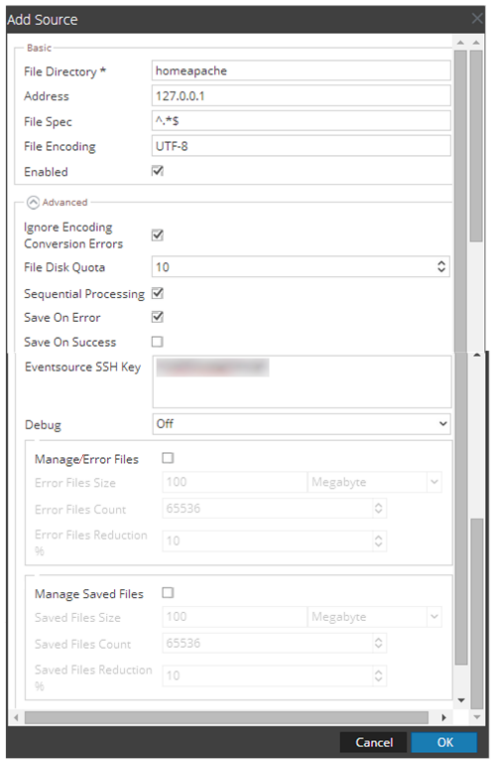


6. Select the new type in the Event Categories panel and click + in the Sources panel toolbar.

   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.

Trademarks

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